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

HP-UX

5.0.1

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 5.0.1

Document version 5.0.1.0

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

http://www.symantec.com/business/services/category.jsp?pcid=support_services

Contacting Technical Support

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

www.symantec.com/business/support/assistance_care.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:

https://licensing.symantec.com

Customer service

Customer service information is available at the following URL:

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

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance 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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Section 1

SF Oracle RAC requirements and planning

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 optional components
- About SF Oracle RAC features
- About SF Oracle RAC licensing

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 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 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. 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.
- Use of clustered file system for placement of Oracle Cluster Registry and voting disks. Clustered file system and volume management technologies provide robust shared block and raw interfaces for placement of Oracle Cluster Registry 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 and SAN switches.
- 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 Reservation (PGR) based I/O fencing.

- 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
- Optimized I/O performance through storage mapping technologies and tunable attributes.

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.
Oracle Clusterware	Oracle Clusterware manages the cluster membership and communications between cluster nodes. It manages all of the Oracle processes automatically. Anything that Oracle Clusterware manages is known as a cluster resource, which could be a database, an instance, a service, a listener, a virtual IP (VIP) address, or an application process. Oracle Clusterware is a requirement for using Oracle RAC.

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 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 25.
Veritas Cluster Server Management Console	See "About Veritas Cluster Server Management Console" on page 24.

To configure the optional components, make sure to install all packages when the installation program prompts you.

About Veritas Cluster Server Management Console

Veritas Cluster Server Management Console is a high availability management solution that enables monitoring and administering clusters from a single Web console.

You can configure Veritas Cluster Server Management Console to manage multiple clusters.

Refer to the *Veritas Cluster Server Management Console Implementation Guide* for installation, upgrade, and configuration instructions.

For information on updates and patches for VCS Management Console, see http://seer.entsupport.symantec.com/docs/308405.htm.

To download the most current version of VCS Management Console, go to www.symantec.com/business/cluster-server and click **Utilities**.

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 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.
- 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 60.

About SF Oracle RAC features

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

- About I/O fencing
- About VCS notifications
- About campus clusters
- About global clusters
- About Veritas Volume Replicator
- About Veritas Storage Checkpoint and Storage Rollback

- About Veritas Database FlashSnap
- About Veritas Dynamic Storage Tiering

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 installsfrac program installs the SF Oracle RAC I/O fencing driver, VRTSvxfen. 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.

About I/O fencing components

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

- Data disks—Store shared data
  See "About data disks" on page 26.
- Coordination points—Act as a global lock during membership changes
  See "About coordination points" on page 27.

About data disks

Data disks are standard disk devices for data storage and are either physical disks or RAID Logical Units (LUNs). These disks must support SCSI-3 PR and are part of standard VxVM or CVM disk groups.

CVM is responsible for fencing data disks on a disk group basis. Disks that are added to a disk group and new paths that are discovered for a device are automatically fenced.

About coordination points

Coordination points provide a lock mechanism to determine which nodes get to fence off data drives from other nodes. A node must eject a peer from the coordination points before it can fence the peer from the data drives. Racing for control of the coordination points to fence data disks is the key to understand how fencing prevents split brain.

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

Dynamic Multipathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. On cluster nodes with HP-UX 11i v3, you must use DMP devices or iSCSI devices for I/O fencing. The following changes in HP-UX 11i v3 require you to not use raw devices for I/O fencing:

- Provides native multipathing support
- Does not provide access to individual paths through the device file entries

The metanode interface that HP-UX provides does not meet the SCSI-3 PR requirements for the I/O fencing feature. You can configure coordinator disks to use Veritas Volume Manager Dynamic Multipathing (DMP) feature.

See the *Veritas Volume Manager Administrator's Guide*.

About VCS notifications

You can configure both SNMP and SMTP notifications for VCS. Symantec recommends you to configure 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 User'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. You are required to have a separate license to configure global clusters. You may add this license during the installation or at any time after the installation completes.

About 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 Veritas Storage Checkpoint and Storage Rollback

Veritas Storage Checkpoint is used for efficient backup and recovery of Oracle databases. It provides a consistent point-in-time image of the database. A Storage Checkpoint can be mounted as read-only or read-write, and allows access to the files as if it were a regular file system.

Storage Rollback rolls back the changed blocks in a Storage Checkpoint into the primary file system for faster database restoration.

For detailed information about the feature, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

About Veritas Database FlashSnap

Database FlashSnap offers you a flexible way to efficiently manage multiple point-in-time snapshots of your data, and reduce resource contention on your business-critical servers.

A database snapshot can be used for the following off-host processing applications:

- Data backup
- Data warehousing
- Decision-support queries

For detailed information about the feature, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

About Veritas Dynamic Storage Tiering

Veritas Database Dynamic Storage Tiering (DBDST) enables you to manage your data so that less-frequently used data can be moved to slower, less expensive disks. Thus, frequently-accessed data can be stored on faster disks for quicker retrieval.

To use Database Dynamic Storage Tiering, your storage must be managed using the following features:

- VxFS multi-volume file system
- VxVM volume set
- Volume tags
- Dynamic Storage Tiering policies

For detailed information about the feature, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

About SF Oracle RAC licensing

SF Oracle RAC requires a license key certificate. The certificate specifies the product keys and the number of product licenses purchased. A single key lets you install the product on the number and type of systems for which you purchased the license.

Note: A key may enable the operation of more products than are specified on the certificate; however, you are legally limited to the number of product licenses purchased.

Chapter 2

Installation planning and requirements

This chapter includes the following topics:

Important preinstallation information

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

- Hardware compatibility list to confirm the compatibility of your hardware:
  http://entsupport.symantec.com/docs/283161
- TechNote for late-breaking and new information on updates, patches, and software issues regarding this release:
  http://entsupport.symantec.com/docs/281875
- Latest information on support for Oracle database versions. See the Technical Support TechNote:
  http://entsupport.symantec.com/docs/280186
- 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.

Installation requirements

Make sure that each node on which you want to install or upgrade SF Oracle RAC meets the following installation requirements:

- Hardware requirements
- Supported software
- Supported HP-UX operating systems
- Supported replication technologies for global clusters
- License requirements

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 32.
For campus clusters	See Table 2-2 on page 33.

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. HP-UX 11i v3 March 2009 OEUR release or later must be installed on these systems.
DVD drive	One drive that is accessible to all 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 following command: `# ./installsfrac -precheck node_name` For details on the additional space that is required for Oracle, see the Oracle documentation.

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

Item	Description
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	The minimum swap space requirement for Oracle RAC 10g is 4 GB. The minimum swap space requirement for Oracle RAC 11g is 8 GB. The operating system requirement for minimum swap space is two times the size of RAM. Between the minimum requirements of Oracle RAC and the operating system, make sure that you meet the minimum requirement that is higher. For example, if the operating system requirement for minimum swap space computes to 5 GB on your Oracle RAC 11g systems, make sure that you meet the minimum swap space requirement of Oracle RAC, that is 8 GB.
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.
Fibre Channel or SCSI host bus adapters	At least one built-in SCSI adapter per system to access the operating system disks. 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 both sites.

Table 2-2 Hardware requirements for campus clusters *(continued)*

Item	Description
Network	■ Oracle requires that all nodes use the IP addresses from the same subnet. ■ Volumes must be mirrored with storage allocated from both sites. ■ Symantec recommends two Network Interface Cards (NIC) per host for LLT heartbeats. Oracle Clusterware requires one private and one virtual IP for each host. ■ 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. ■ 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.

Supported software

Table 2-3 lists supported software versions.

Table 2-3 Supported software

Software	Version
Oracle RAC	**Note:** SF Oracle RAC supports only 64-bit Oracle. ■ Oracle RAC 10g Release 2 ■ Oracle RAC 11g Release 1
HP-UX operating system	See "Supported HP-UX operating systems" on page 35.
Other HP-UX software	See "Other required HP-UX software" on page 36.

Table 2-3 Supported software *(continued)*

Software	Version
VCS, VxVM, VxFS, VVR	Use only versions of VCS, VxVM, VxFS, and VVR provided on the software disc. Remove other versions before you install the software from the SF Oracle RAC product disc. **Warning:** SF Oracle RAC and all component software must be at the same version across all nodes in an SF Oracle RAC cluster, in this case 5.0.1. Symantec strongly recommends upgrading all SF Oracle RAC component products to the same version at the same time.

To verify the latest information on support for Oracle database versions, see the Technical Support TechNote:

http://entsupport.symantec.com/docs/280186

Supported HP-UX operating systems

SF Oracle RAC 5.0.1 can be installed on the following operating systems:

- HP-UX 11i v3 March 2009 OEUR release or later

The following operating environments (OEs) are supported for SF Oracle RAC on HP-UX:

HPUX11i-OE	HP-UX 11i v3 Foundation OE
HPUX11i-OE-Ent	HP-UX 11i v3 Enterprise OE
HPUX11i-OE-MC	HP-UX 11i v3 Mission Critical OE

Required HP-UX patches

Table 2-4 lists the required HP-UX patches.

Table 2-4 Required patches

HP-UX patch ID	Description
PHSS_36311	This patch fixes a security vulnerability in HP-UX IA-64 platforms. The Veritas Enterprise Administrator Service Core and VRTSobc33 depots require this patch on IA-64 platforms.
PHKL_40022	This patch distributes vxiod threads to processors other than the moncarch CPU.

Table 2-5 lists the recommended HP-UX patches.

Table 2-5 Recommended patches

HP-UX patch ID	Patch name
PHKL_39401	This patch fixes a Virtual-Memory defect. This patch must be installed for Veritas File System (VxFS) to respond to memory pressure situations.

Warning: Install all the latest required HP-UX patches before you install SF Oracle RAC. You can use the `swlist` command to determine whether the correct update and patches are installed. The installation procedure terminates if the correct patches are not found.

HP may release patches that supersede the ones in this list. To verify that you have the latest HP-UX patches, go to the Symantec support website to view the relevant TechNote:

http://entsupport.symantec.com/docs/281875

Other required HP-UX software

If you plan to install SF Oracle RAC from an NFS mounted directory, you must install the software `ONCplus - HP-UX 11i v3 version B.11.31.07.01`. The `ONCplus B.11.31.06` software bundled with HP-UX 11i v3 March 2009 OEUR release reports issues with long path names. This causes the installation to fail as the installer can not copy files from the mounted directory to the systems on which you want to install SF Oracle RAC.

To download the software:

- Go to http://software.hp.com.
- Search for the software depot `ONCplus`.
- Download ONCplus for HP-UX 11i v3 version B.11.31.07.01.

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

License requirements

The following licenses are required for campus cluster and global cluster environments:

- SF Oracle RAC with HA/DR
- FlashSnap (FMR3) license
- Site awareness license for consistent mirror reattach

Planning your installation setup

This section provides guidelines and best practices for planning a resilient, high-performant SF Oracle RAC cluster. These best practices suggest optimal configurations for your core clustering infrastructure such as network and storage. Recommendations are also provided on planning for continuous data protection and disaster recovery.

Review the following planning guidelines before you install SF Oracle RAC:

- Planning your network configuration
- Planning the storage
- Planning volume layout
- Planning file system design
- Planning for I/O fencing
- 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 characteristics such as 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.
- Enable/disable Jumbo frames for network communication. Jumbo frames for network communications are not recommended when you use the Veritas supplied cache fusion library that employs Low Latency Transport (LLT) protocol for inter-instance communication. Jumbo frames are recommended when you use the User Datagram Protocol (UDP). Extreme inter-instance cache fusion load is necessary to yield any benefit from UDP and jumbo frames.
- Set the recommended values for LLT peer inactivity timeout and CSS miss-count.

  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 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 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.

  The default value for the CSS miss-count in case of SF Oracle RAC is 600 seconds. The value of this parameter is kept 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.

Planning the private network configuration for Oracle RAC

The private network for Oracle RAC requires a minimum of two unused IP addresses. Oracle Clusterware requires an IP address on each node for inter-node heartbeat communication. The Oracle RAC database requires an IP address for the cache-fusion data.

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

Depending on the version of Oracle RAC you want to install, you have the following options for setting up your private network configuration:

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. Depending on your deployment needs, this IP address may be a dedicated IP address or one that is shared with Oracle Clusterware.

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

The following practices are recommended for 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. There are multiple options available to achieve the same. Configuring the Oracle Clusterware interconnects over bonded NIC interfaces or IP failover solutions such as IPMP can provide the first level of protection.
  In the absence of such mechanisms, 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.
  See "High availability solutions for Oracle RAC private network" on page 40.

- 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.
- Configure multiple public networks for redundancy so that Oracle can failover virtual IP addresses if there is a public link failure.

For sample deployment scenarios illustrating the use of PrivNIC and MultiPrivNIC agents:

See "*SF Oracle RAC deployment scenarios*" on page 529.

High availability solutions for Oracle RAC private network

Table 2-6 lists the high availability solutions that you may adopt for your private network.

Table 2-6 High availability solutions for Oracle RAC private network

Options	Description
Using IPMP for Oracle Clusterware	If Oracle Clusterware interconnects are configured over IPMP, all the NICs that are configured under LLT must be configured under the IPMP group. In such a configuration, it is recommended not to manage these links using the PrivNIC/MultiPrivNIC agents.
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, a second link needs to be configured to prevent LLT from reporting jeopardy membership. The second link can be either a bonded interface or a simple NIC interface.

Table 2-6 High availability solutions for Oracle RAC private network *(continued)*

Options	Description
Using PrivNIC/MultiPrivNIC agents	Use one of the IP failover solutions, PrivNIC or MultiPrivNIC, in the following scenarios: ■ Due to operating system limitations, you can not use NIC bonding to provide increased bandwidth using multiple network interfaces. ■ The cluster is running multiple databases and you need to isolate the interconnect traffic. For more deployment scenarios that illustrate the use of PrivNIC/MultiPrivNIC deployments: See *"SF Oracle RAC deployment scenarios"* on page 529.

Planning the storage

SF Oracle RAC provides the following options for shared storage:

- CVM
  CVM provides native naming (cXtXdX) 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
  See "Planning for Oracle ASM over CVM" on page 45.

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, two switches and two storage arrays.
- 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 PGR 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.

- Use Database Dynamic Storage Tiering (DBDST) to optimize the storage cost. Using DBDST, less frequently used data can be moved to slower, less expensive disks. This also permits frequently accessed data to be stored on faster disks for quicker retrieval.

Planning the storage for Oracle RAC

Review the storage options and guidelines for Oracle RAC:

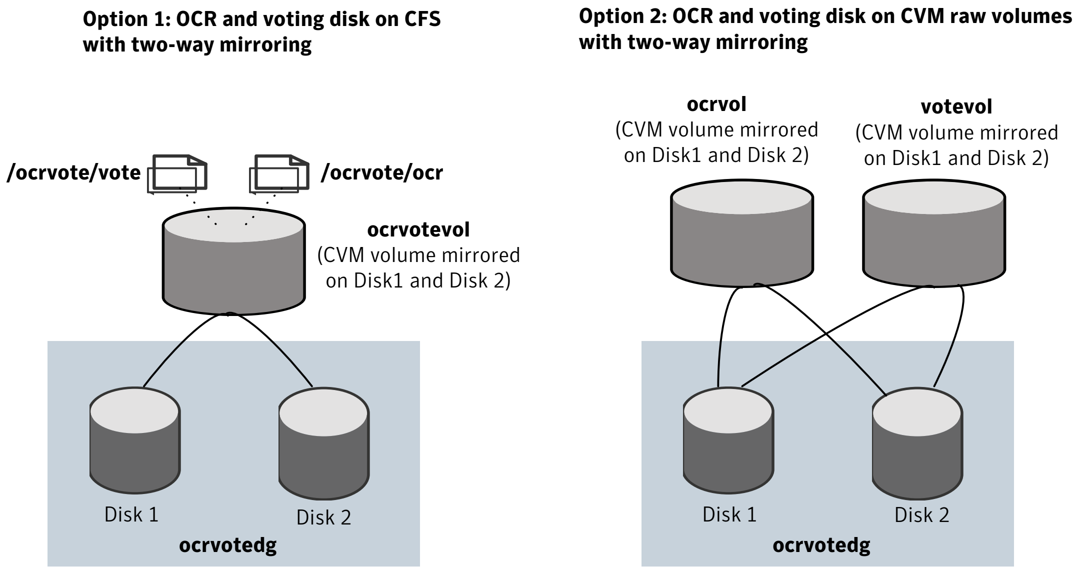
- Storage options for OCR and voting disk
  See "Planning the storage for OCR and voting disk" on page 42.
- Storage options for the Oracle RAC installation directories (ORACLE_BASE, CRS_HOME, and ORACLE_HOME)
  See "Planning the storage for Oracle RAC binaries and data files" on page 43.

Planning the storage for OCR and voting disk

You can place the OCR and voting disk information on a clustered file system or on CVM raw volumes.

Figure 2-1 illustrates the options for storing OCR and voting disk information.

Figure 2-1 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 (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.

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 and Oracle recommend 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.
- 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 2-7 lists the type of storage for Oracle RAC binaries and data files.

Table 2-7 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 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 binaries	Local or shared
Oracle database binaries	Local or shared Placing the Oracle database binaries on local disks enables rolling upgrade of the cluster.
Oracle RAC database	Shared
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 Oracle database home on separate mount points enables you to unmount the database for maintenance purposes without affecting other databases. 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 the storage for SF Oracle RAC

Table 2-8 lists the type of storage required for SF Oracle RAC binaries and data files.

Table 2-8 Type of storage required for SF Oracle RAC binaries and data files

SF Oracle RAC files	Type of storage
SF Oracle RAC binaries	Local

Table 2-8 Type of storage required for SF Oracle RAC binaries and data files *(continued)*

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

Planning for Oracle ASM over CVM

ASM provides storage only for the data files, control files, online and archive log files, and backup files. It does not support Oracle binaries, trace files, alert logs, export files, tar files, core files, Oracle Cluster Registry devices (OCR), and voting disk, application binaries and data.

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 installed 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 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.

Planning for I/O fencing

The following practices are recommended:

- Configure three LUNs as coordinator disks. Verify that the LUN is SCSI-3 compliant using the vxfentsthdw (1M) utility.
- Provide high availability to coordinator disks using DMP and multiple physical access paths.
- In the case of SF Oracle RAC in a stretch cluster, place the third coordinator disk at a third location to ensure cluster availability during split-brain scenarios involving site failure.
  iSCSI devices can now be used as coordinator disks for I/O fencing.

  Note: SF Oracle RAC supports iSCSI devices for I/O fencing. Make sure that the iSCSI devices are SCSI-3 PGR compliant.

- Refer to the following Symantec Tech Note for various options available to lower the risk of split brain:
  http://support.veritas.com/docs/252635

Planning for cluster management

Table 2-9 lists the various agents supported in SF Oracle RAC installations for effective cluster management.

Table 2-9 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 increased bandwidth using multiple network interfaces.

Table 2-9 List of agents *(continued)*

Agent	Description
MultiPrivNIC agent	High availability for multiple private IP addresses The MultiPrivNIC agent provides a reliable alternative in the following scenarios: ■ Operating system limitations prevent you from using NIC bonding to provide increased bandwidth using multiple network interfaces. ■ The interconnect traffic needs to be isolated when the cluster is running multiple databases.

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.

The following best practices may be borne in 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 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.
- In the case of a two-node 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.
- Enable the site consistency feature for site-aware plex detaches. Use site consistency tagging at the enclosure level.
- Set the 'allsites' attribute on the volumes so that the volumes are mirrored automatically across sites.
- Set the global detach policy on the disk groups. The local detach policy is not supported in SF Oracle RAC campus clusters.

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
- The acceptable recovery time after the disaster

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

SF Oracle RAC cluster setup models

SF Oracle RAC supports a variety of cluster configurations.

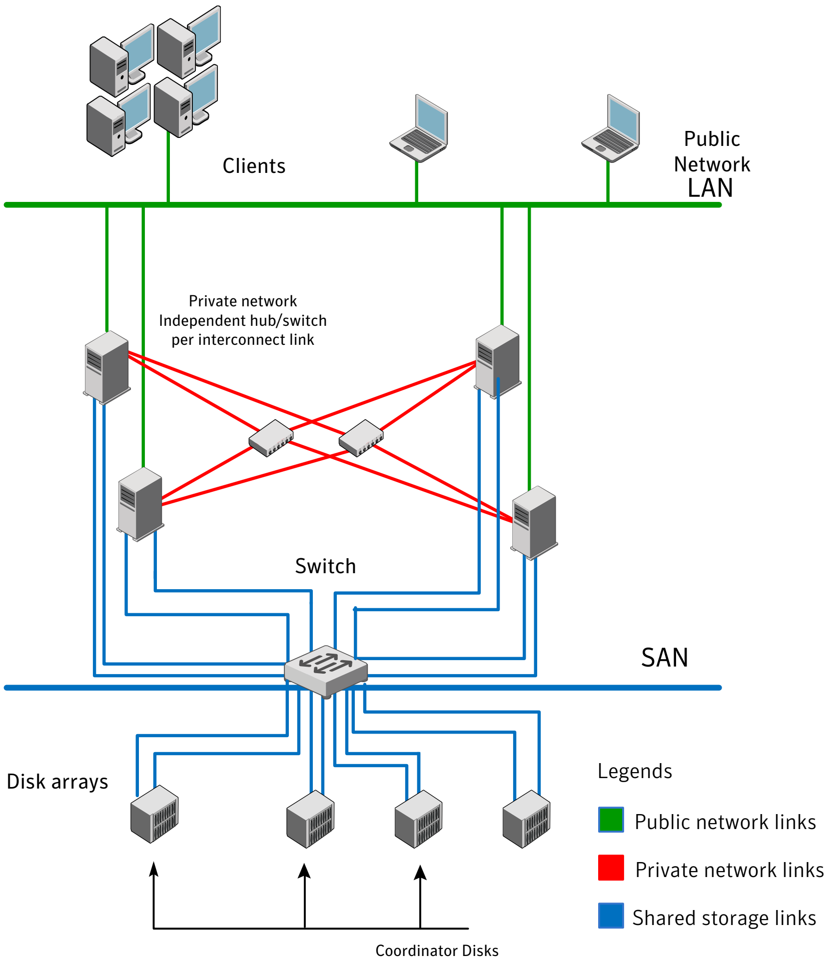
Depending on your business needs, you may choose from the following setup models:

- About basic SF Oracle RAC cluster setup
- About SF Oracle RAC setup for clusters in secure mode
- About SF Oracle RAC setup for cluster management
- About SF Oracle RAC campus cluster setup for disaster recovery
- About SF Oracle RAC global cluster setup for disaster recovery

About basic SF Oracle RAC cluster setup

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

Figure 2-2 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 must be connected with private network links using similar network devices.
- Each system has a VxVM encapsulated root drive or an internal disk.
  The root disk group for the storage must not be shared between systems.
- The Oracle Cluster Registry, vote disks, and data files configured on the shared storage that is available to each node. The shared storage can be a cluster file system or raw VxVM volumes.
- Three standard 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.

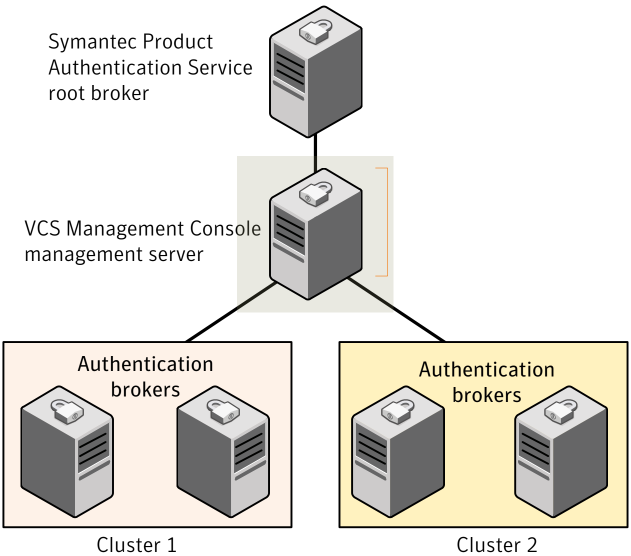
About SF Oracle RAC setup for clusters in secure mode

You can set up Authentication Service for the cluster during the installation or after installation. Before you install the authentication service, refer to the *Symantec Product Authentication Service Installation Guide* at the following location on the Veritas software disc:

A secure cluster setup requires you to configure a system in your enterprise as the root broker and all nodes in the cluster as authentication brokers.

Figure 2-3 illustrates a sample secure cluster setup.

Figure 2-3 SF Oracle RAC secure cluster setup



A secure cluster setup uses the Authentication Service to secure communication between the following:

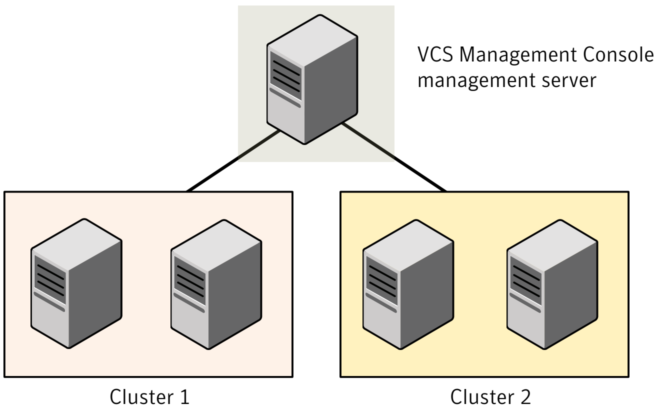
- Cluster nodes and clients, including the VCS Java and the Web consoles.
  You can set up Authentication Service for the cluster during the SF Oracle RAC installation and configuration process.
  If you want to enable Authentication Service after installation, refer to the *Veritas Cluster Server User's Guide*.
- Veritas Cluster Server Management Console management server and the centrally managed SF Oracle RAC clusters.

About SF Oracle RAC setup for cluster management

Veritas Cluster Server Management Console is a high availability management solution that enables you to monitor and administer multiple clusters from a single Web console. SF Oracle RAC nodes must be discovered by the cluster management console server before you can manage the nodes using the server.

Figure 2-4 illustrates centralized management of SF Oracle RAC clusters using Veritas Cluster Server Management Console.

Figure 2-4 Centralized management of SF Oracle RAC cluster



For more information, see the *Veritas Cluster Server Management Console Implementation Guide*.

About SF Oracle RAC campus cluster setup 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).

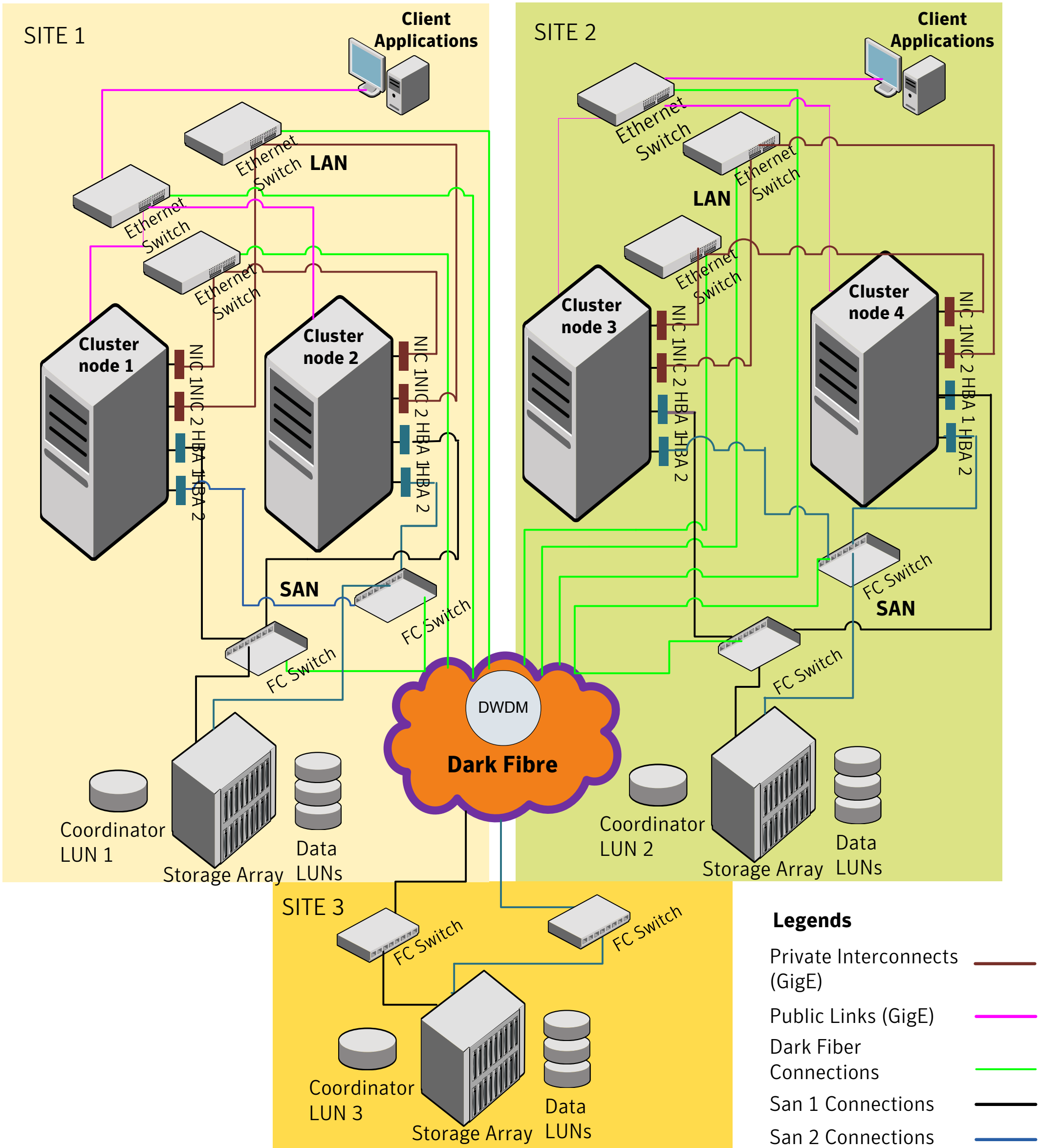
The SF Oracle RAC campus cluster addresses the following basic challenges in campus cluster configurations:

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. You can not use VCS firedrill on SF Oracle RAC campus clusters.

Figure 2-5 illustrates a basic campus cluster setup.

Figure 2-5 Basic campus cluster setup



About SF Oracle RAC global cluster setup 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.

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 supported replication technologies:

See "Supported replication technologies for global clusters" on page 36.

Section 2

SF Oracle RAC installation and configuration

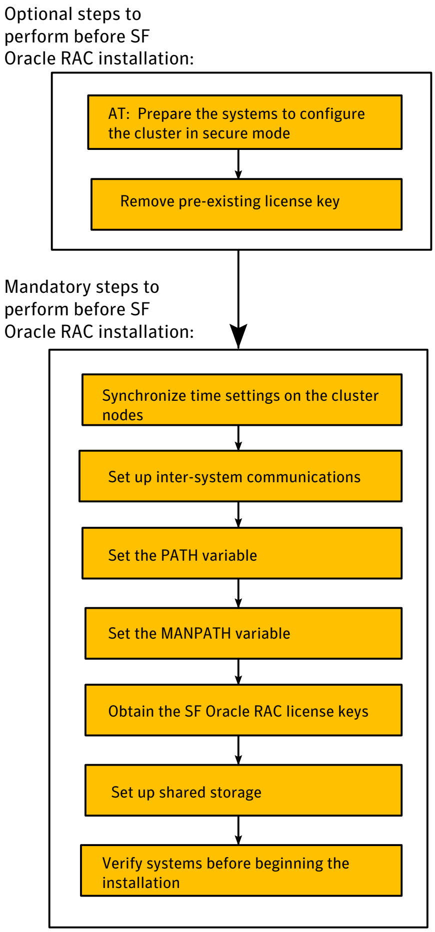
Preparing to install and configure SF Oracle RAC

This chapter includes the following topics:

About preparing to install and configure SF Oracle RAC

Figure 3-1 illustrates an overview of the mandatory and optional pre-installation steps for SF Oracle RAC. The optional tasks are performed only for optional components or features that you plan to use.

Figure 3-1 SF Oracle RAC pre-installation tasks



Preparing to configure the clusters in secure mode

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

If you want to enable AT in a cluster at a later time, refer to the *Veritas Cluster Server User's Guide* for instructions.

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

- A system in your enterprise is configured as root broker (RB).

If a root broker system does not exist, install and configure root broker on a system.
See "Installing the root broker for the security infrastructure" on page 64.

- 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 65.
- The system clocks of the root broker and authentication brokers must be in sync.

The installsfrac program provides the following configuration modes:

Automatic mode	The root broker system must allow rsh 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 rsh or ssh passwordless login. See "Setting up inter-system communication" on page 70.
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 rsh or ssh passwordless login. See "Setting up inter-system communication" on page 70.

Figure 3-2 depicts the flow of configuring SF Oracle RAC cluster in secure mode.

Figure 3-2 Workflow to configure SF Oracle RAC cluster in secure mode

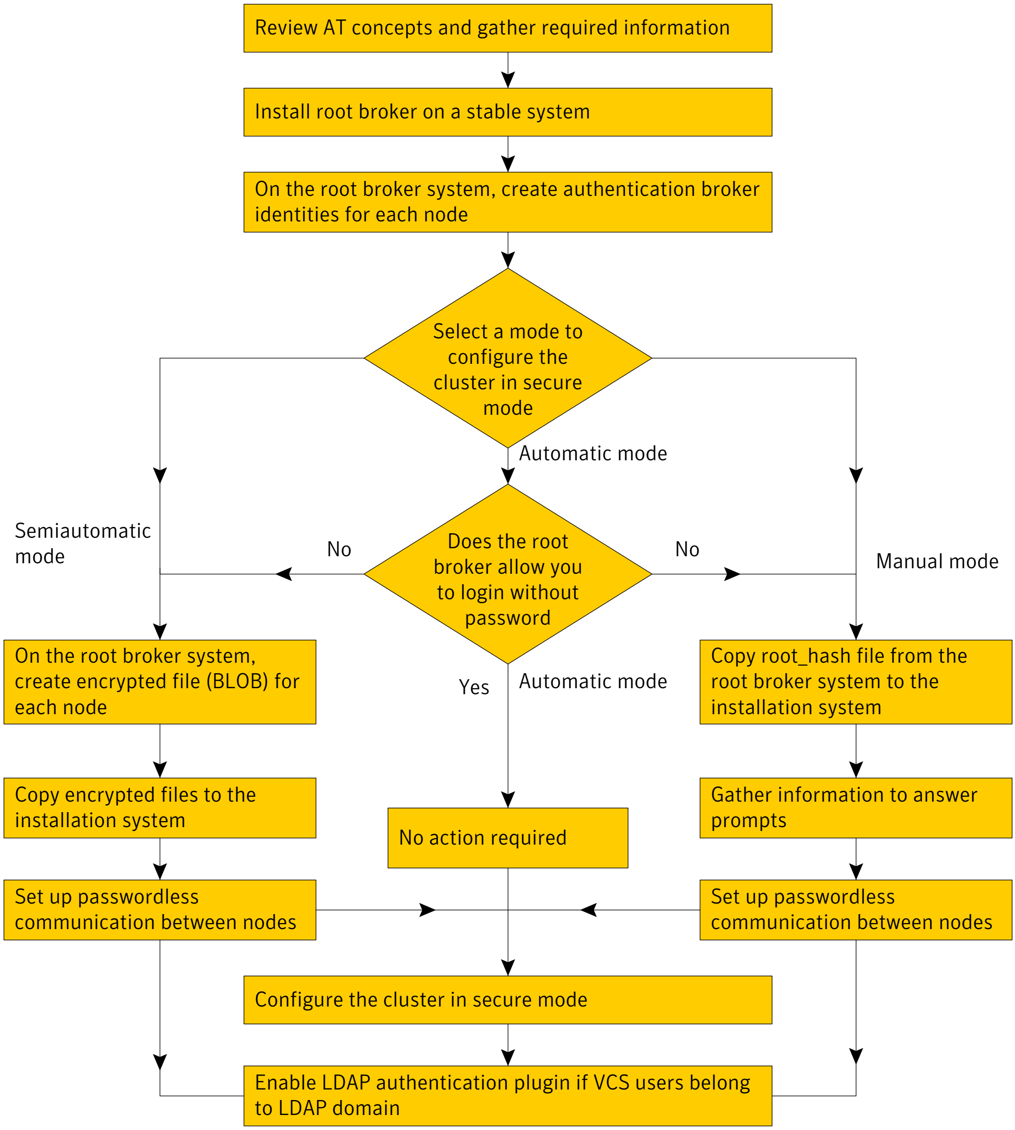


Table 3-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform.

Table 3-1 Preparatory tasks to configure a cluster in secure mode

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 64.	AT administrator
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 65. 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 66. 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
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 68.	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. 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 install the root broker on an AIX, HP-UX, Linux, or Solaris system.

See Symantec Product Authentication Service documentation for more information.

See "About Symantec Product Authentication Service (AT)" on page 25.

To install the root broker

1. Change to the directory where you can start the Veritas product installer:

   ```
   # ./installer
   ```

2. From the opening Selection Menu, choose: I for "Install/Upgrade a Product."
3. From the displayed list of products to install, choose: Symantec Product Authentication Service.
4. To install the root broker, select the mode of AT installation as root mode from the three choices that the installer presents:

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

   Enter the mode which you would like AT installed? [1-3,q] 2
   ```

5. Enter the name of the system where you want to install the root broker.

   ```
   Enter the system name on which to install AT: venus
   ```

6. Review the output as the installer does the following:
   - Checks to make sure that SF Oracle RAC supports the operating system
   - Checks if the system is already configured for security
7. Review the output as the installer checks for the installed packages on the system.

   The installer lists the packages 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 Enter **y** when the installer prompts you to configure the Symantec Product Authentication Service.

10 Press the Enter key to start the Authentication Server processes.

```
Do you want to start Symantec Product Authentication Service
processes now? [y,n,q] y
```

11 Enter an encryption key. Make sure that you enter a minimum of five characters.

You must use this encrypted key with the `-enckeyfile` option when you use the `-responsefile` option for installation.

12 Press Enter to continue and review the output as the installer displays the location of the installation log files, summary file, and the response file.

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 65.
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 65.
broker_admin_password	The value for the authentication broker password for Administrator account on the node. This password must be at least five characters.

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=vx:root@venus.symantecexample.com
root_broker=venus.symantecexample.com:2821
broker_admin_password=ab_admin_password
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 files to the installer node.

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.

Preparing to install SF Oracle RAC

Perform the following tasks before you install SF Oracle RAC:

- Setting the umask before installation
- Synchronizing time settings on cluster nodes
- Setting up inter-system communication
- Mounting the product disc
- Setting up shared storage
- Setting the environment variables
- Creating the Oracle user and groups manually
- Obtaining SF Oracle RAC license keys
- Removing pre-existing license keys
- Obtaining and installing license keys for a global cluster
- Verifying the systems before installation

Setting the umask before installation

Set the umask to provide appropriate permissions for SF Oracle RAC binaries and files.

```
# umask 0022
```

Synchronizing time settings on cluster nodes

Symantec recommends that the time settings on all cluster nodes be synchronized by running the Network Time Protocol (NTP) daemon.

Setting up inter-system communication

By default, the installer uses SSH for inter-system communication. You must grant permissions to allow the root user to invoke passwordless SSH or remsh communication between cluster nodes.

Check the following resources for information on setting up passwordless inter-system communication:

- If you encounter issues during configuration, contact the operating system support provider.
- To access online manuals and other resources, visit the OpenSSH website: http://openssh.org
- If you configured remsh for communication, on each node, place a "+ +" character in the first line of the /.rhosts file to give remote access to the system that runs the installer program.

Configuring and enabling SSH

The SSH program enables you to log into and execute commands on a remote system. SSH enables encrypted communications and an authentication process between two untrusted hosts over an insecure network. SSH is the preferred method of remote communication because it provides a greater level of security than the RSH suite of protocols.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the authorized_keys file on the target systems.

If you are installing Oracle, you must configure a DSA key and an RSA key for the Oracle user in addition to the DSA key required for the root user to install SF Oracle RAC.

Read the SSH documentation and online manual pages before enabling SSH. Contact your operating system support provider for issues regarding SSH configuration.

Visit the OpenSSH website that is located at: http://openssh.org to access online manuals and other resources.

To create the DSA key pair

1. On the source system (*galaxy*), log in as root, and navigate to the root directory.

   ```
   galaxy # cd /
   ```

2. To generate a DSA key pair on the source system, type the following command:

   ```
   galaxy # ssh-keygen -t dsa
   ```

   System output similar to the following is displayed:

   ```
   Generating public/private dsa key pair.
   Enter file in which to save the key (//.ssh/id_dsa):
   ```

3. When the program asks you to enter the passphrase, press the Enter key twice.

   ```
   Enter passphrase (empty for no passphrase):
   ```

   Do not enter a passphrase. Press Enter.

   ```
   Enter same passphrase again:
   ```

   Press Enter again.

4. Make sure the /.ssh directory is on all the target installation systems (*nebula* in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

   ```
   nebula # cd /
   nebula # mkdir /.ssh
   ```

   Change the permissions of this directory, to secure it.

   ```
   nebula # chmod go-w /.ssh
   ```

To append the public key from the source system to the authorized_keys file on the target system, using secure file transfer

1. Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (nebula in this example).

   To enable SFTP, the /opt/ssh/etc/sshd_config file must contain the following two lines:

   ```
   PermitRootLogin           yes
     Subsystem          sftp    /opt/ssh/libexec/sftp-server
   ```

2. If the lines are not there, add them and restart SSH:

   ```
   galaxy # /sbin/init.d/secsh start
   ```

3. From the source system (*galaxy*), move the public key to a temporary file on the target system (*nebula*).

   Use the secure file transfer program.

   In this example, the file name id_dsa.pub in the root directory is the name for the temporary file for the public key.

   Use the following command for secure file transfer:

   ```
   galaxy # sftp nebula
   ```

   If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

   ```
   Connecting to nebula ...
   The authenticity of host 'nebula (10.182.00.00)'
   can't be established. DSA key fingerprint is
   fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
   Are you sure you want to continue connecting (yes/no)?
   ```

4. Enter "yes".

   Output similar to the following is displayed:

   ```
   Warning: Permanently added 'nebula,10.182.00.00'
   (DSA) to the list of known hosts.
   root@nebula password:
   ```

5. Enter the root password of *nebula*.

6 At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

7 To quit the SFTP session, type the following command:

```
sftp> quit
```

8 To begin the `ssh` session on the target system (nebula in this example), type the following command on *galaxy*:

```
galaxy # ssh nebula
```

Enter the root password of nebula at the prompt:

```
password:
```

9 After you log in to nebula, enter the following command to append the id_dsa.pub file to the authorization key file:

```
nebula # cat /id_dsa.pub >> /.ssh/authorized_keys
```

10 After the id_dsa.pub public key file is copied to the target system (nebula), and added to the authorized keys file, delete it. To delete the id_dsa.pub public key file, type the following command on nebula:

```
nebula # rm /id_dsa.pub
```

11 To log out of the `ssh` session, type the following command:

```
nebula # exit
```

12 When you install from a source system that is also an installation target, also add the local system id_dsa.pub key to the local authorized_keys file. The installation can fail if the installation source system is not authenticated.

To add the local system id_dsa.pub key to the local authorized_keys file, enter the following command:

```
galaxy # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

13 Run the following commands on the source installation system. If your ssh session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and makes the key globally available for the user root:

```
galaxy # exec /usr/bin/ssh-agent $SHELL
galaxy # ssh-add
```

```
Identity added: //.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

1 On the source system (*galaxy*), type the following command:

```
galaxy # ssh -l root nebula uname -a
```

where nebula is the name of the target system.

2 The command should execute from the source system (*galaxy*) to the target system (*nebula*) without the system requesting a passphrase or password.

3 Repeat this procedure for each target system.

Enabling remsh

Remote shell functionality is enabled automatically after installing an HP-UX system.

Typically, the only requirement to enable remote installations is to modify the .rhosts file. A separate .rhosts file is in the $HOME directory of each user. You must modify this file for each user who remotely accesses the system using `remsh`. Each line of the .rhosts files must contain a fully qualified domain name or IP address for each remote system that has access to the local system. For example, if the root user must remotely access *galaxy* from *nebula*, add an entry for *nebula.companyname.com* to the /.rhosts file on *galaxy*.

```
# echo "nebula.companyname.com" >> $HOME/.rhosts
```

After you complete an installation procedure, delete the .rhosts file from each user's $HOME directory to ensure security:

```
# rm -f $HOME/.rhosts
```

See the operating system documentation and the `remsh`(1M) manual page for more information on configuring remote shell.

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 and configuration.

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 /cdrom
   # mount -F cdfs /dev/rdsk/c3t2d0 /cdrom
   ```

5. Verify that the disc is mounted:

   ```
   # mount
   ```

6. Navigate to the location of the packages:

   ```
   # cd /cdrom/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 utility is located in the directory `cluster_server/tools/vxfentsthdw` on the product disc.

  ```
  # cd /cdrom/cluster_server/tools
  # ./vxfentsthdw
  ```

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:

Bourne Shell (sh or ksh)	`# MANPATH=/usr/share/man:/opt/VRTS/man;\` `export MANPATH`
C Shell (csh)	`# setenv MANPATH /usr/share/man:\` `/opt/VRTS/man`

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:

Bourne Shell (sh or ksh)	`# 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`

C Shell (csh)	`# setenv 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`

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.

On each system, create a local group and local user for Oracle. Be sure to assign the same group ID, user ID, and home directory for the user on each system.

The following procedure creates the group 'oinstall' (Oracle Inventory group) and the user 'Oracle' (Oracle software owner user).

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 user_id -G dba -d /home/oracle oracle
```

3 Enable `rsh` and key-based authentication `ssh` for the oracle user on all nodes.

For more information on creating the Oracle user and group, see the Oracle product documentation.

Obtaining SF Oracle RAC license keys

SF Oracle RAC includes a license key certificate. The certificate specifies the product keys and the number of product licenses purchased. A single key lets you install the product on the number and type of systems for which you purchased the license. A key may enable the operation of more products than are specified on the certificate; however, you are legally limited to the number of product licenses purchased.

Note: If you have pre-existing license keys, you should remove them before proceeding.

For instructions on how to remove a pre-existing license key:

See "Removing pre-existing license keys" on page 79.

If you use VVR for replication, you can enter the VVR license during the SF Oracle RAC installation. If you do not have a VVR license yet, you can install it at a later time.

Table 3-2 lists the features that are enabled for SF Oracle RAC components.

Table 3-2 Features enabled for SF Oracle RAC components

Component	Feature
Veritas File System	■ VXCFS ■ File Change Log ■ Cross-platform Data Sharing ■ Extra-Big File Systems ■ Multi-Volume Support ■ Quality of Storage Service ■ VXCKPT
Veritas Volume Manager	■ VxVM ■ CVM_FULL ■ PGR ■ FMR_DGSJ ■ Dynamic LUN Expansion ■ Hardware assisted copy ■ Cross-platform Data Sharing ■ VVS_CONFIG ■ PGR_TRAINING ■ Site Awareness
Veritas Cluster Server	■ Mode=VCS_RAC ■ Mode=VCS_0
Veritas Volume Replicator	VVR
Veritas Storage Foundation for Oracle RAC HA/DR Option	GCO

Table 3-2 Features enabled for SF Oracle RAC components *(continued)*

Component	Feature
Veritas Mapping Services	Found_Edi_map

Removing pre-existing license keys

You need to remove license keys when an existing license is replaced or removed.

An existing license may be replaced or removed in any of the following cases:

- Upgrading SF Oracle RAC
- Adding a node to a cluster
- Removing a node from a cluster
- Adding HA/DR capability to a cluster

To remove pre-existing license keys

1. View the license key files that are currently installed on a node:

   ```
   # cd /opt/VRTS/bin
   # ./vxlicrep
   ```

   The output lists the license keys and information about the respective products.

2. Navigate to the directory that contains the license key files and list the files:

   ```
   # cd /etc/vx/licenses/lic
   # ls -a
   ```

3. Move the license key files to another location for future reference.

   For example, in the directory that contains the license key files, create a subdirectory and move the files to the subdirectory:

   ```
   # mkdir OLD
   # mv * OLD
   ```

Obtaining and installing license keys for a global cluster

If you want to set up a global cluster, make sure that you have licenses for the following products:

- Veritas Storage Foundation for Oracle RAC HA/DR

- Veritas Volume Replicator (VVR) if you use it for replication

If you use software for hardware-based replication, make sure that the required licenses from your vendor are enabled.

For licensing details:

See "Obtaining SF Oracle RAC license keys" on page 77.

See "Removing pre-existing license keys" on page 79.

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

The product installation procedure includes instructions on how to activate the key. If you encounter problems while licensing this product, visit the Symantec licensing support Web site at:

https://licensing.symantec.com

Verifying the systems before installation

Run the installsfrac program with the "-precheck" option to verify your system before the installation.

To verify the systems before installation

1. Insert the product disc with the SF Oracle RAC software into a drive that is connected to the system.
2. Install the `VRTSvlic` package:

   ```
   # swinstall -s /cdrom/depot/ VRTSvlic
   ```

3. Install the license key:

   ```
   # vxlicinst -k license_key
   ```

4. Start the preinstallation check:

   ```
   # cd /cdrom/storage_foundation_for_oracle_rac
   # ./installsfrac -precheck [-rsh] galaxy nebula
   ```

   The program proceeds in a non-interactive mode, examining the systems for licenses, packages, disk space, and system-to-system communications. The program displays the results of the check and saves the results of the check in a log file. The location of the log file is displayed at the end of the precheck process.

Chapter 4

Installing SF Oracle RAC

This chapter includes the following topics:

Installing SF Oracle RAC

You can install SF Oracle RAC using the SF Oracle RAC installer (installsfrac program) or the Veritas product installer (installer program). The installsfrac program offers a direct approach to installing or configuring SF Oracle RAC. The Veritas product installer offers a high-level approach to installing or configuring multiple Veritas products.

Note: If you obtained SF Oracle RAC from an electronic download site, you must use the installsfrac program instead of the Veritas product installer.

Before you start the installation program:

- Make sure that SSH or RSH is set up for passwordless communication. If SSH or RSH is not set up and enabled, the installation process fails.
  By default, the installer uses SSH for remote communication. If you want to use RSH, specify the -rsh option with the installation program.
- Review the SF Oracle RAC installation and configuration worksheets. Make sure that you have the values ready for the installation. You are prompted for these values during the installation process.

To install SF Oracle RAC

1. Log in as the superuser.
2. Start the installation program:

SF Oracle RAC installer	Navigate to the directory that contains the installation program: # **cd /cdrom/storage_fountation_for_oracle_rac** Run the program: # **./installsfrac [-rsh] -installonly**
Veritas product installer	Navigate to the directory that contains the installation program: # **cd /cdrom** Run the program: # **./installer [-rsh]** From the opening Selection Menu, choose: "**I**" for "Install/Upgrade 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 logs are created.

3. 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 5.0.1.

4. Enter the names of the systems on which you want to install SF Oracle RAC.

```
Enter the system names separated by spaces on which to install
SF Oracle RAC: galaxy nebula
```

   The installer checks that the local node that runs the script can communicate with remote nodes. It also checks whether or not a previous version of SF Oracle RAC is installed.

   If a previous version of SF Oracle RAC is installed, the installer provides an option to upgrade.

   See "Supported upgrade paths and task overview" on page 143.

   The installer checks whether or not the VRTSvlic package that enables licensing is present on the system

- If the VRTSvlic package is not present on the system, the installer installs it on each node after it checks the availability of sufficient disk space.
- If a previous version of the VRTSvlic package is present, the installer replaces the package with the current version.

5 Enter the license key for SF Oracle RAC as the installer prompts for each node.

```
Enter a SFRAC license key for galaxy: [?]
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX successfully registered on
galaxy
SFRAC license registered on galaxy
```

6 Enter keys for additional product features such as SF Oracle RAC HA/DR and VVR, if you want to set up a global cluster and disaster recovery environment.

You can add these keys at a later time if you are not prepared to configure these features now.

See “Installing licenses manually” on page 84.

```
Do you want to enter another license key for galaxy? [y,n,q,?]
(n) y

Enter a SFRAC license key for galaxy: [?]
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX successfully registered on
galaxy

Do you want to enter another license key for galaxy? [y,n,q,?]
(n)
```

7 Enter the license keys for other nodes.

```
SFRAC is not licensed on nebula
.
.
Do you want to enter another license key for nebula? [y,n,q,?]
(n)
SFRAC licensing completed successfully.
```

The installer performs the following tasks:

- Checks for previously installed packages.

- Checks the operating system patches installed on the system. 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.

8 Choose the SF Oracle RAC packages that you want to install. Do one of the following:
   - Enter **1** to install only the required SF Oracle RAC packages.
   - Enter **2** to install all the SF Oracle RAC packages. Option 2 is the default option.
     You must install the optional packages for any optional feature you plan to use.

9 Review the list of packages that are selected for installation on each node.

10 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.

11 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
```

Installing licenses manually

You may install additional product licenses at any time after the installation.

The following commands and their manual pages are available on the system after you complete the SF Oracle RAC installation.

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

The following procedure provides steps to install the HA/DR and VVR license keys.

To install the HA/DR and VVR licenses

1. Install the HA/DR-enabled license key:

   ```
   # vxlicinst -k xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xx (CVM/VVR)
   ```

   Verify that HA/DR is enabled:

   ```
   # vxlicrep | grep -i global
   ```

2. Install the VVR license:

   ```
   # vxlicinst -k xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xx (CVM/VVR)
   ```

   Verify that VVR is enabled:

   ```
   # vxlicrep | grep -i vvr
   ```

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

https://licensing.symantec.com

Chapter 5

Configuring SF Oracle RAC

This chapter includes the following topics:

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.

The menu options that are marked **INSTRUCTIONS ONLY** require you to:

- Follow the instructions in the order mentioned. These options do not perform any configuration tasks.
- Keep the shells on all systems open with superuser privileges.

The configuration program provides the following options:

Check systems for SFRAC	Provides the guidelines to verify private interconnects for LLT Verifies the disks that are intended for shared storage support. See "Performing basic system checks" on page 92.
Configure SFRAC	The option enables you to perform the following tasks: ■ Configure the SF Oracle RAC components—VCS, CVM, and CFS. ■ Review the instructions to configure I/O fencing. You must configure I/O fencing manually following the program instructions.
Prepare to install Oracle	Provides the guidelines for installing Oracle. Prompts for completion of the preinstallation tasks for Oracle in an SF Oracle RAC environment.
Install or relink Oracle	Launches the Oracle installer to install Oracle RAC. Links Oracle with the Veritas IPC library.

At the end of the configuration process, the installer creates a new directory with the following files:

- 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.
- A summary file that contains the output of the install scripts.

The location of the files is indicated by the installer.

Figure 5-1 illustrates the tasks that are involved in configuring SF Oracle RAC.

Figure 5-1 Workflow to configure SF Oracle RAC

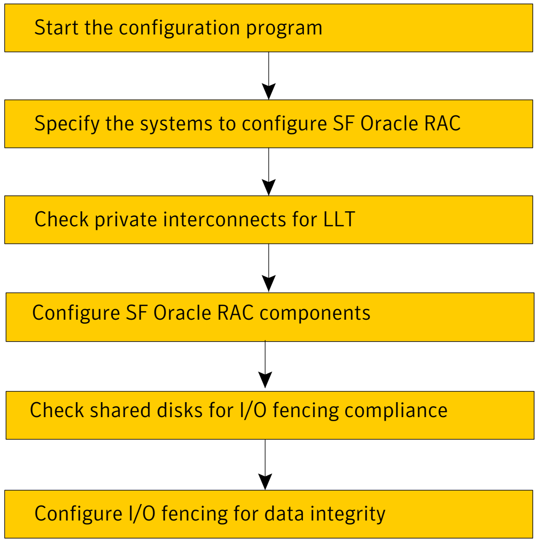


Table 5-1 lists the high-level tasks for configuring SF Oracle RAC along with references to the corresponding procedures.

Table 5-1 Tasks to configure SF Oracle RAC

Task	Reference
Invoke the configuration program	See "Invoking SF Oracle RAC configuration program" on page 90.
Check private interconnects for LLT	See "Preparing the private interconnects for LLT" on page 93.
Configure SF Oracle RAC components	See "Configuring the SF Oracle RAC components" on page 94.
Check shared disks for I/O fencing	See "About configuring SF Oracle RAC clusters for data integrity" on page 117. See "Preparing to configure I/O fencing" on page 121.
Configure I/O fencing	See "Setting up I/O fencing" on page 126.

Invoking SF Oracle RAC configuration program

Run the installsfrac program with the -configure option or use the Veritas product installer to start the SF Oracle RAC configuration. The -configure option can be used to reconfigure an SF Oracle RAC cluster. SF Oracle RAC must not be running on systems when this reconfiguration is performed.

Starting the software configuration

You can configure SF Oracle RAC using the Veritas product installer or the installsfrac program.

To configure SF Oracle RAC using the product installer

1 Confirm that you are logged in as the superuser.

2 Navigate to the folder that contains the installer program:

```
# cd /cdrom
```

3 Start the installer:

```
# ./installer
```

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

4 From the opening Selection Menu, choose **C** for "Configure an Installed Product."

5 From the displayed list of products, choose **Veritas Storage Foundation for Oracle RAC**.

To configure SF Oracle RAC using the installsfrac program

1 Confirm that you are logged in as the superuser.

2 Navigate to the folder that contains the installsfrac program: .

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

3 Start the installsfrac program with the `-configure` option:

```
# ./installsfrac [-rsh] -configure
```

By default, the installsfrac program uses SSH for remote communication. However, to use `rsh`, specify the -rsh option with the installsfrac program.

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

Specifying systems for configuration

The configuration program prompts for the name of the systems on which you want to configure SF Oracle RAC. It then performs an initial system check to verify that the communication between systems is set up appropriately.

To specify the system names for configuration

1. At the prompt, confirm that you want to proceed with the configuration.
2. Enter the names of the nodes on which you want to configure the software.

   ```
   Enter the system names separated by spaces on which to configure
   SFRAC: galaxy nebula
   ```

3. Review the output as the program checks that the local node that runs the script can communicate with remote nodes. It also checks whether SF Oracle RAC 5.0.1 is installed successfully.

   If SF Oracle RAC 5.0.1 is not installed, the program exits.

Choosing the configuration task

The configuration program provides you menu options from which you can choose the configuration task. The menu options that are marked **INSTRUCTIONS ONLY** require you to:

- Follow the instructions in the order mentioned.
- Keep the shells on all systems open with superuser privileges.

To choose the configuration task

1. After the program verifies the license keys for SF Oracle RAC, review the configuration options that the installer presents.

   See "About configuring SF Oracle RAC" on page 87.

2. Perform the following tasks to configure SF Oracle RAC cluster:

Check private interconnects for LLT.	From the main menu, select **Check systems for SFRAC > Check LLT links** for instructions to perform LLT checks. See "Performing basic system checks" on page 92.
Configure SF Oracle RAC components.	From the main menu, select **Configure SFRAC > Configure VCS, CVM, and CFS**. Review the output as the program stops various response files and processes. Answer the prompts to configure the different components and their optional features. See "Configuring the SF Oracle RAC components" on page 94.
Check shared disks for I/O fencing.	From the main menu, select **Check systems for SFRAC > Check I/O fencing disks** for instructions to check I/O fencing disks. See "Preparing to configure I/O fencing" on page 121.
Configure I/O fencing.	From the main menu, select **Configure SFRAC > Configure I/O fencing** for instructions to configure I/O fencing. See "Setting up I/O fencing" on page 126.

Performing basic system checks

Choose Check systems for SFRAC from the configuration program's menu to perform the basic system checks for SF Oracle RAC.You can follow the SF Oracle RAC configuration program instructions to check the private interconnects for LLT and to check the shared disks for I/O fencing.

Note: For DMP disk devices, verify the disks for I/O fencing compliance only after you configure SF Oracle RAC components.

To perform system checks

1. Choose one of the following options from the SF Oracle RAC configuration menu:
   - Perform all the following tasks
   - Check LLT links **INSTRUCTIONS ONLY**
   - Check I/O fencing disks **INSTRUCTIONS ONLY**

   For DMP disk devices, choose **Check LLT links** at this time. You must verify the disks for I/O fencing compliance only after you configure SF Oracle RAC components.
2. If you choose **Perform all the following tasks**, follow the guidelines as the program takes you through the other menu options individually.
3. If you choose **Check LLT links**, the program lists the prerequisites for the LLT links and prompts you to check each LLT link on all cluster nodes.

   See "Preparing the private interconnects for LLT" on page 93.
4. If you choose **Check I/O fencing disks**, follow the program guidelines to check I/O fencing disks on all nodes.

   You must check I/O fencing disks that use dynamic multi-pathing (DMP) after you configure the SF Oracle RAC components.

   See "Preparing to configure I/O fencing" on page 121.

Preparing the private interconnects for LLT

You must attach each network interface that you plan to configure for LLT to a separate physical network. You may use either crossover links or aggregate links for LLT. Do not use dissimilar network cards for the private links.

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 switches or hubs used for the interconnects must match that of the interface cards. Incorrect settings cause poor network performance or even network failure.

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

- If you have hubs or switches for LLT interconnects, Symantec recommends using the Autonegotiation media speed setting on each Ethernet card on each node.

- If you have hubs or switches for LLT interconnects and you do not use the Autonegotiation media speed setting, set the hub or the switch port to the same setting as that used on the cards on each node.
- Symantec does not recommend using dissimilar network cards for private links.

For details on setting the media speeds for specific devices, consult the device's documentation.

Configuring the SF Oracle RAC components

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

See "About preparing to install and configure SF Oracle RAC" on page 59.

At the end of the configuration, the VCS, CVM, and CFS components are configured to provide a cluster-aware environment.

You need to perform the following steps to configure the SF Oracle RAC components—VCS, CVM, and CFS:

- Configuring the SF Oracle RAC cluster
- Configuring SMTP email notification
- Configuring SNMP trap notification
- Configuring global clusters
- Setting permissions for database storage management features
- Configuring the Cluster Volume Manager
- Configuring VVR on each node
- Starting SF Oracle RAC processes

To start the configuration of SF Oracle RAC components

◆ Choose **Configure SFRAC > Configure VCS, CVM and CFS** from the configuration program's menu.

  Answer the configuration program prompts to configure the SF Oracle RAC components—VCS, CVM, and CFS.

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 basic cluster

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

3. Review the NICs available on the first system as the installer discovers and reports them.

   The private heartbeats can either use NIC or aggregated interfaces. To use aggregated interfaces for private heartbeat, enter the name of the aggregated interface. To use a NIC for private heartbeat, enter a NIC which is not part of an aggregated interface.

4. Enter the network interface card details for the private heartbeat links.

   You must choose the network interface cards or the aggregated interfaces that the installer discovers and reports. If you want to use aggregated interfaces that the installer has not discovered, then you must manually edit the /etc/llttab file before you start SF Oracle RAC when the installer prompts after product configuration.

   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 NIC on galaxy:
   [b,?] lan1
   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,?] lan2
   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)
   ```

5 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.

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.

6 Verify and confirm the information that the installer summarizes.

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 installsfrac program 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 60.

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 98.

2 Select one of the options to enable security.

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

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

`Option 1`. Automatic configuration	Enter the name of the Root Broker system when prompted. Requires a remote access to the Root Broker. Review the output as the installer verifies communication with the Root Broker system, checks vxatd process and version, and checks security domain.
`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:`
	`east.symantecexample.com`
	`Enter root broker FQDN: [b]`
	`(symantecexample.com)`
	`symantecexample.com`
	`Enter root broker domain: [b]`
	`(root@east.symantecexample.com)`
	`root@east.symantecexample.com`
	`Enter root broker port: [b] (2821)` **`2821`**
	`Enter path to the locally accessible`
	`root hash [b] (/var/tmp/`
	`installvcs-1Lcljr/root_hash)`
	`/root/root_hash`
	
	Enter the following Authentication Broker information as the installer prompts you for each node:
	
	`Enter authentication broker principal name on`
	`galaxy [b]`
	`(galaxy.symantecexample.com)`
	`galaxy.symantecexample.com`
	`Enter authentication broker password on galaxy:`
	`Enter authentication broker principal name on`
	`nebula [b]`
	`(nebula.symantecexample.com)`
	`nebula.symantecexample.com`
	`Enter authentication broker password 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 *Veritas Cluster Server User'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 password for the Admin user
   (default password='password')? [y,n,q] (n) y

   Enter New 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: [?] smith
   Enter New Password:*******

   Enter Again:*******
   Enter the privilege for user smith (A=Administrator, O=Operator,
   G=Guest): [?] 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 SF Oracle RAC 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 User'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] (y) 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 100.
3. Provide information to configure SMTP notification.

   Provide the following information:

   - Enter the SMTP server's host name.

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

   - Enter the email address of each recipient.

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

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

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

5 Verify and confirm the SMTP notification information.

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

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

Configuring SNMP trap notification

You can choose to configure SF Oracle RAC 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 User's Guide* for more information.

To configure the SNMP trap notification

1 Review the required information to configure the SNMP notification feature of SF Oracle RAC.

2 Specify whether you want to configure the SNMP notification.

```
Do you want to configure SNMP notification? [y,n,q] (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 with other set of questions for CVM and CFS.

See "Configuring global clusters" on page 101.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the SNMP trap daemon port.

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

- Enter the SNMP console system name.

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

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

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

5 Verify and confirm the SNMP notification information.

```
SNMP Port: 162
Console: 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. Note that you can also run the gcoconfig utility in each cluster later to update the VCS configuration file for global cluster.

See *Veritas Storage Foundation for Oracle RAC Administrator's Guide* for instructions to set up SF Oracle RAC global clusters.

To configure the global cluster option

1. Review the required information to configure the global cluster option.
2. Specify whether you want to configure the global cluster option.

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

Setting permissions for database storage management features

After you install SF Oracle RAC, the default settings allow only the superuser to use the database storage management features. You need to set permissions that enable the database administrators to use the database storage management features.

You may set permissions when the installer prompts you or you may defer it to the time when you set up the repository for the database storage management features.

For more information on setting up the repository, see the *Veritas Storage Foundation for Oracle RAC Administrator's Guide*.

To set permissions for database storage management features

1 If you want to add single user access, enter the name of the DBA user.

```
Do you want to add single user access on galaxy [y,n,q,?]  (y)
Enter login account name for DBA user: oracle
```

2 If you want to add group access, enter the group name for the DBA users.

```
Do you want to add group access on galaxy [y,n,q,?] (y)
Enter group name for DBA users: oinstall
```

Configuring the Cluster Volume Manager

The Cluster Volume Manager configuration includes the following tasks:

- Setting up the naming scheme
- Setting up the default disk group

Setting up the naming scheme

The disks used in SF Oracle RAC are controlled by CVM. By default, CVM follows native operating system naming convention while naming the devices. In an SF Oracle RAC cluster, CVM may name the same device with different native names on different nodes.

For ease of administration, Symantec recommends the following steps:

- Use enclosure-based naming scheme wherein the same enclosure-based name is given for a device by CVM on all nodes in the cluster. Dynamic multi-pathing (DMP) is a prerequisite for enclosure-based naming schemes.
- Irrespective of the chosen naming scheme, keep the same naming scheme on all nodes in the cluster.

Note: If the disk path is too long, the installer sets up the enclosure-based naming scheme even though you enter **n**.

Refer to the Veritas Volume Manager documentation for more information on enclosure-based naming scheme.

To set up the naming scheme

1. Enter **y** to set up the enclosure-based naming scheme.

```
Do you want to set up the enclosure-based naming scheme?
[y,n,q,?] (n) y
```

2. Enter **y** to use the new naming scheme for all eligible systems.

```
Do you want to use the enclosure-based naming scheme for all of
the eligible systems? [y,n,q,?] (y) y
```

Setting up the default disk group

Most of the Veritas Volume Manager (VxVM) commands require a disk group to be specified. The installer enables you to register the name of a default VxVM disk group on each eligible node. The default disk group can also be created or modified later using the `vxdctl defaultdg` command.

To set up a default disk group

1. Enter **y** to to set up a default disk group for each system.

```
Do you want to set up a system wide default disk group?
[y,n,q,?] (y) y

Which disk group? [<group>,list,q,?] default_dg
```

2. Confirm the configuration information.
3. If you registered a default disk group, review the setup output.

```
Volume Manager default disk group setup and daemon startup
Setting default diskgroup to default_dg on galaxy ......... Done
Starting vxrelocd on galaxy  ...................... Started
Starting vxcached on galaxy ....................... Started
Starting vxconfigbackupd on galaxy ................ Started
```

Configuring VVR on each node

If you added a license for Veritas Volume Replicator during installation, you can now accept the default settings or modify the settings for VVR. The installer prompts you for the information on VVR ports, statistics collection and other VVR tunables on each node.

Note: The VVR configuration information is requested by the installer only if you have chosen to configure VVR at the following prompt during the SF Oracle RAC installation.

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

Setting up VVR ports

The installer identifies the default ports that are used for VVR. You can also assign different ports.

Note: The port settings must be identical for the systems that are part of the same Replicated Data Set. They must also be identical for all the systems in a cluster.

To set up VVR ports

1. Review and accept the default port values that the configuration program displays.

   ```
   Do you want to change any of the VVR ports on galaxy? [y,n,q]
   (n)
   ```

2. If you want to change any of the VVR ports on the system, enter `y`.

   ```
   Do you want to change any of the VVR ports on galaxy?  [y,n,q]
   (n) y
   ```

3. Follow the instructions to change the port values.

Tuning the VVR statistics collection

The VVR administrative daemon `vradmind` collects and maintains various statistics, which are helpful in solving VVR performance issues.

You can tune the collection using the following tunables:

Frequency	The frequency in seconds for gathering the statistics default = 10 seconds
Number of days	The number of days for which the collected statistics should be preserved, after which the earlier statistics are automatically deleted. default = 3 days

To tune the VVR statistics collection

1. Enter `y` at the prompt to change the default setting.
2. Enter the values when the installer prompts.

Configuring VVR tunables

As an advanced user, you can modify the VVR tunable parameters.

Refer to Veritas Volume Replicator documentation for more information.

To configure VVR tunables

1. Enter `y` to view or modify the VVR tunables.
2. Review the output to check whether the configuration is successful.

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.

Starting SF Oracle RAC processes

The installer starts SF Oracle RAC, SF Oracle RAC processes, and configures the agents that you selected during the configuration phase.

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

See "Configuring the basic cluster" on page 95.

To start SF Oracle RAC processes

1. Confirm that you want to start the SF Oracle RAC processes.

   ```
   Do you want to start Veritas Storage Foundation for Oracle RAC
   processes now? [y,n,q] (y)
   ```

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

   See "About setting up I/O fencing" on page 118.

3. Review the output as the program starts the VxVM daemons and configures the SF Oracle RAC agents.

4. Review the output as the configuration program sets the default disk group on each node. You must have a specified a default disk group for VxVM during the configuration,

5. Review the output at the end of the configuration and note the location of the summary file, response file, and log file for future reference.

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.

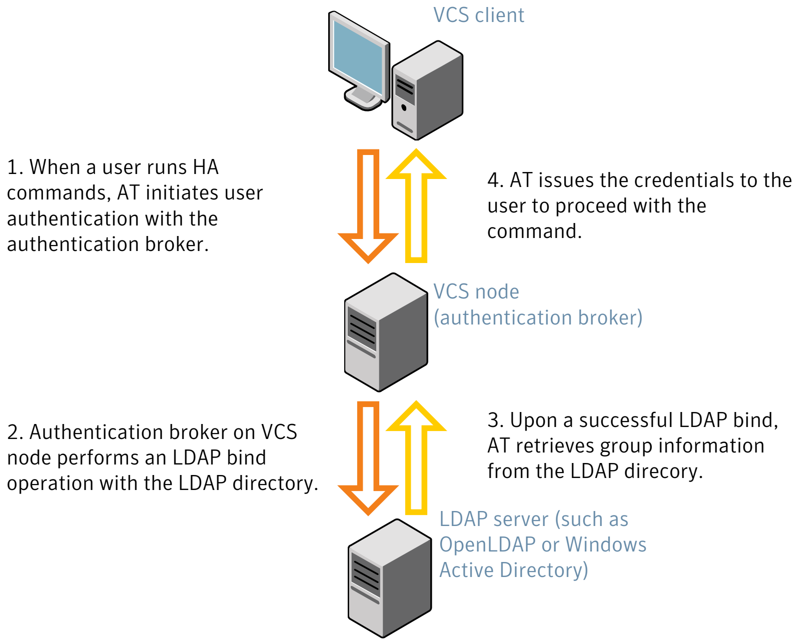
See "Enabling LDAP authentication for clusters that run in secure mode" on page 109.

If you have not already added VCS users during installation, you can add the users later.

See the *Veritas Cluster Server User's Guide* for instructions to add VCS users.

Figure 5-2 depicts the SF Oracle RAC cluster communication with the LDAP servers when clusters run in secure mode.

Figure 5-2 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 4.3.40 or later.

  ```
  # /opt/VRTSat/bin/vssat showversion
  vssat version: 4.3.40.0
  ```

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.

Chapter 6

Configuring I/O fencing for SF Oracle RAC

This chapter includes the following topics:

About configuring SF Oracle RAC clusters for data integrity

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

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

- Broken set of private networks
  If a system in a two-node cluster fails, the system stops sending heartbeats over the private interconnects. The remaining node then takes corrective action. The failure of the private interconnects, instead of the actual nodes, presents identical symptoms and causes each node to determine its peer has departed. This situation typically results in data corruption because both nodes try to take control of data storage in an uncoordinated manner
- System that appears to have a system-hang

If a system is so busy that it appears to stop responding, the other nodes could declare it as dead. This declaration may also occur for the nodes that use the hardware that supports a "break" and "resume" function. When a node drops to PROM level with a break and subsequently resumes operations, the other nodes may declare the system dead. They can declare it dead even if the system later returns and begins write operations.

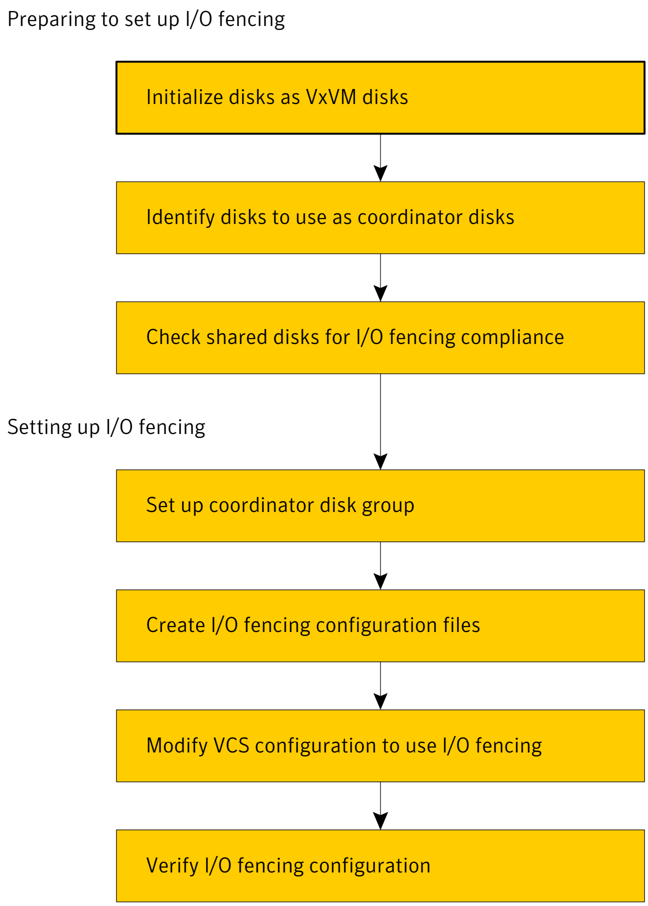
I/O fencing is a feature that prevents data corruption in the event of a communication breakdown in a cluster. SF Oracle RAC uses I/O fencing to remove the risk that is associated with split brain. I/O fencing allows write access for members of the active cluster. It blocks access to storage from non-members so that even a node that is alive is unable to cause damage.

After you install and configure SF Oracle RAC, you must configure I/O fencing in SF Oracle RAC to ensure data integrity.

About setting up I/O fencing

Figure 6-1 illustrates the tasks involved to configure I/O fencing.

Figure 6-1 Workflow to configure I/O fencing



See "Preparing to configure I/O fencing" on page 121.

See "Setting up I/O fencing" on page 126.

I/O fencing requires the coordinator disks be configured in a disk group. The coordinator disks must be accessible to each node in the cluster. These disks enable the vxfen driver to resolve potential split-brain conditions and prevent data corruption.

Review the following requirements for coordinator disks:

- You must have three coordinator disks.
  The coordinator disks can be DMP devices or iSCSI devices.
  You must use DMP disk policy for iSCSI-based coordinator disks.

For the latest information on supported hardware visit the following URL:
http://entsupport.symantec.com/docs/283161

- 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.

The I/O fencing configuration files include:

/etc/vxfendg	You must create this file to include the coordinator disk group information.
/etc/vxfenmode	You must set the I/O fencing mode to SCSI-3. You must configure the vxfen module to use DMP devices or iSCSI devices, and set the SCSI-3 disk policy as dmp.

/etc/vxfentab	When you run the vxfen startup file to start I/O fencing, the script creates this /etc/vxfentab file on each node with a list of all paths to each coordinator disk. The startup script uses the contents of the /etc/vxfendg and /etc/vxfenmode files.
	
	Thus any time a system is rebooted, the fencing driver reinitializes the vxfentab file with the current list of all paths to the coordinator disks.
	
	Note: The /etc/vxfentab file is a generated file; do not modify this file.
	
	An example of the /etc/vxfentab file on one node resembles as follows:
	
	`/dev/vx/rdmp/c1t1d0`
	`/dev/vx/rdmp/c2t1d0`
	`/dev/vx/rdmp/c3t1d0`

In some cases you must remove disks from or add disks to an existing coordinator disk group.

Warning: If you remove disks from an existing coordinator disk group, then be sure to remove the registration and reservation keys from these disks before you add the disks to another disk group.

About setting up shared storage for I/O fencing

You need to set up shared storage so that it is visible to the SCSI layer from all the nodes in the cluster. The shared storage that you add for use with SF Oracle RAC software must support SCSI-3 persistent reservations, a functionality that enables the use of I/O fencing.

Make sure that your system has at least SCSI-3 enabled disks set up and ready.

See "Checking shared disks for I/O fencing" on page 123.

Preparing to configure I/O fencing

Perform the following preparatory tasks to configure I/O fencing:

Initialize disks as VxVM disks	See "Initializing disks as VxVM disks" on page 121.
Identify disks to use as coordinator disks	See "Identifying disks to use as coordinator disks" on page 123.
Check shared disks for I/O fencing The tasks involved in checking the shared disks for I/O fencing are as follows: ■ Verify that the nodes have access to the same disk ■ Test the disks using the vxfentsthdw utility	See "Checking shared disks for I/O fencing" on page 123.

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

1 Make the new disks recognizable. 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 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.

3 Verify that the ASL for the disk array is installed on each of the nodes. Run the following command on each node and examine the output to verify the installation of ASL.

   The following output is a sample:

```
# vxddladm listsupport all
LIBNAME                      VID
==============================================================

libvxautoraid.sl             HP
libvxCLARiiON.sl             DGC
libvxemc.sl                  EMC
```

4 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.

5 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 Managers 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

After you add and initialize disks, 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 list
   ```

2. Pick three SCSI-3 PR compliant shared disks as coordinator disks.

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 `rsh` communication. To confirm whether a disk (or LUN) supports SCSI-3 persistent reservations, two nodes must simultaneously have access to the same disks. Because a shared disk is likely to have a different name on each node, check the serial number to verify the identity of the disk. Use the `vxfenadm` command with the `-i` option. This command option verifies that the same serial number for the LUN is returned on all paths to the LUN.

Make sure to test the disks that serve as coordinator disks.

The vxfentsthdw utility has additional options suitable for testing many disks. Review the options for testing the disk groups (`-g`) and the disks that are listed in a file (`-f`). You can also test disks without destroying data using the `-r` option.

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

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

- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 124.

- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 124.

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.

   ```
   /sbin/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:

   ```
   # /sbin/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:

   ```
   # /sbin/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
```

To test the disks using vxfentsthdw utility

1. Make sure system-to-system communication functions properly.

   See "Setting up inter-system communication" on page 70.

   After you complete the testing process, remove permissions for communication and restore public network connections.

   See "Removing permissions for communication" on page 131.

2. From one node, start the utility.

   Do one of the following:

   - If you use `ssh` for communication:

     ```
     # /opt/VRTSvcs/vxfen/bin/vxfentsthdw
     ```

   - If you use `rsh` for communication:

     ```
     # /opt/VRTSvcs/vxfen/bin/vxfentsthdw -n
     ```

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

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

   ```
   ******** WARNING!!!!!!!! ********
   THIS UTILITY WILL DESTROY THE DATA ON THE DISK!!

   Do you still want to continue : [y/n] (default: n) y
   Enter the first node of the cluster: galaxy
   Enter the second node of the cluster: nebula
   ```

4. Enter the names of the disks that you want to check. Each node may know the same disk by a different name:

```
Enter the disk name to be checked for SCSI-3 PGR on node galaxy in
the format: /dev/vx/rdmp/cxtxdx
/dev/vx/rdmp/c2t13d0
Enter the disk name to be checked for SCSI-3 PGR on node nebula in
the format: /dev/vx/rdmp/cxtxdx
Make sure it's the same disk as seen by nodes galaxy and nebula
/dev/vx/rdmp/c2t13d0
```

   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:

```
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.

Setting up I/O fencing

Make sure you completed the preparatory tasks before you set up I/O fencing.

Tasks that are involved in setting up I/O fencing include:

Table 6-1 Tasks to set up I/O fencing

Action	Description
Setting up coordinator disk groups	See "Setting up coordinator disk groups" on page 127.
Creating I/O fencing configuration files	See "Creating I/O fencing configuration files" on page 128.
Modifying SF Oracle RAC configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 128.
Start SF Oracle RAC on all nodes	See "Starting SF Oracle RAC on all nodes" on page 129.

Table 6-1 Tasks to set up I/O fencing *(continued)*

Action	Description
Verifying I/O fencing configuration	See "Verifying I/O fencing configuration" on page 131.

Setting up coordinator disk groups

From one node, create a disk group named vxfencoorddg. This group must contain three disks or LUNs. If you use VxVM 5.0 or later, 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. If you use VxVM 5.0 or later, 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
```

Modifying VCS configuration to use I/O fencing

After you add coordinator disks 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
)
```

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 138.

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 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

◆ On all nodes, type:

```
# hagrp -state cvm
```

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

◆ On one of the nodes, type:

```
# vxfenadm -d

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)
```

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 `rsh`, remove the temporary `rsh` access permissions that you set for the nodes and restore the connections to the public network.

If the nodes use `ssh` for secure communications, and you temporarily removed the connections to the public network, restore the connections.

Chapter 7

Verifying cluster installation and configuration

This chapter includes the following topics:

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 369.

See "Sample main.cf file after SF Oracle RAC installation" on page 371.

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.

The information that these LLT and GAB configuration files contain is as follows:

- The /etc/llthosts file
  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 is identical on each node in the cluster.
  For example, the file /etc/llthosts contains the entries that resemble:

  ```
  0       galaxy
  1       nebula
  ```

- The /etc/llttab file
  The file `llttab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the private network links that correspond to the specific system.
  For example, the file /etc/llttab contains the entries that resemble:

  ```
  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.
  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.

- The /etc/gabtab file
  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. By default, *N* is the number of nodes in the cluster.

Note: The use of the `-c -x` option for `/sbin/gabconfig` is not recommended. The Gigabit Ethernet controller does not support the use of `-c -x`.

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 135.
4. Verify GAB operation.

   See "Verifying GAB" on page 138.
5. Verify the cluster operation.

   See "Verifying the cluster" on page 139.

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.
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 | more
   ```

   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:34
   1 nebula        OPEN
                             lan1 UP     08:00:20:8F:D1:F2
                             lan2 DOWN
   2              CONNWAIT
   ```

```
                        lan1 DOWN
                        lan2 DOWN
3         CONNWAIT
                        lan1 DOWN
                        lan2 DOWN
.
.
.

31        CONNWAIT
                        lan1 DOWN
                        /dev/lan:2 DOWN
```

Note that the output lists 32 nodes. The command reports the status on the two nodes in the cluster, galaxy and nebula, along with the details for the non-existent nodes.

For each correctly configured node, the information must show the following:

- A state of OPEN
- A status for each link of UP
- An address for each link

However, the output in the example shows different details for the node nebula. The private network connection is possibly broken or the information in the /etc/llttab file may be incorrect.

6 To obtain information about the ports open for LLT, type `lltstat -p` on any node.

For example, type `lltstat -p` on the node galaxy in a two-node cluster:

```
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 ... 28 29 30 31
        connects:    0 1
  7     gab          0x7
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 28 29 30 31
        connects:    0 1
  31    gab          0x1F
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 28 29 30 31
        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 7-1 lists the different ports that the software configures for different functions.

Table 7-1 GAB port description

Port	Function
a	GAB
b	I/O fencing
d	Oracle Disk Manager (ODM)
f	Cluster File System (CFS)

Table 7-1 GAB port description *(continued)*

Port	Function
h	Veritas Cluster Server (VCS: High Availability Daemon)
o	VCSMM driver
v	Cluster Volume Manager (CVM)
w	vxconfigd (module for CVM)

For more information on GAB, refer to the *Veritas Cluster Server User'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 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 User'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
```

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 User'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     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         Fri May 22 17:22:48 2009

galaxy     ConnectorState        Down

galaxy     CurrentLimits

galaxy     DiskHbStatus

galaxy     DynamicLoad           0

galaxy     EngineRestarted       0

galaxy     EngineVersion         5.0.31.0

galaxy     Frozen                0

galaxy     GUIIPAddr

galaxy     LLTNodeId             0
```

```
#System    Attribute             Value
galaxy     LicenseType           DEMO
galaxy     Limits
galaxy     LinkHbStatus          lan1 UP lan2 UP
galaxy     LoadTimeCounter       0
galaxy     LoadTimeThreshold     600
galaxy     LoadWarningLevel      80
galaxy     NoAutoDisable         0
galaxy     NodeId                0
galaxy     OnGrpCnt              1
galaxy     ShutdownTimeout       120
galaxy     SourceFile            ./main.cf
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
```

Chapter 8

Upgrading to SF Oracle RAC 5.0.1

This chapter includes the following topics:

Supported upgrade paths and task overview

You can upgrade to SF Oracle RAC 5.0.1 from the following versions:

- SF Oracle RAC 4.1, 4.1 MP1, 4.1 MP2
- SF Oracle RAC 5.0, 5.0 MP1, 5.0 MP2

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 5.0.1. 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 software must be at the same version across all nodes in an SF Oracle RAC cluster, in this case 5.0.1. All components and point products of SF Oracle RAC must be from the same version of the release, in this case 5.0.1.

Note: Symantec strongly recommends upgrading all SF Oracle RAC component products to the same version at the same time. In a CVM/CFS environment, dependencies between SF Oracle RAC component products will not be met if you do not upgrade all components to the same version.

Figure 8-1 illustrates the overview of tasks required to upgrade SF Oracle RAC.

Figure 8-1 SF Oracle RAC upgrade task overview

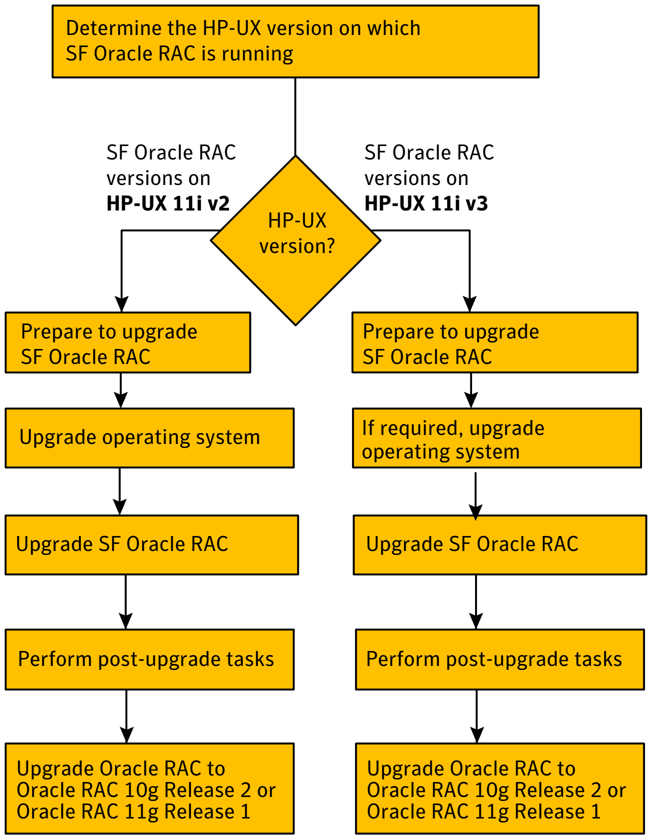


Table 8-1 lists the supported upgrade paths.

Table 8-1 Supported upgrade paths

From SF Oracle RAC versions	To SF Oracle RAC version	Task summary
SF Oracle RAC versions on HP-UX 11iv2: 4.1, 4.1 MP1, 4.1 MP1PP1, 4.1 MP2, 5.0, 5.0 MP1, 5.0 MP1PP1, 5.0 MP2	SF Oracle RAC 5.0.1	See "Task summary for upgrading from SF Oracle RAC versions on HP-UX 11i v2" on page 145.
SF Oracle RAC versions on HP-UX 11iv3: 5.0	SF Oracle RAC 5.0.1	See "Task summary for upgrading from SF Oracle RAC versions on HP-UX 11i v3" on page 145.

Task summary for upgrading from SF Oracle RAC versions on HP-UX 11i v2

The following procedure provides a summary of the tasks for upgrading from SF Oracle RAC versions on HP-UX 11i v2.

To upgrade from SF Oracle RAC versions on HP-UX 11i v2

1. Prepare to upgrade to SF Oracle RAC 5.0.1:

   See "Preparing to upgrade to SF Oracle RAC 5.0.1" on page 146.

2. Upgrade operating system to HP-UX 11i v3 March 2009 Fusion.

   See "Upgrading the operating system" on page 150.

3. Upgrade to SF Oracle RAC 5.0.1:

   See "Upgrading SF Oracle RAC using the installsfrac installer" on page 151.

4. Perform post-upgrade tasks:

   See "Performing post-upgrade tasks" on page 156.

5. If on unsupported version, upgrade Oracle RAC to Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1.

   For instructions, see the chapter "Upgrading Oracle RAC and migrating the database" in this document.

Task summary for upgrading from SF Oracle RAC versions on HP-UX 11i v3

The following procedure provides a summary of the tasks for upgrading from SF Oracle RAC versions on HP-UX 11i v3.

To upgrade from SF Oracle RAC versions on HP-UX 11i v3

1. Prepare to upgrade to SF Oracle RAC 5.0.1:

   See "Preparing to upgrade to SF Oracle RAC 5.0.1" on page 146.

2. If you are not on a supported version of the operating system, upgrade it to HP-UX 11i v3 March 2009 OEUR or later.

   See "Upgrading the operating system" on page 150.

3. Upgrade to SF Oracle RAC 5.0.1:

   See "Upgrading SF Oracle RAC using the installsfrac installer" on page 151.

4. Perform post-upgrade tasks:

   See "Performing post-upgrade tasks" on page 156.

5. If necessary, upgrade Oracle RAC to Oracle RAC 11g Release 1.

   For instructions, see the chapter "Upgrading Oracle RAC and migrating the database" in this document.

Preparing to upgrade to SF Oracle RAC 5.0.1

Note: Do not follow the instructions in this section if you are performing a rolling upgrade of SF Oracle RAC.

If you are preparing to upgrade from SF Oracle RAC 4.1x, 5.0x on HP-UX 11i v2 to SF Oracle RAC 5.0.1:

See "To prepare for upgrade from SF Oracle RAC versions on HP-UX 11i v2:" on page 147.

If you are preparing to upgrade from SF Oracle RAC 5.0 or 5.0 RP1 on HP-UX 11i v3 to SF Oracle RAC 5.0.1:

See "To prepare for upgrade from SF Oracle RAC versions on HP-UX 11i v3:" on page 149.

To prepare for upgrade from SF Oracle RAC versions on HP-UX 11i v2:

1. Log in as superuser to one of the nodes, *galaxy* for example, in the cluster.
2. Create a backup of the existing cluster configuration. Back up the main.cf, types.cf, and OracleTypes.cf on all cluster nodes:

   ```
   # 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
   ```

3. For Oracle RAC 9i, log in as Oracle user on each node and stop `gsd`:

   ```
   $ $ORACLE_HOME/bin/gsdctl stop
   ```

4. For Oracle RAC 10g and Oracle RAC 11g, stop all Oracle RAC resources.
   - If the database instances are under CRS control, then run the following on one node:

     ```
     $ srvctl stop database -d database_name
     ```

5. If the database instances are under VCS control, take the corresponding VCS service groups offline. As superuser, enter:

   ```
   # hagrp -offline group_name -any
   ```

6. For Oracle RAC 10g or Oracle RAC 11g, stop CRS on each node in the cluster.
   - If CRS is controlled by VCS, log in as superuser on any system in the cluster and enter:

     ```
     # hares -offline cssd-resource -sys galaxy
     # hares -offline cssd-resource -sys nebula
     ```

   - If CRS is not controlled by VCS, log in as superuser on each system in the cluster and enter:

     ```
     # /sbin/init.d/init.crs stop
     ```

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 /etc/fstab file.

8 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.

9 Take offline all VCS groups that contain CFSMount and CVMVolDg.

```
# hagrp -offline group -sys galaxy
```

```
# hagrp -offline group -sys nebula
```

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

```
# umount /mount_point
```

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

```
# fuser -cu mount-point
```

12 Stop all VCS service groups.

To view the current state of the service groups:

```
# hagrp -state
```

To stop each group:

```
# hagrp -offline servicegroup -sys node_name
```

13 Make sure that no disk groups are imported:

```
# vxdg list
NAME          STATE           ID
#
^^^ NOTE: no diskgroups imported
```

14 Freeze the VCS service groups. Run the following commands:

```
# haconf -makerw
# hagrp -freeze servicegroup -persistent
# haconf -dump -makero
```

15 Stop VCS on all nodes:

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

16 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.

17 On each node, edit the /etc/vxfenmode file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

Note that to upgrade from SF 4.1 for Oracle RAC on HP-UX 11iv2, create /etc/vxfenmode file and populate it as above.

18 On each node, change LLT_START=0 in the file /etc/rc.config.d/lltconf.

19 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
```

To prepare for upgrade from SF Oracle RAC versions on HP-UX 11i v3:

1 Log in as superuser to one of the nodes, *galaxy* for example, in the cluster.

2 Create a backup of the existing cluster configuration. Back up the main.cf, types.cf, and OracleTypes.cf on all cluster nodes:

```
# 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
```

3 Take offline all service groups configured under VCS.

```
# hagrp -offline group_name -sys node_name
```

4 Verify that the service groups are offline. The following example shows the cvm and Oracle service groups offline.

```
# /opt/VRTSvcs/bin/hagrp -state
#Group Attribute System Value
Oracle1 State galaxy |OFFLINE|
Oracle1 State nebula |OFFLINE|
cvm State galaxy |OFFLINE|
cvm State nebula |OFFLINE|
```

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 /etc/fstab file.

6 Stop all applications using the CFS mounts not under VCS control.

- Ensure that no processes are using the CFS mount point.

  ```
  # fuser -c mount_point
  ```

- Stop any processes using a CFS mount point.

  ```
  # fuser -ck mount_point
  ```

7 Unmount any CFS file systems that are not under VCS control on all nodes.

- Determine the file systems to unmount by checking the /etc/mnttab file. For example:

  ```
  # cat /etc/mnttab | grep vxfs | grep cluster
  ```

  The output shows each line of the /etc/mnttab file that contains an entry for a VxFS file system mounted in the cluster mode.

- By specifying the mount point for the file system, unmount each file system listed in the output:

  ```
  # umount mount_point
  ```

Upgrading the operating system

If you are on an unsupported version of the operating system, you need to upgrade it to HP-UX 11i v3 March 2009 OEUR release or later.

Note: If you are upgrading from SF Oracle RAC 5.0 or 5.0 RP1 on HP-UX 11i v3, you need to stop VCS before you upgrade the operating system. To stop VCS on all nodes, run the following command as the superuser:

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

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 March 2009 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 opearting system depots:

```
# 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 installsfrac installer

You may use the product installer or the `installsfrac` program to upgrade SF Oracle RAC.

To upgrade to SF Oracle RAC 5.0.1

1 Mount the software disc.

See "Mounting the product disc" on page 75.

2 On the node where the disk is mounted, browse to the directory containing the installer program.

3 Start the product upgrade.

```
# ./installsfrac [-rsh] galaxy nebula
```

After viewing a copyright notice, review the report after the program examines the configuration files and discovers the existing cluster configuration.

4 To upgrade to SF Oracle RAC 5.0.1, press `Enter`.

```
Do you want to upgrade to version 5.0.1 on these systems using the
current configuration? [y,n,q,?] (y) y
```

5 Confirm that you want to continue with the installation at the installer prompt. Note that the installation program will replace any previous version of VxVM that was bundled with HP-UX with VxVM 5.0.1.

6 Review the output as the program performs the following:

- Checks system licensing and installs the licensing package
- Checks the installed packages on each node
- Lists the SF Oracle RAC packages that the program will install or upgrade

7 Confirm that you want to upgrade SF Oracle RAC. Note that the installer will stop all the currently running SF Oracle RAC processes.

8 Review the output as the installer stops the CVM and CFS agents, and updates the gabtab files on each node in the cluster.

9 Confirm that you are ready to upgrade SF Oracle RAC. Note that the installation program makes configuration updates and stops the cluster to upgrade the SF Oracle RAC packages.

10 Review the output as the program does the following:

- Backs up the configuration files
- Freezes all the VCS service groups
- Updates the types.cf files

Refer to the *Veritas Cluster Server Installation Guide* for more information on the types.cf updates.

- Updates gabtab files on each node

11 Review the output as the program stops SF Oracle RAC processes and shuts down SF Oracle RAC on all nodes in the cluster.

12 Review the output as the program uninstalls the packages from the previous version of SF Oracle RAC.

13 Review the output as the program installs SF Oracle RAC 5.0.1 packages.

14 Note the location of the summary and log files for future reference.

15 Uncomment the VxFS mount point entries in the /etc/fstab file.

16 Restart the nodes:

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

17 If you upgraded from SF Oracle RAC versions on HP-UX 11i v2 to SF Oracle RAC 5.0.1, proceed to configure SF Oracle RAC:

See "Configuring SF Oracle RAC after upgrading to version 5.0.1" on page 154.

If you upgraded from SF Oracle RAC versions on HP-UX 11i v3 to SF Oracle RAC 5.0.1, proceed to perform the following post-upgrade tasks:

- Verify the output of the gabconfig -a command to ensure that SF Oracle RAC is configured correctly.
  Run the following command on all nodes. For example:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen ada401 membership 0123
Port b gen ada40d membership 0123
Port d gen ada409 membership 0123
Port h gen ada40f membership 0123
Port o gen ada406 membership 0123
```

- Mount any VxFS file systems that are not under VCS control.
- Unfreeze the VCS service groups. Run the following commands:

```
# haconf -makerw
# hagrp -unfreeze servicegroup -persistent
# haconf -dump -makero
```

- From one of the nodes, stop the VCS engine:

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

- Add the include statements for `MultiPrivNIC.cf` and `OracleASMTypes.cf` in the main.cf file.

  ```
  include "types.cf"
  include "CFSTypes.cf"
  include "CVMTypes.cf"
  include "PrivNIC.cf"
  include "OracleTypes.cf"
  include "MultiPrivNIC.cf"
  include "OracleASMTypes.cf"
  ```

- Start the VCS engine on each system:

  ```
  # hastart
  ```

- If Oracle Clusterware is not controlled by VCS, log in as the root user on each system in the cluster and start Oracle Clusterware:

  ```
  # /sbin/init.d/init.crs start
  ```

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

  ```
  $ srvctl start database -d database_name
  ```

- Verify all VCS groups are now online and the database instances are up and running.
- Import any VxVM disk groups that are not under VCS control.
- Complete other post-upgrade tasks:
  See "Performing post-upgrade tasks" on page 156.

Configuring SF Oracle RAC after upgrading to version 5.0.1

Perform this step only if you upgraded from an SF Oracle RAC version on HP-UX 11i v2.

You may choose to use the previous configuration of SF Oracle RAC or reconfigure SF Oracle RAC. If you want to take advantage of the new features in this release, reconfigure SF Oracle RAC using the configuration program.

To configure SF Oracle RAC after upgrading to version 5.0.1

1. Start the configuration program.
2. Enter the names of the nodes on which you want to configure the software.

   Review the output as the program checks that the local node running the script can communicate with remote nodes and checks whether SF Oracle RAC 5.0.1 is installed successfully.
3. Enter **y** to confirm that you want to use the previous configuration of SF Oracle RAC.

   Review the output as the program checks the system licensing.
4. Select **Configure SFRAC > Configure VCS, CVM, and CFS** and confirm at the installer prompt that you want to continue with the configuration.

   Review the output as the program stops various SF Oracle RAC processes on each node.
5. If you want the database administrators (DBAs) to access SF Oracle RAC components, then you must set the required permissions.

   The default settings permit only the superuser to access the /opt/VRTSdbed folder.

   See "Setting permissions for database storage management features" on page 102.
6. Review the output as the installer performs the following tasks:
   - Starts the SF Oracle RAC processes
   - Starts the VxVM daemons,
   - Unfreezes the VCS service groups and brings the service groups online

   Note the location of the upgrade log files and summary files.
7. Enable fencing.

   ```
   # hastop -all
   # cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
   # /sbin/init.d/vxfen stop
   # /sbin/init.d/vxfen start
   ```
8. Set the clusterwide attribute "UseFence" to use SCSI3. Add the following line to the /etc/VRTSvcs/conf/config/main.cf file:

   ```
   UseFence=SCSI3
   ```

9 Start the VCS engine on each system:

```
# hastart
```

10 Complete other post-upgrade tasks.

See "Performing post-upgrade tasks" on page 156.

Performing post-upgrade tasks

You need to perform the following post-upgrade tasks:

- Relinking Oracle RAC libraries with the SF Oracle RAC libraries
- Modifying the CVMVolDg resource type
- Upgrading the CVM configuration
- Upgrading the disk layout versions
- Upgrading the repository database

Relinking Oracle RAC libraries with the SF Oracle RAC libraries

You must relink the Oracle RAC libraries with the SF Oracle RAC libraries afer 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 Release 1:
  See "To relink Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1 using the installer" on page 157.
- 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 Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1:
  See "To relink the Oracle RAC libraries with SF Oracle RAC libraries manually" on page 158.

Note: You must upgrade the database to a supported version (Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1) after you complete the post-upgrade tasks.

To relink Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1 using the installer

1 On each node, shut down the Oracle service group:

```
# hagrp -offline oracle_group -sys system_name
```

2 Invoke the `installsfrac` installer:

```
# cd /opt/VRTS/install
# ./installsfrac -configure galaxy nebula
```

3 Navigate to the “Install or Relink Oracle” menu.

- Select the appropriate Oracle version:

```
Oracle 10gR2
Oracle 11g
```

- Select “Relink Oracle” from the menu:

```
1) Install Oracle Clusterware (CRS)
2) Install Oracle RDBMS server
3) Relink Oracle
b) [Go to previous menu]
```

4 Provide the following information:

```
Enter Oracle UNIX user name: [b] (oracle) oracle
Enter Oracle UNIX group name: [b] (oinstall) oinstall
Enter Oracle base directory: [b] /app/oracle
Enter absolute path of CRS home directory: [b] /app/crshome
Enter absolute path of Database Home directory: [b] /app/oracle/
orahome
```

5 Confirm your responses in the verification screen. The installer copies the SF Oracle RAC libraries to $ORACLE_HOME/lib.

```
Oracle environment information verification
Oracle Unix User: oracle
Oracle Unix Group: oinstall
Oracle Clusterware (CRS) Home: /app/crshome
Oracle Release: 10.2
Oracle Base: /app/oracle
Oracle Home: /app/oracle/orahome
Is this information correct? [y,n,q](y)
```

6. On each node, start the Oracle service group:

   ```
   # hagrp -online oracle_group -sys system_name
   ```

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 for Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1.

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:

   For Oracle RAC 9i:

   ```
   $ /opt/VRTSvcs/rac/bin/linkrac 9i
   ```

   For Oracle RAC 10g Release 1:

   ```
   $ /opt/VRTSvcs/rac/bin/linkrac 10gR1
   ```

   For Oracle RAC 10g Release 2:

   ```
   $ /opt/VRTSvcs/rac/bin/linkrac 10gR2
   ```

   For Oracle RAC 11g Release 1:

   ```
   $ /opt/VRTSvcs/rac/bin/linkrac 11gR1
   ```

   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/\
  libskgxporacleversion_ver24_64.sl
  ```

  On HP-UX (PA) for Oracle RAC 9i:

  ```
  $ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/pa20_64/\
  libskgxporacleversion_ver24_64.sl
  ```

  On HP-UX (IA) for Oracle RAC 10g Release 1:

```
$ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/hpux64/\
libskgxporacleversion_ver25_64.sl
```

On HP-UX (PA) for Oracle RAC 10g Release 1:

```
$ export IPC_LIB_PATH=/opt/VRTSvcs/rac/lib/pa20_64/\
libskgxporacleversion_ver25_64.sl
```

where *oracleversion* is 9 (for Oracle RAC 9i) or 10 (for Oracle RAC 10g)

- Repeat step 2 and step 3.

Modifying the CVMVolDg resource type

Perform this step only if you upgraded from SF Oracle RAC 5.0 on HP-UX 11i v3 and if the CVMVolDg resource type contains the CVMDGAction attribute.

To modify the CVMVolDg resource type

1. Check whether the CVMVolDg resource type contains the CVMDGAction attribute:

```
# /opt/VRTS/bin/haattr -display CVMVolDg \
| grep -w CVMDGAction
```

2. If the CVMVolDg resource type contains the CVMDGAction attribute, get the argument list for the attribute:

```
# hatype -display CVMVolDg | grep ArgList
```

3. Verify that the CVMDGaction attribute is at the end of the argument list:

```
# /opt/VRTS/bin/hatype -display CVMVolDg | grep ArgList
CVMVolDg     ArgList                 CVMDiskGroup       CVMDGAction
CVMVolume       CVMActivation
```

4 If the CVMDGAction attribute is not at the end of the argument list, move it to the end of the argument list:

```
# /opt/VRTS/bin/haconf -makerw
# /opt/VRTS/bin/hatype -modify CVMVolDg ArgList \
CVMDiskGroup CVMVolume CVMActivation CVMDGAction
```

5 Verify that the CVMDGaction attribute is now at the end of the argument list:

```
# /opt/VRTS/bin/hatype -display CVMVolDg | grep ArgList
CVMVolDg     ArgList                  CVMDiskGroup       CVMVolume
CVMActivation   CVMDGAction
```

Upgrading the CVM configuration

To take advantage of the new features in this release, you must upgrade the Veritas Cluster Volume Manager (CVM) configuration.

To upgrade the CVM configuration

1 Log in to one of the nodes in the cluster and take all the service groups offline on all nodes:

```
# hagrp -offline group_name -sys system_name
```

2 Upgrade the CVM agent configuration:

```
# vxcvmconfig upgrade
```

If this command is not run, you will see a warning in the engine log file, `/opt/VRTSvcs/log/engine_A.log`.

3 Bring the cvm group online on all the nodes:

```
# hagrp -online cvm -sys system_name
```

4 Bring the other service groups online on all the nodes:

```
# hagrp -online group_name -sys system_name
```

5 If you upgraded SF Oracle RAC from pre-5.0x versions, upgrade the disk group version to 140 by entering the following command on the master node:

```
# vxdg -T 140 upgrade disk_group_name
```

Verify the cluster protocol version:

```
# /opt/VRTS/bin/vxdctl protocolversion
```

Note: If you upgraded from 5.0 on HP-UX 11i v2 or HP-UX 11i v3, the disk group version is 140 and does not need to be upgraded.

Upgrading the disk layout versions

SFCFS 5.0.1 supports disk layouts Versions 4, 5, 6 and 7 for locally mounted file systems and disk layouts Versions 6 and 7 for cluster mounted file systems. If you have cluster mounted file systems with disk layout versions lower than 6, then after upgrading to SFCFS 5.0.1, perform the following additional steps to prepare the file system for being mounted on all nodes of the cluster:

To upgrade the disk layout versions

1 Select one of the nodes of the cluster and `mount` the file system locally on this node. For example, mount it without the `-o cluster` option. Enter,

```
# mount -F vxfs block_device_path /mnt1
```

2 Current disk layout version on a file system can be found using

```
# fstyp -v char_device_path | grep version | \
    awk '{print $2}'
```

3. On the node selected in 1, incrementally upgrade the disk layout of this file system to layout Version 6 or layout Version 7. For example, if you had a cluster mounted file system of disk layout Version 4 while running with SFCFS 3.5 on HP-UX 11i Version 1, after upgrading to SFCFS 5.0.1, you would need to upgrade the disk layout to version 6 or version 7 incrementally as follows:

   ```
   # vxupgrade -n 5 /mnt1
   # vxupgrade -n 6 /mnt1
   # vxupgrade -n 7 /mnt1
   ```

4. On the node selected in 1, after the disk layout has been successfully upgraded, unmount the file system.

   ```
   # umount /mnt1
   ```

5. This file system can be mounted on all nodes of the cluster using `cfsmount`.

Upgrading the repository database

After you have completed the SF Oracle RAC upgrade, if you plan to use the commands for Database Storage Checkpoints, Database FlashSnap, Database Dynamic Storage Tiering , or Storage Mapping, you must:

- Change permissions
- Upgrade the repository database

Note: Do not recursively change permissions, groups, or owners.

To change permissions

1. Change permissions for the following directory:

   ```
   # chmod 750 /opt/VRTSdbed
   ```

2. Reset owner and group settings to the appropriate owner and group for the database administrators on your system.

   For example, to change owner to the user oracle and the group dba, run the following command:

   ```
   # chown oracle:dba /opt/VRTSdbed
   ```

To upgrade the repository from 5.0 to 5.0.1 in a cluster environment

1. Save the repository disk group name, mount point, and other attributes.
2. Unconfigure the SFUA repository from the VCS configuration:

   ```
   # /opt/VRTSdbcom/bin/sfua_db_config -o unconfig_cluster
   ```

   This command:

   - Removes the repository information from the VCS configuration
   - Unmounts the repository
   - Deports the disk group
   - Takes the volumes offline
3. Reconfigure the repository:

   ```
   # vxdg import sfua_rep
   ```

   ```
   # vxvol -g sfua_rep startall
   ```
4. Mount the repository file system manually.

   ```
   # mount -F vxfs /dev/vx/dsk/sfua_rep/dbed_rep /sfua_rep
   ```
5. Create a new repository:

   ```
   # /opt/VRTSdbcom/bin/sfua_db_config
   ```

   The following is required to configure the repository for SF Oracle RAC:

   - A mount point of already mounted Veritas Volume on a shared storage, with Veritas File system
   - A public NIC used by each system in the cluster
   - A Virtual IP address and netmask
6. Run the following command as the oracle user to update the repository:

   ```
   $ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
   ```

   Where:

   $ORACLE_SID is the database instance identifier

   $ORACLE_HOME is the Oracle home directory

To upgrade the repository from 4.x to 5.0.1 in a cluster environment

1. Create a local disk group.
2. Create a VxVM volume and VxFS mount point.
3. Create a new repository:

   ```
   # /opt/VRTSdbcom/bin/sfua_db_config
   ```

   The following is required to configure the repository for SF Oracle RAC:

   - A mount point of already mounted Veritas Volume on a shared storage, with Veritas File system
   - A public NIC used by each system in the cluster
   - A Virtual IP address and netmask
4. Run the following command as the oracle user to update the repository:

   ```
   $ dbed_update -S $ORACLE_SID -H $ORACLE_HOME
   ```

   Where:

   $ORACLE_SID is the database instance identifier

   $ORACLE_HOME is the Oracle home directory

Performing phased upgrade of SF Oracle RAC clusters

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

SF Oracle RAC supports phased upgrade of the cluster from the following versions:

- Version 5.0 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 on HP-UX 11i v3

Before you upgrade, complete the following tasks:

- Upgrade the operating system to HP-UX 11i v3 March 2009 OEUR release or later.
  See “Upgrading the operating system” on page 166.
- Back up the configuration files.
  See “Backing up the configuration files” on page 167.

Upgrading the operating system

Perform a rolling upgrade of the operating system as described in the following procedure one node at a time.

To upgrade the operating system

1. Stop all the applications on the node that are not under VCS control. Use native application commands to stop the applications.
2. If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.
3. Switch the failover groups from the node to any of the other nodes in the cluster.

   ```
   # hagrp -switch failover_group -to jupiter/mercury
   ```

4. Stop VCS on the node.

   ```
   # hastop -local
   ```

5. Upgrade the operating system.

   See “Upgrading the operating system” on page 150.

6 Uncomment the VxFS mount point entries in the /etc/fstab file.

7 Repeat steps 1 to 6 on each node in the cluster.

Backing up the configuration files

On the first half of the nodes in the cluster, back up the configuration files:

```
# 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
```

Upgrading from version 5.0 on HP-UX 11i v3 to SF Oracle RAC 5.0.1

Perform the steps in the following procedure to upgrade SF Oracle RAC clusters from version 5.0 on HP-UX 11i v3 with Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1.

Note: Do not disable fencing as the high availability daemon must be up and running for the upgrade.

To perform a phased upgrade of SF Oracle RAC

1 Switch the failover groups from the first half of the cluster to one of the nodes in the second half of the cluster.

```
# hagrp -switch failover_group -to jupiter
```

2 Stop all VCS service groups:

```
# hagrp -offline group_name -sys galaxy
```

```
# hagrp -offline group_name -sys nebula
```

3 Unmount all the VxFS file systems that are not under VCS control.

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

4 If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.

5 Stop VEA if it is running:

```
# /opt/VRTSob/bin/vxsvcctrl stop
```

6 Upgrade SF Oracle RAC on the first half of the cluster:

```
# ./installsfrac [-rsh] galaxy nebula
```

Caution: DO NOT reboot the first half of the cluster when prompted.

---

7 Move the LLT, GAB, VXFEN, VCSMM, and ODM startup scripts to another location on the first half of the cluster to ensure that the scripts do not start up on the nodes if the nodes reboot accidentally.

Note: If you fail to move these scripts and the node reboots accidentally, the second half of the cluster may panic.

```
# mv /sbin/init.d/llt /sbin/init.d/llt_preupgrade

# mv /etc/llttab /etc/llttab_preupgrade

# mv /sbin/init.d/gab /sbin/init.d/gab_preupgrade

# mv /sbin/init.d/vxfen /sbin/init.d/vxfen_preupgrade

# mv /sbin/init.d/vcsmm /sbin/init.d/vcsmm_preupgrade

# mv /sbin/init.d/odm /sbin/init.d/odm_preupgrade
```

8 After the installation completes, relink the Oracle RAC libraries with SF Oracle RAC on the first half of the cluster.

See “Relinking Oracle RAC libraries with the SF Oracle RAC libraries” on page 156.

Note: Your downtime starts now.

---

9 On the second half of the cluster, repeat steps 2 to 5.

10 Upgrade SF Oracle RAC on the second half of the cluster:

```
# ./installsfrac [-rsh] galaxy nebula
```

11 When all the SF Oracle RAC processes are stopped during the upgrade, restore the LLT, GAB, VXFEN, VCSMM, and ODM startup scripts (backed up in step 6) to the original location.

```
# mv /sbin/init.d/llt_preupgrade /sbin/init.d/llt

# mv /etc/llttab_preupgrade /etc/llttab

# mv /sbin/init.d/gab_preupgrade /sbin/init.d/gab

# mv /sbin/init.d/vxfen_preupgrade /sbin/init.d/vxfen

# mv /sbin/init.d/vcsmm_preupgrade /sbin/init.d/vcsmm

# mv /sbin/init.d/odm_preupgrade /sbin/init.d/odm
```

12 Uncomment the VxFS mount point entries in the /etc/fstab file.

13 Reboot the first half of the cluster:

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

Note: Your downtime ends here.

---

14 Verify that the following ports are up on the first half of the cluster:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen ada401 membership 01
Port b gen ada40d membership 01
Port d gen ada409 membership 01
Port h gen ada40f membership 01
Port o gen ada406 membership 01
```

15 Modify the CVMVolDg resource type configuration on the first half of the cluster.

See "Modifying the CVMVolDg resource type" on page 160.

16 Unfreeze all the VCS service groups and bring them online on the first half of the cluster.

```
# haconf -makerw
# hagrp -unfreeze servicegroup -persistent
# haconf -dump -makero
# hagrp -online group_name -sys galaxy
# hagrp -online group_name -sys nebula
```

17 Upgrade the CVM configuration on the first half of the cluster.

See "Upgrading the CVM configuration" on page 161.

18 After the upgrade completes on the second half of the cluster, relink the Oracle RAC libraries with SF Oracle RAC.

See "Relinking Oracle RAC libraries with the SF Oracle RAC libraries" on page 156.

19 Uncomment the VxFS mount point entries in the /etc/fstab file on the second half of the cluster.

20 Reboot the second half of the cluster:

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

When the second half of the cluster comes up, it joins the cluster.

21 Upgrade the repository database by performing the instructions in the following section:

See "Upgrading the repository database" on page 163.

Performing phased upgrade of SF Oracle RAC from versions 4.1x or 5.0x on HP-UX 11i v2

The phased upgrade involves the following steps:

- Upgrading the first half of the cluster, galaxy and nebula

Note: Your downtime starts after you complete the upgrade of the first half of the cluster.

- Stopping the second half of the cluster, jupiter and mercury
- Bringing online the first half of the cluster, galaxy and nebula

Note: Your downtime ends after you bring the first half of the cluster online.

- Upgrading the second half of the cluster, jupiter and mercury

Perform the following steps on the first half of the cluster, galaxy and nebula, to upgrade the first half of the cluster.

To upgrade the first half of the cluster

1 Stop all the applications that are not configured under VCS.

To stop Oracle Clusterware:

```
$ /sbin/init.d/crs stop
```

To stop the Oracle database:

```
$ srvctl stop database -d db-name
```

2 Switch the failover groups from the first half of the cluster to one of the nodes in the second half of the cluster:

```
# hagrp -switch failover_group -to jupiter
```

3 Stop all VCS service groups (including the cvm group):

```
# hagrp -offline group_name -sys galaxy
# hagrp -offline group_name -sys nebula
```

4 Freeze the nodes in the first half of the cluster

```
# haconf makerw
# hasys -freeze -persistent galaxy
# hasys -freeze -persistent nebula
# haconf -dump -makero
```

5 Stop VCS on the first half of the cluster:

```
# hastop -local -force
```

6 If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.

7 Set the LLT_START attribute to 0 in the `/etc/rc.config.d/lltconf` file:

```
LLT_START=0
```

8 On each node of the first half of the cluster, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

Note: To upgrade from SF Oracle RAC 4.1 on HP-UX 11i v2, create the `/etc/vxfenmode` file and populate it as above.

---

9 If the cluster-wide attribute `UseFence` is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file.

10 On each node of the first half of the cluster, 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
```

11 Upgrade the operating system.

See "Upgrading the operating system" on page 150.

12 Upgrade SF Oracle RAC:

```
# ./installsfrac [-rsh] galaxy nebula
```

Caution: DO NOT reboot the cluster.

Perform the following steps on the second half of the cluster, jupiter and mercury, to stop the second half of the cluster.

Note: The downtime starts now.

To stop the second half of the cluster

1. Stop all the applications that are not configured under VCS.

   To stop Oracle Clusterware:

   ```
   $ /sbin/init.d/crs stop
   ```

   To stop the Oracle database:

   ```
   $ srvctl stop database -d db-name
   ```

2. Stop all VCS service groups (including the cvm group):

   ```
   # hagrp -offline group_name -sys jupiter
   # hagrp -offline group_name -sys mercury
   ```

3. Freeze the VCS service groups on the second half of the cluster:

   ```
   # haconf -makerw
   # hagrp -freeze group_name -persistent
   # haconf -dump -makero
   ```

4. Stop VCS on the second half of the cluster:

   ```
   # hastop -local -force
   ```

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 /etc/fstab file.

6. Set the LLT_START attribute to 0 in the `/etc/rc.config.d/lltconf` file:

   ```
   LLT_START=0
   ```

7. On each node of the second half of the cluster, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode:

   ```
   # cat /etc/vxfenmode
   vxfen_mode=disabled
   ```

   Note: To upgrade from SF Oracle RAC 4.1 on HP-UX 11i v2, create the `/etc/vxfenmode` file and populate it as above.

   ---

8. 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.

9 Stop all the modules on the second half of the cluster:

```
# /sbin/vcsmmconfig -U
# /sbin/lmxconfig -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
# kcmodule lmx=unused
# kcmodule gab=unused
# lltconfig -U
# kcmodule llt=unused
```

10 On each node of the second half of the cluster, 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
```

Perform the following steps on the first half of the cluster, galaxy and nebula, to bring the first half of the cluster online.

To bring the first half of the cluster online

1 Uncomment the VxFS mount point entries in the **/etc/fstab** file.

2 Mount the VxFS file systems that were commented in step 6

3 Enable fencing:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

4 Remove the following line from `/etc/VRTSvcs/conf/config/main.cf`:

```
Frozen=1
```

5 Set the clusterwide attribute `UseFence` to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

```
UseFence=SCSI3
```

6 Add the include statements for `MultiPrivNIC.cf` and `OracleASMTypes.cf`in the `/etc/VRTSvcs/conf/config/main.cf` file.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "PrivNIC.cf"
include "OracleTypes.cf"
include "MultiPrivNIC.cf"
include "OracleASMTypes.cf"
```

7 Reset the LLT_START attribute to 1 in the `/etc/rc.config.d/lltconf` file:

```
LLT_START=1
```

8 Remove the file `.SFRAC.upgrade` located in the directory `/opt/VRTS/install`.

9 Relink the Oracle RAC libraries with SF Oracle RAC on the first half of the cluster.

See "To relink the Oracle RAC libraries with SF Oracle RAC libraries manually" on page 158.

10 Reboot the first half of the cluster:

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

11 After the nodes come up, seed the cluster membership:

```
# gabconfig -x
```

The first half of the cluster is now up and running.

Note: The downtime ends here.

---

12 Complete the following post-upgrade tasks:

- Modifying the CVMVolDg resource type
- Upgrading the CVM configuration

- Upgrading the disk layout version

  For instructions:

  See "Performing post-upgrade tasks" on page 156.

Perform the following steps on the second half of the cluster, jupiter and mercury, to upgrade the second half of the cluster.

To upgrade the second half of the cluster

1. Upgrade the operating system.

   See "Upgrading the operating system" on page 150.

2. Upgrade SF Oracle RAC:

   ```
   # ./installsfrac [-rsh] jupiter mercury
   ```

   Caution: DO NOT reboot the cluster.

   ---

3. Uncomment the VxFS mount point entries in the **/etc/fstab** file.
4. Mount the VxFS file systems that were commented in step 5
5. Enable fencing:

   ```
   # cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
   ```

6. Reset the LLT_START attribute to 1 in the `/etc/rc.config.d/lltconf` file:

   ```
   LLT_START=1
   ```

7. Remove the file `.SFRAC.upgrade` located in the directory `/opt/VRTS/install`.
8. Relink the Oracle RAC libraries with SF Oracle RAC on the first half of the cluster.

   See "To relink the Oracle RAC libraries with SF Oracle RAC libraries manually" on page 158.

9. Reboot the second half of the cluster:

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

   The nodes jupiter and mercury now join the first half of the cluster.

10. Start the applications that are not configured under VCS. Use native application commands to start the applications.

11 Upgrade the repository database by performing the instructions in the following section:

See "Upgrading the repository database" on page 163.

12 Upgrade Oracle RAC.

See the chapter *Upgrading Oracle RAC and migrating the database* in this document.

Section 3

Oracle RAC installation in an SF Oracle RAC environment

Chapter 9

Preparing to install Oracle RAC

This chapter includes the following topics:

About preparing to install Oracle RAC

This chapter provides instructions for completing the pre-installation tasks for Oracle RAC 10g and Oracle RAC 11g installations. The instructions are common to both versions of Oracle RAC, except where stated otherwise.

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.

The examples in this chapter assume a two-node cluster comprising the nodes galaxy and nebula.

Before installing Oracle RAC:

- Keep the Oracle worksheets handy as you perform the pre-installation tasks.
  See "Oracle RAC Worksheets" on page 432.

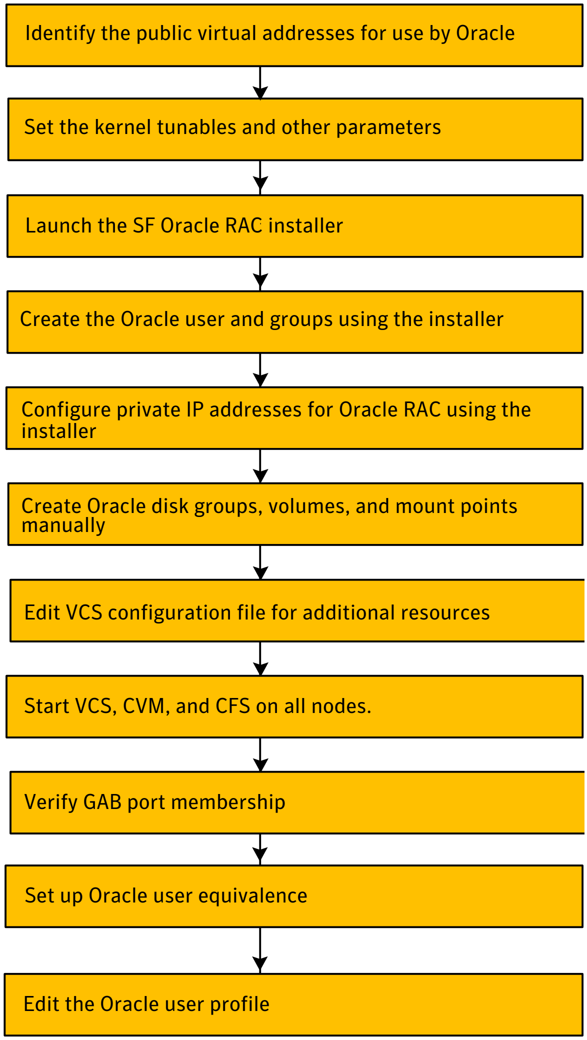
- Review your Oracle installation manuals and the appropriate Oracle support websites.

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.

Figure 9-1 Oracle RAC pre-installation tasks

Figure 9-2 displays the steps required to prepare for an Oracle RAC installation.

Figure 9-2 Oracle RAC pre-installation tasks



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.

Perform the following tasks before you install Oracle RAC:

- Identifying the public virtual IP addresses for use by Oracle
- Setting the kernel parameters
- Launching the SF Oracle RAC installer
- Creating Oracle user and groups
- Setting privileges for the DBA user
- Configuring private IP addresses for Oracle RAC
- Creating disk groups, volumes, and mount points for Oracle RAC
- Editing the VCS configuration file for additional Oracle Clusterware resources
- Starting VCS, CVM, and CFS on all nodes
- Verifying GAB port membership
- Setting up Oracle user equivalence
- Editing the Oracle user profile

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 manages the virtual IP addresses.

The IP address and the corresponding host name should be registered in the domain name service (DNS) for each public network interface. Alternatively, an entry for the virtual IP address and virtual public name can be placed in the `/etc/hosts` file.

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 for the nodes must be different from the host's current fully qualified domain name (FQDN).

Setting the kernel parameters

You need to tune the kernel parameters as required by Oracle RAC.

For complete instructions and guidelines, see the Oracle documentation.

Restart the nodes for the new values to take effect.

Launching the SF Oracle RAC installer

The following procedure describes the Oracle RAC pre-installation tasks using the SF Oracle RAC configuration program and menu. Make sure that you have installed and configured SF Oracle RAC before performing the instructions in this section.

To perform pre-installation tasks in the configuration menu

1. If the SF Oracle RAC configuration program is not currently running, launch the SF Oracle RAC configuration program.

   As root user on any one system, enter:

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

   ```
   # ./installsfrac  [-rsh] -configure
   ```

   By default, the installsfrac program uses SSH for remote communication.

   To use RSH, specify the -rsh option with the installsfrac program.

2. The SF Oracle RAC configuration program displays the Symantec copyright information, as well as the location of the installsfrac logs.

   Note: If necessary, the installsfrac logs can be used for troubleshooting purposes.

   ---

3. If you have previously configured SF Oracle RAC, then information from the SFRAC configuration files currently on the system appears. This information will include the cluster name, cluster ID, systems for the cluster, and cluster service groups.

   Next, you will be prompted whether you wish to configure SFRAC from these systems.

   ```
   Do you want to configure SFRAC from these systems? [y,n,q] (y)
   ```

4. The SF Oracle RAC configuration program then performs an initial system check of the SSH or RSH communication, SF Oracle RAC installation, and architecture on the nodes.

5. The SF Oracle RAC configuration program then checks your system license on the nodes. You will be asked whether you want to enter another license key on each system.

   If not, then enter "n" to proceed.

6 The SF Oracle RAC configuration program then displays the following information about its INSTRUCTIONS ONLY steps:

```
* Do not perform any action
* Require you to understand the instructions and act
* May require you to refer to the documentation
```

Press enter to proceed.

The following additional information is provided:

```
* Keep root shells open on all systems to run INSTRUCTIONS ONLY steps
* Follow the steps in order
* Navigation keys for all screens: q to quit, b for previous menu
```

7 The configuration program menu is then displayed:

```
1) Check systems for SFRAC ** INSTRUCTIONS ONLY **
2) Configure SFRAC
3) Prepare to install Oracle
4) Install or relink Oracle
```

From this menu, you can choose to perform all installation tasks, or to perform specific tasks.

From the configuration program menu, select **Prepare to install Oracle**.

8 After selecting the **Prepare to install Oracle** option, the following menu is presented:

```
 1)  [Perform all the following tasks]
2)  Create userid and groupid for Oracle
3)  Configure private IP addresses for failover (PrivNIC Configuration)
4)  Configure private IP addresses for failover (MultiPrivNIC Configuration
5)  Create disk groups, volumes and file systems for Oracle ** INSTRUCTIONS
b)  [Go to previous menu]
```

Proceed to select the appropriate options for your installation and follow the steps to pre-install Oracle RAC.

- For information about option 2 (Create userid and groupid for Oracle): See "Creating Oracle user and groups" on page 187.
- For information about option 3 (Configure private IP addresses for failover (PrivNIC Configuration): See "Configuring private IP addresses for Oracle RAC" on page 191.
- For information about option 4 (Configure private IP addresses for failover (MultiPrivNIC Configuration):

See "Configuring private IP addresses for Oracle RAC" on page 191.

- For information about option 5 (Create disk groups, volumes, and file systems for Oracle ** INSTRUCTIONS ONLY **):
  See "Creating disk groups, volumes, and mount points for Oracle RAC" on page 196.

Creating Oracle user and groups

Perform this step only if you have not already created the Oracle user and groups while preparing to install SF Oracle RAC.

You must create the Oracle groups oinstall (the Oracle Inventory group) and dba. You must create the Oracle user oracle. You must assign the primary group for Oracle to be oinstall and the secondary group for Oracle to be dba.

Note: Refer to the latest Oracle documentation for additional information.

You can create Oracle users and groups using the SF Oracle RAC configuration program. As discussed above, refer to the Oracle documentation for information about creating the oinstall (Oracle Inventory), `dba` and `oper` groups, and the oracle user. After reviewing the Oracle documentation, proceed to create these Oracle groups and user.

Note: Make sure that the user and group IDs are unused on all the nodes in the cluster.

To create Oracle user and groups

1. Select **Create userid and groupid for Oracle** from the configuration menu within the SF Oracle RAC configuration program.
2. Provide the required information for the configuration program.

   The first step in this configuration process creates the user and group ids on all cluster nodes for Oracle.

   The configuration program assigns the same values on all nodes. The text within parentheses is the default, which you may select by pressing Enter.

   ```
   Enter Oracle UNIX user name: [b] (oracle)
   Enter Oracle UNIX user id (numerical): [b] 100
   Enter Oracle UNIX user home dir: [b] /home/oracle
   Enter Oracle UNIX group name: [b] (oinstall)
   Enter Oracle UNIX group id: [b] 1000
   User oracle does not exist on any node. Do you want to create it
   with the information provided [y,n,q] (y)
   ```

   Note: The set of Oracle user IDs and group IDs in each cluster node must be the same. Furthermore, if you are configuring GCO, then the user IDs and group IDs of all nodes of both the primary and secondary clusters must be the same.

3. The installer verifies that the specified `userid` does not exist on any of the systems in the cluster and then creates it. Enter y to create the oracle user with the information provided.

4 Next, enter the information to create secondary groups, "dba" and "oper".

The secondary group "oper" is optional.

The SF Oracle RAC configuration program displays the following message:

```
This step creates secondary group ids on all cluster nodes.
Oracle requires some other special groups for identifying
operating system accounts that have database admin (SYSDBA)
privileges and for those accounts that have limited sets
of database admin (SYSOPER) privileges. You should create
such groups on all systems and Oracle user should be part
of these groups.
```

The following options are then presented. Enter the appropriate values for your installation or accept the default values.

```
Do you want to create another secondary group for Oracle user? [y,n,q]

Enter Oracle UNIX secondary group name: [b] dba
Enter Oracle UNIX secondary group id (numerical): [b] 1001

Group dba does not exist on any node. Do you want to create it
with the information provided [y,n,q] (y) y
    Creating group dba on galaxy ......................... Done
    Adding Oracle user (oracle) to group (dba) on galaxy .. Done
    Creating group dba on nebula ......................... Done
    Adding Oracle user (oracle) to group (dba) on nebula .. Done
```

5 Create a password for the oracle user on each node:

```
# passwd oracle
```

6 Next, you are prompted to perform SSH or RSH verification. Enter "y" to perform verification. Review as the configuration program verifies access for Oracle user on all the nodes. The Oracle installation process requires SSH or RSH permission to be set for the Oracle user. If the SSH or RSH verification fails on any nodes, enable SSH or RSH access for those nodes.

   To enable RSH access for the nodes, leave the installer at this prompt and proceed to set up access. Open a new session to set up access. You can return to this session after setting up oracle user equivalence.

7 Edit the Oracle user .profile file to enable paths to $CRS_HOME, $ORACLE_HOME, and $ORACLE_BASE on each node.

   On each node, set the proper environment variables (the following examples are for ksh):

```
$ export ORACLE_BASE=/app/oracle
$ export ORACLE_HOME=/app/oracle/orahome
$ export CRS_HOME=/app/crshome
$ export LIBPATH=$ORACLE_HOME/lib:$ORACLE_HOME/lib32:$CRS_HOME/\
  lib:$CRS_HOME/lib32:/usr/lib:/lib
$ export PATH=$PATH:$CRS_HOME/bin:$ORACLE_HOME/bin
$ export CLASSPATH=$CLASSPATH:$ORACLE_HOME/JRE:$ORACLE_HOME\
/jlib:$ORACLE_HOME/rdbms/jlib:$ORACLE_HOME/network/jlib
```

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
   ```

Configuring private IP addresses for Oracle RAC

You can configure clusterware and UDP private addresses for failover using either the SF Oracle RAC installer or manually. To configure clusterware and UDP private addresses for failover using the SF Oracle RAC installer, perform the tasks described in the following procedures:

- Configure private IP addresses for clusterware and UDP cache fusion
- Add private IP addresses to the /etc/hosts file
- Verify the private IP addresses

Configure private IP addresses for clusterware and UDP cache fusion

1. Review your configuration and decide whether you want to set up clusterware and UDP cache fusion using either the PrivNIC or MultiPrivNIC agent.
2. Select the appropriate option to configure your private IP addresses for clusterware and UDP cache fusion:

- Select option 3 from the SF Oracle RAC configuration menu for a clusterware and UDP cache fusion configuration using the PrivNIC agent. The path to this configuration option is:

  ```
  Main Menu > Prepare to install Oracle >
  Configure private IP addresses for failover (PrivNIC Configuration)
  ```

- Select option 4 from the SF Oracle RAC configuration menu for a clusterware and UDP cache fusion configuration using the MultiPrivNIC agent. The path to this configuration option is:

  ```
  Main Menu > Prepare to install Oracle >
  Configure private IP addresses for failover (MultiPrivNIC Configuration)
  ```

If you want to use multiple private IP addresses for Oracle database cache fusion, then add the IP addresses to the oracle init file after you create the database. For information about the procedure to add UDP IP addresses to the oracle init file:

3 For option 3 (PrivNIC agent), enter the private IP address information for each host. You will be prompted for this information.

```
Enter the private IP for galaxy: [b] 192.168.12.1

Enter the NIC for private network 1 for galaxy (x if done): [b] lan1

Enter the NIC for private network 2 for galaxy (x if done): [b] lan2

Enter the NIC 3 for private network for galaxy (x if done): [b] x

Enter the private IP for nebula: [b] 192.168.12.2

Enter the NIC for private network 1 for nebula (x if done): [b] lan1

Enter the NIC for private network 2 for nebula (x if done): [b] lan2

Enter the NIC for network 3 for nebula (x if done): [b] x
```

Next, proceed to step 6.

4 For option 4 (MultiPrivNIC agent), SF Oracle RAC configuration program proceeds to discover and display NIC devices on each of the nodes. You are prompted to select the NIC devices on each node.

```
Discovering NICs on galaxy .... discovered lan0 lan1 lan2 lan3
Enter NIC 0 for galaxy (x if done): [b] lan1
Enter NIC 1 for galaxy (x if done): [b] lan2
Enter NIC 2 for galaxy (x if done): [b] x

Discovering NICs on nebula .... discovered lan0 lan1 lan2 lan3
Enter NIC 0 for galaxy (x if done): [b] lan1
Enter NIC 1 for galaxy (x if done): [b] lan2
Enter NIC 2 for galaxy (x if done): [b] x
```

5 For option 4 (MultiPrivNIC agent), enter the private IP address information for each host. You will be prompted for this information.

```
Enter IP address 1 for galaxy for lan1 (x if done): [b] 192.168.1.1
Enter IP address 2 for galaxy for lan1 (x if done): [b] 192.168.1.2
Enter IP address 3 for galaxy for lan1 (x if done): [b] x


Enter IP address 1 for galaxy for lan2 (x if done): [b] 192.168.2.1
Enter IP address 2 for galaxy for lan2 (x if done): [b] x


Enter IP address 1 for nebula for lan1 (x if done): [b] 192.168.1.3
Enter IP address 2 for nebula for lan1 (x if done): [b] 192.168.1.4
Enter IP address 3 for nebula for lan1 (x if done): [b] x


Enter IP address 1 for nebula for lan2 (x if done): [b] 192.168.2.2
Enter IP address 2 for nebula for lan2 (x if done): [b] x
```

6 For both options, enter the netmask for the private network:

```
Enter the netmask for private network: [b] 255.255.255.0
```

7 The SF Oracle RAC configuration program then displays the configured parameters for the private IP address information.

Review and confirm the private IP address information displayed.

After confirming the values, the SF Oracle RAC configuration program adds a new section in the VCS configuration file (main.cf) for the PrivNIC or MultiPrivNIC resource in the CVM group.

See " PrivNIC agent" on page 495.

See " MultiPrivNIC agent" on page 500.

8 After the private IP address is configured, you can exit the installer by entering **q** or continue with your configuration.

Add private IP addresses to the /etc/hosts file

1 Log to each system as root.

2 For a configuration using the PrivNIC agent and using vi or another text editor, add the following entries to the /etc/hosts file:

```
198.168.12.1   galaxy_priv

198.168.12.2   nebula_priv
```

For a configuration using the MultiPrivNIC agent and using vi or another text editor, add the following entries to the /etc/hosts file:

```
198.168.1.1   galaxy_priv

198.168.1.3   nebula_priv
```

Verify the VCS configuration for PrivNIC and MultiPrivNIC

1. Access and view the VCS main.cf located in the following directory: /etc/VRTSvcs/conf/config.

   Enter the following command:

   ```
   # more /etc/VRTSvcs/conf/config/main.cf
   ```

2. For a configuration using the PrivNIC agent, verify that the PrivNIC resource, ora_priv, displays in VCS main.cf:

```
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"
                   )
```

3. For a configuration using the MultiPrivNIC agent, verify that the MultiPrivNIC resource, multi_priv, displays in VCS main.cf:

```
MultiPrivNIC multi_priv (
             Critical = 0
             Device @galaxy = {lan1= 0, lan2 = 1}
             Device @nebula = {lan1= 0, lan2 = 1}
             Address @galaxy = {"192.168.1.1" =0, "192.168.1.2" =0, "192.168.2.1" =1}
             Address @nebula = {"192.168.1.3" =0, "192.168.1.4" =0, "192.168.2.2" =1}
             NetMask = "255.255.255.0"
             )
```

4. For a configuration using the PrivNIC agent, verify that the "ora_priv" resource is online on all systems in the cluster by issuing the following command:

   ```
   # hares -state ora_priv
   # Resource Attribute System Value
     ora_priv State    galaxy   ONLINE
     ora_priv State    nebula   ONLINE
   ```

5 For a configuration using the MultiPrivNIC agent, verify that the "multi_priv" resource is online on all systems in the cluster, by entering the following command:

```
# hares -state multi_priv
# Resource    Attribute        System      Value
multi_priv       State          galaxy     ONLINE
multi_priv       State          nebula     ONLINE
```

6 On each system, check the output of "ifconfig".

```
#  ifconfig -a
```

7 From each system, ping the private IP addresses to ensure that they are operational:

```
# ping nebula_priv

PING nebula_priv: 64 byte packets
64 bytes from 192.168.12.2: icmp_seq=0. time=0. ms
64 bytes from 192.168.12.2: icmp_seq=1. time=0. ms
64 bytes from 192.168.12.2: icmp_seq=2. time=0. ms

# ping galaxy_priv

PING galaxy_priv: 64 byte packets
64 bytes from 192.168.12.1: icmp_seq=0. time=0. ms
64 bytes from 192.168.12.1: icmp_seq=1. time=0. ms
64 bytes from 192.168.12.1: icmp_seq=2. time=0. ms
```

Creating disk groups, volumes, and mount points for Oracle RAC

This section describes the procedures for creating disk groups, volumes, and mount points for Oracle RAC.

To create disk groups, volumes, and mount points for Oracle RAC

1 Select **Create disk groups, volumes and file systems for Oracle ** INSTRUCTIONS ONLY **** from the menu if you want to specifically perform this task.

2 Review the displayed guidelines and proceed to the following step.

3 Before you install the Oracle Clusterware and Oracle RAC binaries, you must create storage space for these installations.

Note: Symantec recommends you to install the Oracle Clusterware and Oracle RAC database binaries on local storage on each node.

Create storage space for:

■ The home directory ($CRS_HOME) for Oracle Clusterware binaries.	On each node, create a volume and file system for $CRS_HOME. For detailed information: See "Preparing to store the Oracle Clusterware binaries" on page 197.
■ The home directory ($ORACLE_HOME) for Oracle binaries.	For detailed information: See "Preparing to store the Oracle RAC database binaries" on page 199.
■ The clusterware files for Oracle Cluster Registry (OCR) and the voting disk.	The clusterware files can reside in volumes on raw device, or in directories in a cluster file system. For detailed information: See "Creating volumes or directories for OCR and voting disk" on page 205.

Preparing to store the Oracle Clusterware binaries

The Oracle Clusterware binaries (CRS_HOME) can either be installed locally on each system or on a cluster file system. Local installations provide improved protection against a single point of failure and support phased upgrade.

CFS installations provide a single Oracle installation to manage, regardless of number of nodes. This scenario offers a necessary reduction in storage requirements and easy addition of nodes.

Note: Symantec and Oracle strongly recommend using local installations for CRS_HOME.

On each system in the SF Oracle RAC cluster, create a directory for CRS_HOME. The minimum disk space required is 2 GB for Oracle RAC 10g and 3 GB for Oracle RAC 11g. The example procedure uses galaxy as one of the nodes.

Keep the information required to prepare $CRS_HOME handy.

See "Oracle RAC Worksheets" on page 432.

To create storage for Oracle Clusterware binaries on local disks

1. Make sure you are logged in as superuser on one system
2. On one node, create a private disk group on local storage. For example:

   ```
   # vxdg init crsdg_galaxy c4t0d0
   ```

3. Create the volume in the group for the CRS_HOME. The volume should be a minimum of 2 GB for Oracle RAC 10g and 3 GB for Oracle RAC 11g:

   ```
   # vxassist -g crsdg_galaxy make crsvol_galaxy 2000M
   ```

4. Create a VxFS file system on which to install Oracle Clusterware. For example:

   ```
   # mkfs -F vxfs /dev/vx/rdsk/crsdg_galaxy/crsvol_galaxy
   ```

5. Create the mount point for the file system.

   ```
   # mkdir /app/crshome
   ```

6. Mount the file system, using the device file for the block device:

   ```
   # mount -F vxfs /dev/vx/dsk/crsdg_galaxy/crsvol_galaxy \
   /app/crshome
   ```

7. Add an entry to the /etc/fstab file. For example:

   ```
   /dev/vx/dsk/crsdg_galaxy/crsvol_galaxy /app/crshome vxfs
   delaylog 0 2
   ```

8. Set the CRS_HOME directory for the oracle user as /app/crshome.
9. Assign ownership of the CRS_HOME directory to oracle and the group oinstall:

   ```
   # chown -R oracle:oinstall /app/crshome
   ```

10. Repeat the above steps on each of the other nodes in the cluster.

To create storage space for Oracle Clusterware binaries on shared storage

1. As the root user, create a VxVM shared disk group `bindg`:

   ```
   # vxdg -s init crsbindg c4t0d2
   ```

2. Set the activation mode for the disk group on all the nodes.

   ```
   # vxdg -g crsbindg set activation=sw
   ```

3 Create separate volumes for Oracle Clusterware (`crsbinvol`) and Oracle database (`orabinvol`):

```
# vxassist -g crsbindg make crsbinvol 5G
```

4 Log onto the master node and start the volumes:

```
# vxvol -g crsbindg startall
```

5 On each node, create the ORACLE_BASE and CRS_HOME directories:

```
# mkdir -p /app/oracle
```

```
# mkdir -p /app/crshome
```

6 Create the file system with the volume `crsbinvol`:

```
# mkfs -F vxfs /dev/vx/rdsk/crsbindg/crsbinvol
```

7 On each node, mount the file systems:

```
# mount -F vxfs -o cluster /dev/vx/dsk/crsbindg/crsbinvol \
/app/crshome
```

8 On each node, change the ownership and permissions:

```
# chown -R oracle:oinstall /app
# chmod -R 744 /app
```

9 Add the CFSMount and CVMVolDg resources to the VCS configuration.

See "To add the CFSMount and CVMVolDg resources to the VCS configuration using CLI" on page 202.

Preparing to store the Oracle RAC database binaries

The Oracle RAC database binaries (ORACLE_HOME) can either be installed locally on each system or on a cluster file system. Local installations provide improved protection against a single point of failure and support phased upgrade.

CFS installations provide a single Oracle installation to manage, regardless of number of nodes. This scenario offers a necessary reduction in storage requirements and easy addition of nodes.

Note: Symantec and Oracle strongly recommend using local installations.

You must create the disk group, volume, and mount points on each node that would be a part of the cluster.

Keep the required information handy.

See "Oracle RAC Worksheets" on page 432.

Perform the following steps in each node in the cluster.

To create storage space for Oracle RAC database binaries on local disks

1. Log in as superuser on one node.
2. On one node, create a disk group in the available local storage.

   ```
   # vxdg init orabindg_galaxy c4t0d2
   ```

3. Create the volume in the group. For the Oracle RAC binaries, make the volume 7 GB.

   ```
   # vxassist -g orabindg_galaxy make orabinvol_galaxy 7168M
   ```

4. Create a VxFS file system on orbin_vol to install the Oracle RAC binaries. For example:

   ```
   # mkfs -F vxfs /dev/vx/rdsk/orabindg_galaxy/orabinvol_galaxy
   ```

5. Create the mount point for the file system.

   ```
   # mkdir /app/oracle/orahome
   ```

6. Mount the file system using the device file for the block device.

   ```
   # mount -F vxfs /dev/vx/dsk/orabindg_galaxy/orabinvol_galaxy \
   /app/oracle/orahome
   ```

7. Edit the /etc/fstab file and list the new file system. For example:

   ```
   /dev/vx/dsk/orabindg_galaxy/orabinvol_galaxy
   /app/oracle/ orahome vxfs delaylog 0 1
   ```

8. Assign ownership of the Oracle directory to oracle:

   ```
   # chown -R oracle:oinstall /app/oracle/orahome
   ```

   ```
   # chmod 775 /app/oracle/orahome
   ```

9. Repeat the above steps on the other nodes.

To create storage space for Oracle files on shared storage

1. As the root user, create a VxVM shared disk group `bindg`:

   ```
   # vxdg -s init orabindg c4t0d2
   ```

2. Set the activation mode for the disk group on all the nodes.

   ```
   # vxdg -g orabindg set activation=sw
   ```

3. Create separate volumes for Oracle Clusterware (`crsbinvol`) and Oracle database (`orabinvol`):

   ```
   # vxassist -g orabindg make orabinvol 7G
   ```

4. Log onto the master node and start the volumes:

   ```
   # vxvol -g orabindg startall
   ```

5. On each node, create the ORACLE_HOME directory:

   ```
   # mkdir -p /app/oracle/orahome
   ```

6. Create the file system with the volumes `crsbinvol, orabinvol`:

   ```
   # mkfs -F vxfs /dev/vx/rdsk/orabindg/orabinvol
   ```

7. On each node, mount the file systems:

   ```
   # mount -F vxfs -o cluster /dev/vx/dsk/orabindg/orabinvol \
   /app/oracle/orahome
   ```

8. On each node, change the ownership and permissions:

   ```
   # chown -R oracle:oinstall /app
   # chmod -R 744 /app
   ```

9. Add the CFSMount and CVMVolDg resources to the VCS configuration.

   See "To add the CFSMount and CVMVolDg resources to the VCS configuration using CLI" on page 202.

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 crsbin_voldg CVMVolDg cvm

# hares -add orabin_voldg CVMVolDg cvm

# hares -modify crsbin_voldg CVMDiskGroup crsbindg

# hares -modify orabin_voldg CVMDiskGroup orabindg

# hares -modify crsbin_voldg CVMVolume crsbinvol

# hares -modify orabin_voldg CVMVolume orabinvol

# hares -modify crsbin_voldg CVMActivation sw

# hares -modify orabin_voldg CVMActivation sw
```

3. Set up the file system under VCS:

```
# hares -add crsbin_mnt CFSMount cvm

# hares -modify crsbin_mnt Critical 0

# hares -modify crsbin_mnt MountPoint "/app/crshome"

# hares -modify crsbin_mnt BlockDevice  \
"/dev/vx/dsk/crsbindg/crsbinvol"

# hares -add orabin_mnt CFSMount cvm

# hares -modify orabin_mnt Critical 0

# hares -modify orabin_mnt MountPoint "/app/oracle/orahome"

# hares -modify orabin_mnt BlockDevice  \
"/dev/vx/dsk/orabindg/orabinvol"
```

4 Link the parent and child resources:

```
# hares -link crsbin_voldg cvm_clus

# hares -link orabin_voldg cvm_clus

# hares -link crsbin_mnt crsbin_voldg

# hares -link orabin_mnt orabin_voldg

# hares -link crsbin_mnt vxfsckd

# hares -link orabin_mnt vxfsckd
```

5 Enable the resources:

```
# hares -modify crsbin_voldg Enabled 1

# hares -modify orabin_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.

```
CFSMount crsbin_mnt (
               Critical = 0
               MountPoint = "/app/crshome"
               BlockDevice = "/dev/vx/dsk/crsbindg/crsbinvol"
               )

CFSMount orabin_mnt (
               Critical = 0
               MountPoint = "/app/oracle/orahome"
               BlockDevice = "/dev/vx/dsk/orabindg/orabinvol"
               )

CVMVolDg crsbin_voldg (
              Critical = 0
              CVMDiskGroup = crsbindg
              CVMVolume = { crsbinvol }
              CVMActivation = sw
              )
CVMVolDg orabin_voldg (
              Critical = 0
              CVMDiskGroup = orabindg
              CVMVolume = { orabinvol }
              CVMActivation = sw
              )

crsbin_mnt requires crsbin_voldg
crsbin_mnt requires vxfsckd
orabin_mnt requires orabin_voldg
orabin_mnt requires vxfsckd
crsbin_voldg requires cvm_clus
orabin_voldg requires cvm_clus
```

7 Verify that the resources are online on all systems in the cluster.

```
# hares -state crsbin_voldg
```

```
# hares -state orabin_voldg
```

```
# hares -state crsbin_mnt
```

```
# hares -state orabin_mnt
```

Note: The crsorabin_voldg resource is reported offline though the underlying volume is online. You need to manually bring the resource online on each node.

To bring the resource online manually:

```
# hares -online crsbin_voldg -sys galaxy
```

```
# hares -online crsbin_voldg -sys nebula
```

```
# hares -online orabin_voldg -sys galaxy
```

```
# hares -online orabin_voldg -sys nebula
```

Creating volumes or directories for OCR and voting disk

The OCR and voting disk must be shared among all nodes in a cluster. You can do one of the following:

- Create OCR and voting disk volumes on shared raw volumes.
  See "To create OCR and voting disk volumes on raw volumes" on page 206.
- Create OCR and voting disk directories in a cluster file system.
  See "To create OCR and voting disk directories on CFS" on page 206.

Keep the information required to create OCR and voting Disk directories (on raw volumes or CFS) handy.

See "Oracle RAC Worksheets" on page 432.

Whether you create shared volumes or shared file system directories, you can add them in the VCS configuration to make them highly available.

Symantec recommends creating OCR and voting disk on shared raw volumes that are mirrored across disks. During Oracle Clusterware installation, choose external redundancy for OCR and voting disks.

To create OCR and voting disk volumes on raw volumes

1. Log in as superuser.
2. On the master node, create a shared disk group:

   ```
   # vxdg -s init ocrvotedg c4t0d1
   ```

3. Create volumes in the shared group for OCR and voting disk (minimum volume size required is 256 MB):

   ```
   # vxassist -g ocrvotedg make ocrvol 300M
   ```

   ```
   # vxassist -g ocrvotedg make votevol 300M
   ```

4. Assign ownership of the volumes using the vxedit(1M) command: vxedit -g disk_group set group=group user=user mode=660 volume For example:

   ```
   # vxedit -g ocrvotedg set group=oinstall user=oracle mode=660
   ocrvol
   ```

   ```
   # vxedit -g ocrvotedg set group=oinstall user=oracle mode=660
   votevol
   ```

5. Start the volume:

   ```
   # vxvol -g ocrvotedg startall
   ```

To create OCR and voting disk directories on CFS

1. Log in as superuser.
2. On the master node, create a shared disk group:

   ```
   # vxdg -s init ocrvotedg c4t0d1
   ```

3. Set the activation mode for the disk group on all cluster nodes:

   ```
   # vxdg -g ocrvotedg set activation=sw
   ```

4. Create volumes in the shared disk group for OCR and voting disk:

   ```
   # vxassist -g ocrvotedg make ocrvotevol 2000M
   ```

5. Start the volume:

   ```
   # vxvol -g ocrvotedg startall
   ```

6 Create the file system:

```
# mkfs -F vxfs /dev/vx/rdsk/ocrvotedg/ocrvotevol
```

7 Create a mount point for the voting disk and OCR files on all the nodes.

```
# mkdir /ocrvote
```

8 On all nodes, mount the file system:

```
# mount -F vxfs -o cluster /dev/vx/dsk/ocrvotedg/ocrvotevol\
/ocrvote
```

9 Set “oracle” to be the owner of the file system, and set “755” as the permissions:

```
# chown -R oracle:oinstall /ocrvote
```

```
# chmod 755 /ocrvote
```

Editing the VCS configuration file for additional Oracle Clusterware resources

You must manually modify the CVM service group in the main.cf to add or modify other resources for Oracle Clusterware:

- If the OCR and voting disks are created on CVM raw volumes, add the CVMVolDG resource.
- If the OCR and voting disks are created on CFS, add the CFSMount resource in addition to the CVMVolDG resource.
- Add the Application resource that monitors Oracle Clusterware within the CVM service group. If the Application resource is not configured, the commands used to offline the shared mounts (such as `hastop -local`, `hastop -all`, or `hagrp -offline`) cause the nodes to automatically reboot.
- If the PrivNIC or MultiPrivNIC resources are not configured using the installer, configure them manually.

To modify the main.cf for additional Oracle Clusterware resources

1 Log into one of the nodes in the cluster.

2 Save the existing configuration to disk and make the configuration readonly while making the changes:

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

3. To ensure VCS is not running while you edit the main.cf, use the `hastop` command to stop the VCS engine on all nodes and leave the resources available:

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

4. Make a backup copy of the main.cf file:

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

   ```
   # cp main.cf main.orig
   ```

5. Use vi or another text editor to edit the main.cf file.

6. Add the CVMVolDG resource for the volume. In this example, only one volume exists because the OCR and voting disk are directories in a cluster file system:

   ```
   CVMVolDg ocrvote_voldg (
       Critical = 0
       CVMDiskGroup = ocrvotedg
       CVMVolume = { ocrvotevol }
       CVMActivation = sw
       )
   .
   .
   ```

7. If you created a cluster file system for the OCR and voting disk directories, add the CFSMount resources for the cluster file system:

   ```
   CFSMount ocrvote_mnt (
       Critical = 0
       MountPoint = "/ocrvote"
       BlockDevice = "/dev/vx/dsk/ocrvotedg/ocrvotevol"
       )
   .
   .
   ```

8 To manually configure the PrivNIC resource, modify the main.cf file by adding PrivNIC to the cvm group as displayed. Use the following excerpts from a sample main.cf as an example for your configuration.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"
.
.
.


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 = "255.255.240.0"
        )
```

9 To manually configure the MultiPrivNIC resource, modify the main.cf file by adding MultiPrivNIC to the cvm group as displayed. Use the following excerpts from a sample main.cf as an example for your configuration.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"
.
.
.


group cvm (
      SystemList = { galaxy = 0, nebula = 1 }
      AutoFailOver = 0
      Parallel = 1
      AutoStartList = { galaxy, nebula }
      )
.
.
.


MultiPrivNIC multi_priv (
            Critical = 0
            Device@galaxy = {lan1 = 0, lan2 = 1}
            Device@nebula = {lan1 = 0, lan2 = 1}
            Address@galaxy = {"192.168.1.1" = 0,"192.168.1.2" = 0,"192.168.2.1" = 1}
            Address@nebula = {"192.168.1.3" = 0,"192.168.1.4" = 0,"192.168.2.2" = 1}
            NetMask = "255.255.255.0"
            )
.
.
.
.
```

10 Modify the CVM service group to monitor the cssd program that uses the Application resource.

```
Application cssd (
    Critical = 0
    StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
    StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline"
    MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
    CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
    )
```

11 Revise the dependencies section for the CVM group. For example, you must add the dependencies that resembles:

```
cssd requires ocrvote_mnt
cssd requires ora_priv
ocrvote_mnt requires ocrvote_voldg
ocrvote_mnt requires vxfsckd
ocrvote_voldg requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Note: The above dependency example indicates a configuration where CRS_HOME and ORACLE_HOME are on local storage and the private IP address is configured under the PrivNIC resource. Alternatively, if you configure the private IP address under the MultiPrivNIC resource, the corresponding dependency will read as follows: `cssd requires multi_priv`.

---

12 Save and close the main.cf file.

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

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

14 Copy the saved main.cf file to all nodes in the cluster.

Starting VCS, CVM, and CFS on all nodes

With the configuration file in place on each node, start VCS, CVM, and CFS from each node using the following command:

```
# hastart
```

Verify that the resources are online on each node using the following command:

```
# hastatus
```

Verifying GAB port membership

After starting VCS, CVM, and CFS on each node, verify GAB port membership by running the `gabconfig -a` command.

The following is an example of this command and output:

```
# 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 v gen   ada416 membership 01
    Port w gen   ada418 membership 01
```

Setting up Oracle user equivalence

You must establish 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.

The sample procedure provides instructions for establishing user equivalence for RSH and RCP.

For oracle user, cluster node communications without password requirements must be set up. There are many methods available to set up this type of cluster node communication. The following procedure is offered only an example. Use a procedure appropriate to your configuration and systems.

To set up Oracle user equivalence for RSH and RCP

1. Open another terminal session as the Oracle user.
2. As the Oracle user on each system, edit the $HOME/.rhosts file and add entries similar to the following:

   ```
   galaxy oracle

   nebula oracle
   ```

3 On each system, log in as the Oracle user and set the password.

4 On each system, as user "oracle", verify "remsh" access:

```
$ remsh galaxy date

Mon Apr 24 10:02:45 PDT 2006

$ remsh nebula date

Mon Apr 24 10:02:45 PDT 2006
```

Editing the Oracle user profile

Perform this step only if you plan to install Oracle RAC manually.

Edit the Oracle user `.profile` file to set the paths to ORACLE_BASE, CRS_HOME, and ORACLE_HOME on each node.

In the following sample procedure, `ksh` is the shell environment and the Oracle user home directory is `/home/oracle`.

To edit the Oracle user profile

1 As the Oracle user, set the proper environment variables on each node:

```
$ export ORACLE_BASE=/app/oracle
$ export ORACLE_HOME=/app/oracle/orahome
$ export CRS_HOME=/app/crshome
$ export LIBPATH=$ORACLE_HOME/lib:$ORACLE_HOME/lib32:$CRS_HOME/\
  lib:$CRS_HOME/lib32:/usr/lib:/lib
$ export PATH=$PATH:$CRS_HOME/bin:$ORACLE_HOME/bin
$ export CLASSPATH=$CLASSPATH:$ORACLE_HOME/JRE:$ORACLE_HOME\
/jlib:$ORACLE_HOME/rdbms/jlib:$ORACLE_HOME/network/jlib
```

2 Verify the profile changes:

```
$ . /home/oracle/.profile
```

Chapter 10

Installing Oracle RAC

This chapter includes the following topics:

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.

Before you start the installation:

- Keep the Oracle worksheets handy as you perform the installation tasks.
  See "Oracle RAC Worksheets" on page 432.
- Review your Oracle installation manuals and the appropriate Oracle support websites for additional information and guidelines required during the installation of Oracle Clusterware and Oracle RAC database binaries using the Oracle Universal Installer.

When you install Oracle, do not create a database or install a pre-created database. For example, when you choose to use the **Enterprise Edition** or the **Standard Edition** displayed by the Oracle installer, select the **Software only** option to install the binaries without creating a database. If you choose **Custom installation**, do not create a database when prompted. Create the database after installing Oracle and relinking the SF Oracle RAC libraries to Oracle.

Installing Oracle Clusterware using the installsfrac program

You need to set the Oracle environment variables before you start the Oracle Clusterware installation. You can set the environment variables using the installer. After setting the environment variables, the installer invokes the Oracle Universal Installer (OUI) to start the Oracle Clusterware installation.

Note: If you want to pass any arguments to the Oracle installer, then set up the OUI_ARGS environment variable. You must perform this step before you start the SF Oracle RAC configuration program.

Refer to the Oracle documentation for details on the arguments that you can pass to the Oracle installer.

For example: `# export OUI_ARGS=-ignoreSysPrereqs`

To set the Oracle environment variables

1. Launch the SF Oracle RAC configuration program.

   ```
   # ./installsfrac [-rsh] -configure
   ```

   After launching the SF Oracle RAC configuration program, the copyright, license, and log information will be displayed. The system will initialize and a license check will be performed.

   After launching the SF Oracle RAC configuration program, the following general information and options are displayed. Select option 4, Install or relink Oracle.

2. The next configuration screen prompts you to check the supported SFRAC matrix for supported Oracle releases and patches. After checking the SFRAC matrix, proceed to the next step by pressing [RETURN].

3. Select an Oracle version for your installation.

4. Choose the Oracle task. Select option 1 to install Oracle Clusterware.

5. Set the DISPLAY environment variable that is required for the Oracle Universal Installer (OUI). Enter an IP address in the specified format.

   For example:

   ```
   Enter DISPLAY environment variable: [b] 10.20.12.150:0.0
   ```

6. Enter the Oracle UNIX user name. Select the default option (oracle).

   The Oracle UNIX user name was previously set up:

7. Enter Oracle UNIX group name. Select the default option (oinstall).

   The Oracle UNIX group name was previously set up:

8. Enter the absolute path of the Oracle Clusterware install image. After entering the absolute path, press [Return] to proceed.

   For example:

   ```
   /cdrom/Oracle11g/clusterware
   ```

9. Enter the location of the Oracle base directory.

   In this example, enter /app/oracle.

10 Enter the absolute path of Oracle Clusterware Home directory.

In this example, enter /app/crshome.

If the Oracle Clusterware home directory you specified does not exist, then the SF Oracle RAC configuration program provides the following guidelines and commands to create one.

```
This step will create a directory on all cluster nodes.

mkdir -p /app/crshome
chown -R oracle:oinstall /app/crshome
chmod -R 744 /app/crshome

Run above command on all systems?  [y,n,q, b]
```

If necessary, run the above commands and then enter the absolute path. Proceed to the next step.

11 Confirm your configuration information.

The displayed configuration information below is for a sample Oracle RAC 11g installation.

```
Veritas Storage Foundation for Oracle RAC 5.0MP3 Configuration Program

Oracle Unix User: oracle
Oracle Unix Group: oinstall
Oracle Clusterware (CRS) Installation Path:

/cdrom/Oracle11g/clusterware

Oracle Clusterware (CRS) Home: /app/crshome
Oracle Release: 11.1
Oracle Base: /app/oracle

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

12 After confirming the configuration information by entering " y", the SF Oracle RAC configuration program displays the following information:

```
CRS INSTALLATION
ORACLE CRS Installer will be invoked...................Please wait
```

13 The Oracle Universal Installer Welcome GUI then appears. Press "Next" to proceed.

Note: Consult your Oracle documentation for any required information for the Oracle RAC installation, and for directions on how to install Oracle Clusterware using the Oracle GUI interface.

Installing Oracle Clusterware

If you choose the **Install Oracle Clusterware (CRS)** option in the SF Oracle RAC configuration program, then after you set the Oracle RAC environment variables, the configuration program launches the Oracle Universal Installer (OUI).

The OUI installs Oracle Clusterware.

Note: You must set the Oracle RAC environment variables before starting the Oracle Clusterware installation process.

Make sure any required HP-UX patches listed in the Oracle documentation are installed before you install the Oracle Clusterware software. You must install Oracle Clusterware in the $CRS_HOME location on each node that you created.

Proceed to install Oracle Clusterware for your Oracle RAC installation:

To install Oracle Clusterware for an Oracle RAC installation

1. Set the Oracle RAC environment variables as described in the previous section using the SF Oracle RAC configuration program. The SF OracleRAC configuration program then launches the Oracle Universal Installer (OUI) to install Oracle Cluserware.

2. Proceed to follow the directions from the Oracle Universal Installer GUI. As you run the OUI, be prepared with the following information required for the installation and configuration of the Oracle Clusterware component.

Full path of the inventory directory	/oracle/oraInventory
Operating System group name	oinstall
Enter a name for the installation	CRS_HOME
Full path where you want to install the product	/app/crshome

3. You will be prompted for Product-Specific Prerequisite Checks.

   The Oracle installer verifies that your environment meets all of the minimum requirements for installing and configuring. 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.

4. The Oracle Universal Installer displays the cluster and the nodes to be managed by the Oracle Clusterware. Verify the displayed information. For each node verify the name for the public IP address, the name for the private interconnect, and the name for the virtual IP address on the node.

5. The Oracle Universal Installer displays the node's network interfaces. You will need to identify the planned use for each interface: Public, Private, or Do Not use.

   Private interfaces are used by Oracle Clusterware for inter-node traffic.

6. You will need to specify the Oracle Cluster Registry (OCR) location. The Oracle Cluster Registry (OCR) stores cluster and database configuration information. You need to specify a cluster file system or a shared raw device containing at least 256 MB of free space that is accessible from all of the nodes in the cluster.

   For example:

   - OCR location (if created on CFS): /ocrvote/ocr

- OCR location (if created on shared raw volumes): /dev/vx/rdsk/ocrvotedg/ocrvol

External redundancy must be selected for this option.

Note: Mirroring is performed by Volume Manager.

---

7 You will need to specify the voting disk location

The Oracle Clusterware voting disk contains cluster membership information and arbitrates cluster ownership among the nodes of your cluster in the event of network failures. You must specify a cluster file system file or a shared raw device that is accessible by the same name from all of the nodes in the cluster. The Oracle Universal Installer requires at least 256 MB of free space for the voting disk that it creates.

For example:

- Voting disk Location (if created on CFS): /ocrvote/vote
- Voting disk Location (if created on shared raw volumes): /dev/vx/rdsk/ocrvotedg/votevol

---

Note: External redundancy must be selected for this option.

---

8 The Oracle Universal Installer then presents a summary for the Oracle Clusterware and begins the Oracle Clusterware installation.

9 You will then be prompted to execute the following configuration scripts.

- /app/oracle/oraInventory/orainstRoot.sh
- /app/crshome/root.sh

10 For Oracle RAC versions 10.2.0.3 and earlier, patch the init.cssd script before you run the root.sh script.

Note: You do not need to patch the init.cssd script for Oracle RAC versions 10.2.0.4 and later.

- 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
```

Note: The orainstRoot.sh script must be run before running the root.sh script.

Log in as superuser and run the /app/crshome/root.sh script.

11 After running the configuration scripts on all the nodes in your cluster, a status message is displayed on your terminal.

For an example of the end of the status message:

```
Cluster Synchronization Services is active on all the nodes.
Waiting for the Oracle CRSD and EVMD to start.
Oracle CRS stack installed and running init (1M)
Running vipca (silent) for configuring nodeapps
Creating VIP application resource on (2) nodes...
Creating GSD application resource on (2) nodes...
Creating ONS application resource on (2) nodes...
Done
```

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
```

---

12 The Oracle Configuration Assistants GUI appears next to configure and start components previously selected.

13 At this point, the Oracle Universal Installer informs you that the Oracle Clusterware installation was successful.

Installing Oracle RAC database binaries

After installing the Oracle Clusterware component, install the Oracle RAC database binaries.

Review the procedure to install the Oracle RAC software in an SF Oracle RAC environment. Symantec recommends you to install Oracle binaries locally on each node.

Note: For specific information on how to install Oracle, refer to your Oracle documentation.

Note: Make sure any required HP-UX patches listed in the Oracle documentation are installed before you install the Oracle software. Follow the Oracle Universal Installer wizard instructions and complete the installation.

To install Oracle database binaries for Oracle RAC

1. Return to the SF Oracle RAC configuration program, navigate to the main menu, and select option 2 or the **Install Oracle RDBMS server** option.
2. Set the DISPLAY environment variable that is required for the Oracle Universal Installer.

   Enter an IP address in the specified format.
3. Enter Oracle UNIX user name. Select the default option (oracle).

   The Oracle UNIX user name was previously set up:
4. Enter Oracle UNIX group name. Select the default option (oinstall).

   The Oracle UNIX group name was previously set up:
5. Enter absolute path of the Database install image.

   For example:

   ```
   /cdrom/Oracle11g/database
   ```
6. Enter the location of the Oracle base directory.

   For example: /app/oracle
7. Enter absolute path of Oracle Clusterware Home directory.

   For example: /app/crshome

   If the directory does not exist, the SF Oracle RAC will prompt you to create it and creates it for you by running a set of displayed commands.

8 Enter absolute path of Database Home directory.

For example: /app/oracle/orahome

If the directory does not exist, the SF Oracle RAC will prompt you to create it and will create it for you by running a set of displayed commands.

Note: The absolute path entered above is only used for a clean installation of Oracle RAC 11g. If upgrading from an earlier version of Oracle RAC, then a different absolute path must be used for this step.

---

9 The SF Oracle RAC configuration program then displays the configuration information for verification. Confirm your configuration information.

After reviewing and approving this information the Oracle Universal Installer (OUI) is started.

10 The SF Oracle RAC installer invokes the Oracle Universal Installer (OUI) for Database Software Installation.

Note: Consult your Oracle documentation for any required information, and for information about installing the Oracle database software using the Oracle interface.

---

11 From the OUI and for a basic installation, review and approve the various installation locations (Oracle Base and Oracle Home).

12 From the OUI, select the nodes in the hardware cluster where the OUI will install the software.

At this point in the installation process, the OUI runs a product specific prerequisite check. Any items that are flagged must be manually checked and configured.

13 From the OUI, specify the install locations for Oracle Base and software location.

14 When the OUI presents the Select Configuration Option screen, select the **Install Software only** option.

Note: Symantec recommends that you create the database later.

When the OUI presents the Privileged Operating System Groups screen, make any adjustments required for your configuration and select Next to proceed with the installation.

15 The OUI then presents a summary for the Oracle Database and begins the Oracle Database installation.

16 You will then be prompted to execute configuration script. The following script must be executed on your cluster nodes:

- /app/oracle/orahome/root.sh

17 To execute the configuration script, perform the following steps:

First, open a terminal window.

Next, log in as "root" and run the scripts in each cluster node.

Finally, return to the GUI window and click "OK" to continue.

Note: Do not run the scripts simultaneously on your cluster nodes.

After running the script, return to the OUI and the Execute Configuration Script screen and select OK.

18 The OUI will display an End of Installation screen for the Oracle Database installation process.

19 Before proceeding to relink Oracle, verify the Oracle Clusterware and database installation:

See “Verifying the Oracle Clusterware and database installation” on page 231.

20 After the Oracle Database installation process, the SF Oracle RAC configuration program will prompt you to link Oracle with the SFRAC libraries.

You must link Oracle and enable Oracle to use the Veritas ODM and cluster membership (VCSMM) libraries. Enter yes to the SF Oracle RAC configuration program prompt to proceed with this process.

For example:

```
You must link Oracle with SFRAC libraries in order to
complete Oracle installation. Do you wish to
link Oracle now? [y,n,q] (y)
```

Note: Symantec recommends you to relink the SF Oracle RAC libraries only after completing all the required patch additions.

---

21 Proceed to create the Oracle database:

See “Creating the Oracle RAC database” on page 237.

Installing Oracle Clusterware manually

Using the Oracle RAC runInstaller, install the Oracle Clusterware software component as described in the following procedure.

Note: For an Oracle RAC 11g installation, refer to the Oracle Clusterware Installation Guide 11g Release 1 (11.1) for HPUX B28259-05 for additional information. Make sure that any required HP-UX patches listed in the Oracle documentation are installed before you install the Oracle Clusterware software. In addition:

Installing the Oracle Clusterware

1. On the first system, insert the Oracle Clusterware for HP-UX disk in the DVD drive, and enter the following commands:

   ```
   # nohup /usr/sbin/pfs_mountd &
   ```

   ```
   # nohup /usr/sbin/pfsd &
   ```

2. If the software disc is not mounted, mount it by entering:

   ```
   # /usr/sbin/pfs_mount -t rrip /dev/dsk/c#t#d# /cdrom
   ```

   Where c#t#d# is the location of the CD-ROM drive.

3. Log in as the Oracle user. On the first node, set the DISPLAY variable.

   - For Bourne Shell (bash), type:

     ```
     $ DISPLAY=host:0.0 export DISPLAY
     ```

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

     ```
     $ setenv DISPLAY host:0.0
     ```

4. On the first system, run the Oracle Universal Installer:

   ```
   $ cd /dvd_mount
   ```

   ```
   $ ./runInstaller
   ```

5 As you run the installer, be prepared with the following information required for the installation and configuration of the Oracle Clusterware component:

Specify File Locations dialog box	The installation destination ($CRS_HOME) on each node. For example: /app/crshome.
Cluster Configuration dialog box	The names of the nodes and their associated host names. In this Oracle Clusterware example installation, the nodes and their associated host names are galaxy and nebula.
Private Interconnect Enforcement dialog box	The private NIC IP addresses you have set up for each node. For example: lan1 on subnet 1.0.0.0.
Oracle Cluster Registry dialog box	The name of a raw volume for storing Oracle Cluster Registry. For an example of the name of ocr volume: /dev/vx/rdsk/ocrvotedg/ocrvol
Voting Disk dialog box	The name of a raw volume for storing voting disk. For an example of the name of voting volume: /dev/vx/rdsk/ocrvotedg/votevol

6 When you arrive at the Install screen, click **Install**.

7 Follow the wizard instructions to install Oracle Clusterware. After completing the pre-requisite 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.

8 The installer prompts you to run the orainstroot.sh and root.sh script.

9 Run the /oracle/oraInventory/orainstRoot.sh script on each node.

10 When the installer prompts you to run the root.sh script, run the root.sh script on each cluster node.

For Oracle RAC 10g, before you run the root.sh script, you need to add the init.cssd. patch. To add the init.cssd. patch:

- 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
  ```

Log in as superuser to run the root.sh script. For an example of the commands to run the root.sh script:

```
# cd $CRS_HOME

# ./root.sh
```

This starts the CRS daemons on the node where you enter the command.

11 After running the configuration scripts on all the nodes in your cluster, a status message is displayed on your terminal. For an example of the end of the status message:

```
Cluster Synchronization Services is active on all the nodes.
Waiting for the Oracle CRSD and EVMD to start.
Oracle CRS stack installed and running init (1M)
Running vipca (silent) for configuring nodeapps
Creating VIP application resource on (2) nodes...
Creating GSD application resource on (2) nodes...
Creating ONS application resource on (2) nodes...
Done
```

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
```

---

12 The Oracle Configuration Assistants GUI appears next to configure and start components previously selected.

13 At this point, the Oracle Universal Installer informs you that the Oracle Clusterware installation was successful.

Installing Oracle RAC binaries manually

Follow the procedure described below to install the Oracle RAC binaries in an SF Oracle RAC environment. Symantec recommends that you install the Oracle binaries locally on each node.

Before you install the Oracle software, make sure that you follow the directions to prepare to store the Oracle binary and data files:

See "Preparing to store the Oracle RAC database binaries" on page 199.

Before you install the Oracle software, make sure that any required HP-UX patches listed in the Oracle documentation are installed. In addition:

Follow the Oracle Universal Installer wizard instructions and complete the installation. Refer to your Oracle documentation for specific information on how to install Oracle.

Installing Oracle RAC binaries

1. On the first system and as oracle user, run the Oracle utility runInstaller.

   With the Oracle Enterprise Edition CD disc in the CD-ROM drive, enter:

   ```
   $ cd /cdrom
   $ ./runInstaller
   ```

2. As you run the installer, be prepared to provide the following information required for the installation and configuration of the Oracle RAC binaries component:

Specify File Locations dialog box	The installation destination ($ORACLE_HOME) on each node. For example: /app/oracle/orahome
Specify Hardware Cluster Installation Mode dialog box	The names of the nodes and their associated host names. In this Oracle example installation, the nodes and their associated host names are galaxy and nebula.

3. When you come to the Select Database Configuration dialog box, choose not to have a starter database created.

   Click **Do not create a starter database**.

   Symantec recommends that you create a database later.

4. When you arrive at the Install screen, click **Install**.
5. Follow the wizard instructions to install the Oracle RAC binaries.
6. In the Setup Privileges Notice dialog box, click OK. The installer prompts you to run the root.sh script.
7. Run the root.sh script on each node. For example:

   ```
   # cd $ORACLE_HOME
   # ./root.sh
   ```

8. Complete the Oracle RAC installation
9. After installing Oracle RAC software, perform the post-installation tasks.

Verifying the Oracle Clusterware and database installation

The following procedure verifies the Oracle Clusterware 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:

```
# $CRS_HOME/bin/crs_stat -t
```

Verify in the command output that the Oracle Clusterware processes are online on the nodes:

```
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
```

To verify the Oracle RAC database installation, check the oraInventory logs at `/app/oracle/oraInventory/logs/` (/app/oracle is the ORACLE_BASE directory).

Completing Oracle RAC post-installation tasks

Perform the following tasks after installing the Oracle RAC software:

- Adding Oracle RAC patches or patchsets
- Configuring the CSSD resource
- Relinking the SF Oracle RAC libraries with Oracle RAC using the installer
- Creating the Oracle RAC database
- Adding Oracle UDP IPC private IP addresses to the init.ora file
- Preventing automatic database startup
- Configuring VCS service groups for Oracle RAC

Adding Oracle RAC patches or patchsets

Before installing any Oracle RAC patch or patchset software:

- Review the latest information on supported Oracle RAC patches and patchsets: http://entsupport.symantec.com/docs/280186

- You must have installed the base version of the Oracle RAC software.
- Review the notes that accompany the patch or patchset for instructions on installing them and performing the post-installation operations.

Use the following procedure to add Oracle RAC patches to your node if you have installed Oracle, but have not yet configured Oracle in your cluster.

Before installing Oracle RAC patches

1. Log in as oracle user.
2. On one node, create the directory where you intend to copy the Oracle RAC patch software.

   For example:

   ```
   $ mkdir /oracle/patch
   ```

   ```
   $ cd /oracle/patch
   ```

3. Copy all files included with the downloaded Oracle RAC patch software to the /oracle/patch.

   When you uncompress and untar the downloaded ZIP file, the software resides in a Disk1 directory.
4. On each node, edit the .rhosts file to provide the other node access to the local system during the installation.

   Place a "+ +" character in the first line of the file. You can remove this permission after the patch installation is complete.
5. Set the DISPLAY variable. Do one of the following:

Bourne Shell (sh or ksh)	`$ DISPLAY=host:0.0;export DISPLAY`
C Shell (csh or tcsh)	`$ setenv DISPLAY host:0.0`

6. Run the Oracle RAC runInstaller utility.

   ```
   $ $/ORACLE/patch/Disk1/runInstaller
   ```

7. Select products.xml from the /oracle/patch/Disk1/stage directory.

8 In the Node Selection dialog box, select all nodes for installation to install the patches on local disks of each node.

If you are installing Oracle RAC patches on a local file system, install the software by invoking the installer on each node, one node at a time.

9 Proceed with the installation.

10 Apply Oracle patchsets or Oracle bundled patches, as necessary.

If you apply an Oracle patchset to Oracle Clusterware, perform the following steps to patch the `init.cssd` script for Oracle RAC versions 10.2.0.3 and earlier before you run the `root<xxx>.sh` script.

Note: You do not need to patch the `init.cssd` script for Oracle RAC versions 10.2.0.4 and later.

- Log in as oracle user
- Change to the directory where you want to copy the patch. For Oracle 10g Release 2:

```
$ cd $CRS_HOME/install/patch<xxx>/css/admin
```

```
$ cp /opt/VRTSvcs/rac/patch/init.cssd-10gR2.patch init.cssd.patch
```

- Run the following command to install the patch:

```
$ patch < init.cssd.patch init.cssd
```

If you apply an Oracle bundled patch to Oracle Clusterware, perform the following steps to patch the init.cssd script before you run the postrootpatch.sh script:

- Log in as oracle user
- Change to the directory where you want to copy the patch. For Oracle 10g Release 2:

```
$ cd $CRS_HOME/css/admin
```

```
$ cp /opt/VRTSvcs/rac/patch/init.cssd-10gR2.patch init.cssd.patch
```

- Run the following command to install the patch:

```
$ patch < init.cssd.patch init.cssd
```

11 After installing the Oracle RAC patches, you must relink the SF Oracle RAC libraries to Oracle.

Configuring the CSSD resource

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.

To configure the CSSD resource

1 Add the cssd resource to the cvm group:

```
# hares -add cssd Application cvm
```

2 Modify the cssd resource attributes:

```
# hares -modify StartProgram /opt/VRTSvcs/rac/bin/cssd-online
# hares -modify StopProgram  /opt/VRTSvcs/rac/bin/cssd-offline
# hares -modify MonitorProgram /opt/VRTSvcs/rac/bin/cssd-monitor
# hares -modify CleanProgram /opt/VRTSvcs/rac/bin/cssd-clean
```

3 Enable the cssd resource:

```
# hares -modify enabled 1
```

4 Set the dependency of the cssd resource on the CFSMount or CVMVolDg resources that manage OCR and voting disk:

```
# hares -link cssd ocrvote_mnt
```

5 Set the dependency of the cssd resource on the PrivNIC or MultiPrivNIC resources that manage the private IP address for Oracle Clusterware:

```
# hares -link cssd ora_priv
# hares -link cssd multi_priv
```

Relinking the SF Oracle RAC libraries with Oracle RAC using the installer

If you added or upgraded the Oracle patches, you must relink the SF Oracle RAC libraries to Oracle. You must link Oracle with the Veritas cluster membership (VCSMM) libraries and enable Oracle to use the Veritas ODM. For Oracle RAC 10g, the Veritas skgxp library will be used by default for cache fusion after relinking. For Oracle RAC 11g, Oracle UDP IPC is used for cache fusion.

You can relink the libraries using the SF Oracle RAC configuration program.

Note: Symantec recommends you to relink the SF Oracle RAC libraries only after completing all the required patch additions.

Relinking Oracle

1. Review the information from the configuration program, and press RETURN to continue.
2. Enter Oracle UNIX user name. Select the default option (oracle).

   The Oracle UNIX user name was previously set up:

3. Enter Oracle UNIX group name. Select the default option (oinstall).

   The Oracle UNIX group name was previously set up:

4. Enter the location of the Oracle base directory.

   In this example, enter /app/oracle.
5. Enter absolute path of CRS Home directory.

   In this example, enter /app/crshome.
6. Enter absolute path of Database Home directory.

   In this example, enter /app/oracle/orahome.

7. The SF Oracle RAC configuration program then displays the configuration information for verification.

   After reviewing and approving this information the Oracle relinking process is started.

   After the Oracle relinking process is finished, the SF Oracle RAC configuration screen appears. Enter q to quit the program.

   The configuration program links Oracle with Veritas libraries on each cluster node.

   Note: Copy the location of the installsfrac log files. If necessary, these log files can be used for troubleshooting purposes.

   ---

8. Proceed to create the Oracle RAC database:

   See "Creating the Oracle RAC database" on page 237.

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_database_grp -sys system_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 5.0 ODM Library,
   Version 5.0
   ```

   Additionally, for Oracle RAC 10g, verify that the cluster interconnect IPC version is `VERITAS IPC '5.0.31.0'`.

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.

You can relink the libraries using the SF Oracle RAC configuration program.

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 to Oracle RAC 10g, run the following command as oracle user:

```
$ /opt/VRTSvcs/rac/bin/linkrac 10gR2
```

To relink the SF Oracle RAC libraries to Oracle RAC 11g, run the following command as oracle user:

```
$ /opt/VRTSvcs/rac/bin/linkrac 11gR1
```

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 the Oracle RAC database, see the Oracle RAC documentation.

For information about creating a test database:

See "About creating a test database" on page 481.

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.

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 init.ora file" on page 237.

Adding Oracle UDP IPC private IP addresses to the init.ora file

This procedure is applicable to both Oracle RAC 10g and Oracle RAC 11g.

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. You need to configure the `cluster_interconnects` parameter in the Oracle `init.ora` file to use the appropriate private IP addresses.

Additionally, you must remove the`cluster_interconnect` entry from OCR using the following command:

```
$ oifcg delif -global if_name
```

Note: When you use PrivNIC or MultiPrivNIC to provide high availability to the private IP addresses used for database cache fusion, do not use the `cluster_interconnects` parameter to load balance the interconnect traffic across multiple physical links (by setting multiple IP addresses in the `cluster_interconnects` parameter). Using the parameter for load balancing results in loss of high availability to the private interconnects.

To add Oracle UDP IPC private IP addresses to the init.ora file

1. For Oracle RAC 10g: Unlink the Veritas IPC library:
   - 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
     ```

   - Unlink Veritas IPC library:
     Change to the directory `$ORACLE_HOME/rdms/lib` and run the following commands on one of the nodes in the cluster (if the directory is on shared storage) or on all nodes (if the directory is on local storage):

     ```
     $ make -f ins_rdbms.mk rac_on
     $ make -f ins_rdbms.mk ioracle
     ```

   - Restart Oracle database:

     ```
     $ srvctl start database -d db-name
     ```

2. Log in to each system as the root user.
3. If the private interface has already been configured, delete the interface by removing the cluster_interconnect entry from OCR using the following command:

   ```
   # oifcfg delif -global if_name
   ```

   For more information on the command, see the Oracle RAC documentation.

4 Log in to each system as the Oracle user.

5 Set the `cluster_interconnects` parameter in the `spfile/init.ora` file to use the Oracle UDP IPC private IP addresses that are used for database cache fusion and are managed by PrivNIC or MultiPrivNIC.

```
$ sqlplus '/ as sysdba'

SQL> alter system set cluster_interconnects='192.168.1.1
scope=spfile sid='vrts1'

SQL> alter system set cluster_interconnects='192.168.1.2
scope=spfile sid='vrts2'

SQL> exit;
```

6 Restart the database for the changes to take effect.

7 As root user, 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 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. Symantec recommends that the Oracle database be always configured under VCS.

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.

Note: In a setup with multiple databases, you must configure the database under VCS. The configuration without the VCS Oracle agent may be used only in single database setups.

Figure 10-1 illustrates a service group configuration with the VCS Oracle agent.

Figure 10-1 Service group configuration with the VCS Oracle agent

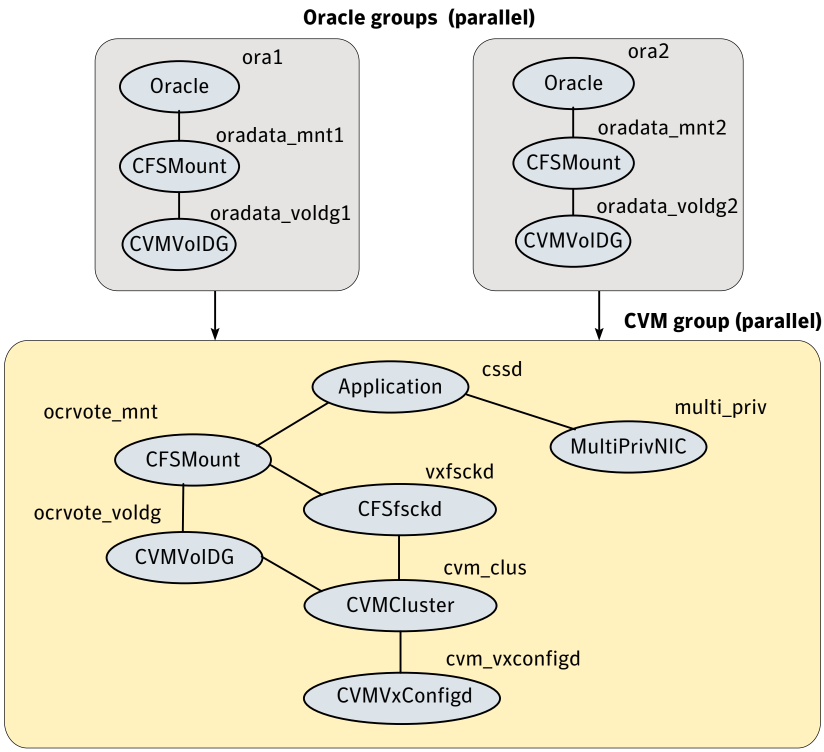
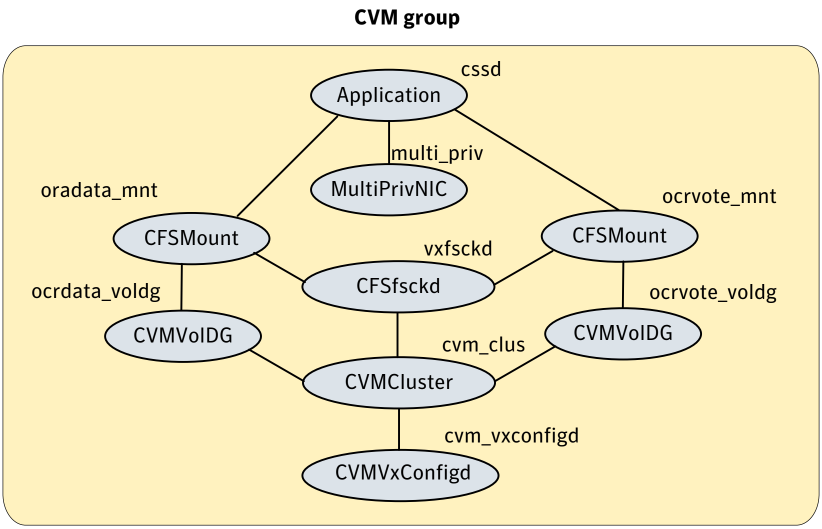


Figure 10-2 illustrates a service group configuration without the VCS Oracle agent.

Figure 10-2 Service group configuration without the VCS Oracle agent



To configure the Oracle database under VCS, create Oracle service groups after installing Oracle RAC and creating a database.

You can create Oracle service groups by modifying the VCS configuration file in one of the following ways:

- Edit the main.cf file
  See "Editing the main.cf file to configure VCS service groups for Oracle RAC" on page 242.
- Use the CLI
  See "Using the CLI to configure VCS service groups for Oracle RAC" on page 244.

Editing the main.cf file to configure VCS service groups for Oracle RAC

This section describes how to manually edit the `/etc/VRTSvcs/conf/config/main.cf` file to configure VCS service groups for Oracle RAC.

Note: Before you edit the main.cf file, change the permissions on the VCS configuration file:`#` **`haconf -makerw`**

You need to perform the steps in the following procedures:

- To configure VCS service groups for Oracle RAC

■ To start VCS after modifying the configuration file

To configure VCS service groups for Oracle RAC

1 Log in as the root user to one of the systems.

2 As root user, save your existing configuration before you modify main.cf:

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

If the configuration is not writable, a warning appears: "Cluster not writable." You may safely ignore the warning.

3 Stop the VCS engine on all systems and leave the resources available:

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

4 Back the `main.cf` file:

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

```
# cp main.cf main.orig
```

5 Using `vi` or another text editor, edit the main.cf file to add the Oracle service groups.

Use the sample configuration files in the appendix as a guideline.

6 Save and close the main.cf file.

7 Verify the syntax of the file :

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

```
# hacf -verify .
```

For additional information and instructions on modifying the VCS configuration by editing the main.cf file:

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

Starting VCS after modifying the configuration file

You need to start VCS for the new configuration to take effect.

To start VCS after modifying the configuration file

1. Start VCS on one of the systems and check its status:

   ```
   # hastart
   ```

   ```
   # hastatus
   ```

2. When "`LOCAL_BUILD`" is listed in the message column, start VCS on the other systems:

   ```
   # hastart
   ```

3. On one of the systems, enter the following command to verify that the service groups for Oracle RAC are brought online:

   ```
   # hagrp -display
   ```

4. Check the status of the groups.

   ```
   # hagrp -state
   ```

5. Check the status of the resources.

   ```
   # hares -state
   ```

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 resourcefor 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 User'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.

Chapter 11

Upgrading Oracle RAC and migrating the database

This chapter includes the following topics:

Supported upgrade paths

Table 11-1 lists the upgrade paths for Oracle RAC.

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

Note: When you upgrade to a different version of Oracle RAC, make sure that the full path of the Oracle RAC 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 5.0.1
- A supported version of the operating system

Upgrading Oracle RAC

Upgrading Oracle RAC involves the following steps:

- Depending on whether you are upgrading from Oracle RAC 10g or Oracle RAC 9i, complete the preparatory steps described in one of the following sections:
  See "Preparing to upgrade from Oracle RAC 10g " on page 248.
  See "Preparing to upgrade from Oracle RAC 9i" on page 249.
- Install target version of Oracle RAC binaries, including patchsets if required.
  Upgrading Oracle RAC binaries
- Migrate the database.
  Migrating the Oracle RAC database
- Relink the Oracle RAC libraries with SF Oracle RAC.
  Performing post-upgrade tasks

Preparing to upgrade from Oracle RAC 10g

Perform the following pre-upgrade tasks before upgrading from Oracle RAC 10g (Release 1 or Release 2) to Oracle RAC 11g Release 1.

To prepare for upgrade from Oracle RAC 10g

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
   - Edit VCS configuration file for additional resources
   - Start VCS, CVM, and CFS on all nodes
   - Verify GAB port membership
   - Set up Oracle user equivalence
   - Edit the Oracle user profile

   For instructions on performing the tasks:

   See "About preparing to install Oracle RAC" on page 181.

Upgrading Oracle RAC binaries

Review your Oracle installation manuals and the appropriate Oracle support websites before upgrading Oracle RAC.

To upgrade Oracle RAC binaries

1. - If you are upgrading from Oracle RAC 9i to Oracle RAC 10g Release 2 or Oracle RAC 11g Release 1, install Oracle Clusterware.
     For instructions, see the Oracle RAC documentation.
   - If you are upgrading from Oracle RAC 10g (Release 1/Release 2), upgrade Oracle Clusterware.
     For instructions, see the Oracle RAC documentation.
2. Make sure that Oracle Clusterware for 11g Release 1 is running.
   - To list the software version of Oracle Clusterware:

     ```
     # $ORA_CRS_HOME/bin/crsctl query crs softwareversion
     ```

   - To list the operating version of Oracle Clusterware:

     ```
     # $ORA_CRS_HOME/bin/crsctl query crs activeversion
     ```

3. Install the Oracle RAC database.

   For instructions, see the Oracle RAC documentation.
4. Complete the following post-installation tasks:
   - Adding Oracle RAC patches or patchsets
     See “Adding Oracle RAC patches or patchsets” on page 231.
   - Relinking the SF Oracle RAC libraries with Oracle RAC
     For upgrades from Oracle RAC 9i:
     See “Relinking the SF Oracle RAC libraries with Oracle RAC manually” on page 236.
     For upgrades from Oracle RAC 10g:
     See “Relinking the SF Oracle RAC libraries with Oracle RAC using the installer” on page 234.
   - For upgrades from Oracle RAC 9i: Add the CSSD resource to the VCS configuration
     See “Configuring the CSSD resource” on page 234.

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 251.

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 init.ora file" on page 237.

4 Configure the Oracle RAC database for manual startup if you want the Oracle RAC database to be managed by VCS using the Oracle agent.

See "Preventing automatic database startup" on page 239.

5 Unfreeze the VCS service groups that were frozen earlier.

As root user, enter:

```
# hagrp -unfreeze oracle_group -persistent

# hagrp -unfreeze cssd_resource -persistent

# haconf -dump -makero
```

Section 4

Adding and removing SF Oracle RAC nodes

Chapter 12

Adding a node to SF Oracle RAC clusters

This chapter includes the following topics:

About adding a node to an SF Oracle RAC cluster

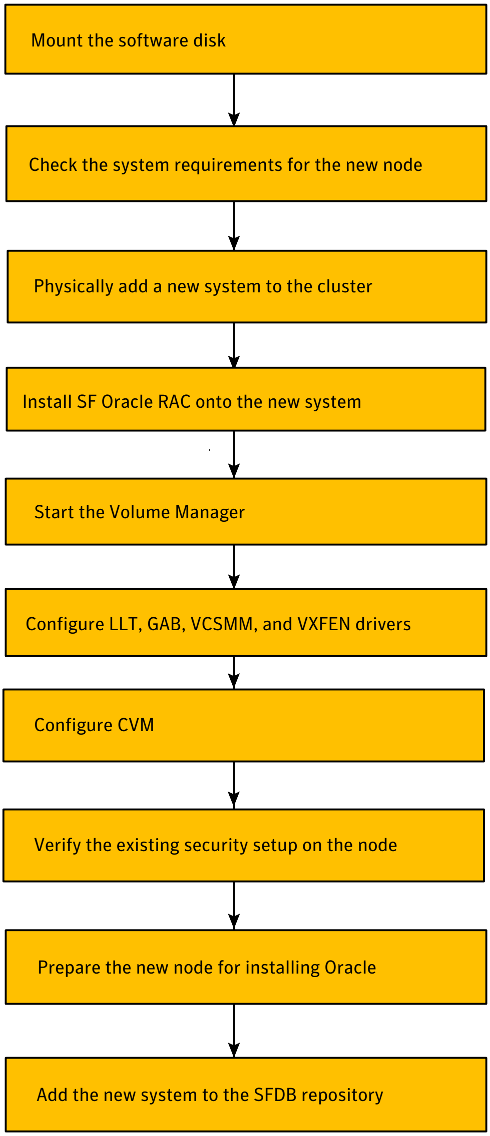
SF Oracle RAC enables you to add and remove nodes to an SF Oracle RAC cluster. An SF Oracle RAC cluster can have as many as eight nodes.

The sample procedures in this chapter describe how to add a node (saturn) to an existing cluster (rac_cluster101) with two nodes (galaxy and nebula).

Adding a node to an existing SF Oracle RAC cluster

Figure 12-1 displays the procedures required to add a node to an SF Oracle RAC cluster. Each step is discussed in detail in this chapter.

Figure 12-1 SF Oracle RAC add node procedures



The following procedures enable you to install SF Oracle RAC to a new node and add it to an existing cluster:

- Mounting the software disc
- Checking system requirements for new node

- Physically adding a new system to the cluster
- Installing Veritas Storage Foundation for Oracle RAC on the new system
- Starting Volume Manager
- Configuring LLT, GAB, VCSMM, and VXFEN drivers
- Configuring CVM
- Verifying the existing security setup on the node
- Preparing the new node for installing Oracle
- Adding the new system to the Storage Foundation repository database

Mounting the software disc

Make sure you have superuser (root) privileges to load the SF Oracle RAC software. You can use the mount command to mount the disc.

To navigate to the folder containing the installsfrac program

◆ Navigate to the /cdrom folder containing the installsfrac script:

```
# cd /cdrom/storage_foundation_for_oracle_rac
```

Checking system requirements for new node

Before installing the SF Oracle RAC software on the new node, you must verify that the new node meets the installation requirements.

Verify that the new nodes joining the cluster meet all of the requirements for installing and using SF Oracle RAC. In addition, the new system must have the identical operating system and patch level as the existing systems.

To check the new node for installation

1. Run the installsfrac program with the `precheck` option to verify the current operating system level, patch level, licenses, and disk space are adequate for a successful installation:

   ```
   # ./installsfrac -precheck saturn
   ```

   The `precheck` function of the utility proceeds without user interaction.

2. Upon completion, review as the utility displays the results of the verification and saves the results in a log file.

3. If the `precheck` function indicates a requirement for licensing, add the license when running the installation utility.

   The `precheck` function may prompt you for other requirements.

4. If the verification is successful, proceed to run installsfrac with the `-installonly` option.

Physically adding a new system to the cluster

The new system must have the identical operating system and patch level as the existing systems. When you physically add the new system to the cluster, make sure the node:

- Is connected to the same shared storage devices as the existing nodes.
- Has private network connections to two independent switches for the cluster.

Refer to the *Veritas Cluster Server Installation Guide*.

After installing SF Oracle RAC on the new system and starting VxVM, the new system can access the same shared storage devices (including coordinator disks). If the new system does not see the same disks as the existing nodes, the new system cannot join the cluster as a new node, as indicated by a CVM error on the console.

Installing Veritas Storage Foundation for Oracle RAC on the new system

Read the pre-installation instructions in this guide before proceeding.

See "About preparing to install and configure SF Oracle RAC" on page 59.

To install Veritas Storage Foundation for Oracle RAC without configuration

1. Log in as root on one of the systems for installation.
2. On the new node, you must use the `-installonly` option to install SF Oracle RAC without performing configuration. Install the Veritas Storage Foundation for Oracle RAC software as described previously in this guide, but run the product installation script instead of the generic installer script. You will configure the new node later using the configuration from the existing cluster nodes.

   Enter the following command from the top-level directory of the mounted disc

   ```
   # ./installsfrac -installonly [-rsh]
   ```

   The `-rsh` option is required if you are using the remote shell (RSH) rather than the secure shell (SSH) to install the software simultaneously on several systems. If remote shell (RSH) or secure shell (SSH) is configured correctly, you can run this command on a single node to install the software on all nodes in the cluster.
3. Enter the name of the new node.
4. After the script performs initial checks, confirm to start the installation.
5. Review the output as the script checks system licensing and installs the licensing package.
6. Enter the license key as the installer prompts.
7. Enter keys for additional product features such as VVR, if you want to set up a global cluster environment.
8. Review the output as the script lists the packages and patches to install and checks whether any of them are present on the node.
9. After the requirements checks are complete, press **Return** to start installing the packages. If you are installing multiple nodes, you have the option of simultaneously installing them. You will be prompted after the installation is complete.
10. After the script installs the packages, note the location of the summary, log, and response files in the output.
11. Ignore the message advising you to run `installsfrac -configure`.
12. Before proceeding to the following procedure, you must restart the new node.

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

Starting Volume Manager

As you run the utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installsfrac` utility.

To start Volume Manager

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 **y** when prompted to select enclosure-based naming for all disks if it is used on the existing nodes.

4. Decline to set up a systemwide disk group for the system by entering **n**. The installation completes.

5. 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, VCSMM, and VXFEN drivers

Proceed to configure the LLT, GAB, VCSMM, and VXFEN drivers.

To configure LLT, GAB, VCSMM, and VXFEN drivers

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/llttab 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/llttab 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 system. 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 If you are adding the new node to a single node cluster, then fencing must be enabled and configured on the original node before proceeding.

Note: For I/O fencing information, refer to the earlier section on Setting up I/O fencing.

---

7 If you are adding the new node to a cluster with more than one node, set up the /etc/vcsmmtab and /etc/vxfendg files on the new system by copying them from one of the other existing nodes:

```
# scp galaxy:/etc/vcsmmtab /etc

# scp galaxy:/etc/vxfendg /etc

# scp galaxy:/etc/vxfenmode /etc
```

8 Start LLT and GAB on the new node:

```
# /sbin/init.d/llt start

# sbin/init.d/gab start
```

9 On the new node, start the VXFEN, VCSMM, and LMX drivers. Use the following commands in this order:

```
# /sbin/init.d/vxfen start
```

```
# /sbin/init.d/vcsmm start
```

```
# /sbin/init.d/lmx start
```

10 On the new node, start the GMS and ODM drivers. Use the commands in the order shown:

```
# kcmodule vxgms=loaded
```

```
# kcmodule odm=loaded
```

```
# /sbin/init.d/odm stop
```

```
# /sbin/init.d/odm start
```

11 On the new node, verify that the GAB port memberships are a, b, d, and o. Run the command:

```
# /sbin/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
```

Configuring CVM

To prepare the new node for installing Oracle, you must configure CVM.

To configure CVM

1. To enable the existing cluster to recognize the new node, execute on one of existing nodes:

   ```
   # haconf -makerw

   # hasys -add saturn

   # hares -modify cvm_clus CVMNodeId -add saturn 2

   # haconf -dump -makero

   # /etc/vx/bin/vxclustadm -m vcs -t gab reinit

   # /etc/vx/bin/vxclustadm nidmap
   ```

2. Repeat the following step in the remaining existing cluster:

   ```
   # /etc/vx/bin/vxclustadm -m vcs -t gab reinit

   # /etc/vx/bin/vxclustadm nidmap
   ```

Verifying the existing security setup on the node

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 runing in a secure mode, proceed with configuring LLT and GAB.

See “Configuring LLT, GAB, VCSMM, and VXFEN drivers” on page 260.

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. Otherwise, proceed to configuring the authentication broker on node saturn.

   See “Configuring the authentication broker on the new node” on page 264.

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.

See "Setting up VCS related security configuration" on page 264.

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
```

Configuring the authentication broker on the new node

Configure a new authentication broker (AB) on node saturn. This AB belongs to root broker RB1.

To configure the authentication broker on new node

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
```

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
```

5 Verify that AB is configured properly.

```
# vssat showbrokermode
```

The command should return 1, indicating the mode to be AB.

Setting up VCS related security configuration

Perform the following steps to configure VCS related security settings.

Setting up VCS related security configuration

1. Start /opt/VRTSat/bin/vxatd process.
2. Create HA_SERVICES domain for VCS.

   ```
   # vssat createpd --pdrtype ab --domain HA_SERVICES
   ```

3. Add VCS 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
   ```

Adding a node in a VxSS group

Perform the following procedure when adding a node in a VxSS group.

Adding a node in a VxSS group

1. On one of the nodes in the existing cluster, set the cluster configuration to read-write mode:

   ```
   # haconf -makerw
   ```

2. Modify the SystemList and AutoStartList attributes of the group on the new node:

   ```
   # hagrp -modify VxSS SystemList -add saturn 2
   ```

   ```
   # hagrp -modify VxSS AutoStartList -add saturn
   ```

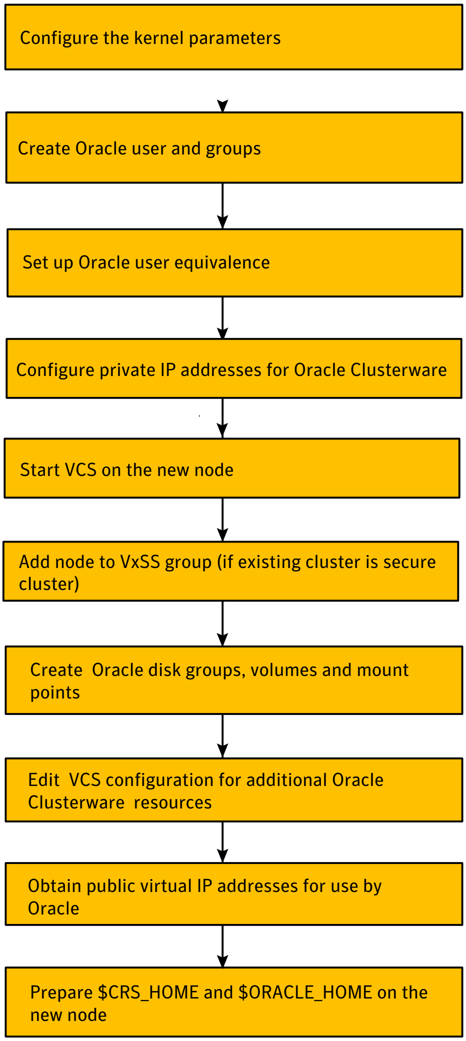
3. Change the cluster configuration to read only mode:

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

Preparing the new node for installing Oracle

Performing pre-installation operations for the new node involves both manual and automated tasks from the SF Oracle RAC configuration program. Figure 12-2 displays the tasks required to prepare the new node. Each task is discussed in detail in this section.

Figure 12-2 Preparing the new node for installing Oracle



Before installing Oracle RAC you must perform the following additional tasks:

- Configure the kernel parameters
- Creating Oracle user and groups
- Setting up Oracle user equivalence

After performing the above preparatory tasks for installing Oracle on a new node, then the following additional procedures must be performed:

Configure the kernel parameters

To prepare the new node for installing Oracle, you must configure the kernel parameters.

For complete instructions and guidelines, see the Oracle documentation.

Creating Oracle user and groups

To prepare the new node for installing Oracle, you must create the oracle user and groups.

Refer to the following section for information:

See "Creating Oracle user and groups" on page 187.

Setting up Oracle user equivalence

To prepare the new node for installing Oracle, you must set up Oracle user equivalence for rsh/ssh and rcp/scp.

Refer to the following section for information about rsh and rcp:

See "Setting up Oracle user equivalence" on page 212.

Configuring private IP addresses for Oracle Clusterware

To prepare the new node for installing Oracle, you must configure private IP addresses for Oracle Clusterware.

The Oracle Clusterware daemon requires a private IP address on each node to enable communications and heartbeating. Determine a private NIC device for which LLT is configured.

Access and view the file /etc/llttab. For example, if a device is used as an LLT interconnect on one system, you can configure an available IP address for it.

Table 12-1 below displays the required information to configure private IP addresses for Oracle Clusterware.

Table 12-1 Required information to configure private IP addresses for Oracle Clusterware

Required information	Example
On galaxy	192.168.12.1
On nebula	192.168.12.2
On saturn	192.168.12.7

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. Use the following commands to add private IP addresses to the ora_priv resource on one of the nodes in the existing cluster:

```
# haconf -makerw
# hagrp -modify cvm SystemList -add saturn 2
# hagrp -modify cvm AutoStartList -add saturn
# 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 "192.168.12.7" -sys saturn
# haconf -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:

   ```
   # hares -modify cssd Critical 0
   ```

2. Create the file `cssd-pretend-offline` on the new node:

   ```
   # touch /opt/VRTSvcs/lock/cssd-pretend-offline
   ```

3. Start VCS on the new node:

   ```
   # hastart
   ```

Creating Oracle disk groups, volumes and mount points

To prepare the new node for installing Oracle, you must create the Oracle disk groups, volumes, and mount points.

Refer to the following section for information:

See “Creating disk groups, volumes, and mount points for Oracle RAC” on page 196.

Editing VCS configuration for additional Oracle Clusterware resources

To prepare the new node for installing Oracle, you must edit the VCS configuration for additional Oracle Clusterware resources.

Refer to the following section for information:

See “Editing the VCS configuration file for additional Oracle Clusterware resources” on page 207.

Identifying the public virtual IP addresses for use by Oracle

To prepare the new node for installing Oracle, you must obtain the public virtual IP addresses for use by Oracle.

Refer to the following section for information:

See "Identifying the public virtual IP addresses for use by Oracle" on page 184.

Preparing $CRS_HOME and $ORACLE_HOME on the new node

To prepare the new node for installing Oracle, you must prepare $CRS_HOME and $ORACLE_HOME on the new node.

The local or cluster file system on shared storage should be the same as on the existing nodes.

Local file system for $CRS_HOME and $ORACLE_HOME

Follow the directions for the following procedures to prepare $CRS_HOME and $ORACLE_HOME on new node:

- Create a file system on local storage for Oracle/CRS binaries (/app):
- Prepare $CRS_HOME on the new node:
- Prepare $ORACLE_BASE on the new node:
- Prepare $ORACLE_HOME on the new node:

Identify the directories required for installing Oracle and CRS software.

Table 12-2 Required information $CRS_HOME on each system

Required information	Example
Disk on each node for Oracle and CRS for Oracle and CRS binaries	Disk 1
Disk group on each local storage	On saturn: orabindg_saturn
Volume for each local disk group	On saturn: orabinvol_saturn
File system on each local volume	vol_saturn /dev/vx/rdsk/orabindg_saturn/orabinvol_saturn
Mount point for each local file system	/app
Directory to install CRS	/app
Directory to install Oracle (ORACLE_HOME)	/app/oracle/orahome

To create a file system on local storage for Oracle/CRS binaries (/app)

1. As root user, first create a VxVM local diskgroup, orabindg_hostname:

```
# vxdg init orabindg_saturn Disk_1
```

2. Create a volume, orabinvol_hostname:

```
# vxassist -g orabindg_saturn make orabinvol_saturn 12G
```

3. Create directory, /app

```
# mkdir /app
```

4. Create a filesystem with this volume, orabinvol_hostname

```
# mkfs -V vxfs /dev/vx/dsk/orabindg_saturn/orabinvol_saturn
```

5. Mount /app:

```
# mount -V vxfs /dev/vx/dsk/orabindg_saturn/orabinvol_saturn /app
```

6. Add the following entry for this filesystem in the /etc/fstab file:

```
/dev/vx/dsk/orabindg_saturn/orabinvol_saturn \
/app vxfs delaylog 0 2
```

To prepare $CRS_HOME on the new node

1. On each system, log in as "root".
2. Create the directory for CRS_HOME:

```
# mkdir -p /app/crshome
```

3. Change ownership and permissions.

```
# chown -R oracle:oinstall /app/crshome
```

```
# chmod -R 744 /app/crshome
```

To prepare $ORACLE_BASE on the new node

1. On each system, log in as "root".
2. Create the directory for ORACLE_BASE:

```
# mkdir -p /app/oracle
```

3. Change ownership and permissions.

```
# chown -R oracle:oinstall /app/oracle
```

```
# chmod -R 744 /app/oracle
```

To prepare $ORACLE_HOME on the new node

1. On each system, log in as "root".
2. Create the directory for ORACLE_HOME:

```
# mkdir -p /app/oracle/orahome
```

3. Change ownership and permissions:

```
# chown -R oracle:oinstall /app/oracle/orahome
```

```
# chmod -R 744 /app/oracle/orahome
```

Cluster file system for $CRS_HOME and $ORACLE_HOME

◆ Create the Oracle base mount point:

```
# mkdir -p /app
```

Using the Oracle RAC add node procedures

For the Oracle RAC procedure for adding a node, refer to your Oracle documentation and the appropriate Oracle web sites. In this procedure, Oracle copies the CRS_HOME and ORACLE_HOME from an existing node in the cluster.

Note: After adding the new node to Oracle RAC, remove the file `cssd-pretend-offline` to start the monitoring of Oracle Clusterware using the CSSD agent.

After performing the Oracle add node procedure, you must relink Oracle binaries to the appropriate Veritas libraries for Oracle RAC.

Adding the new system to the Storage Foundation repository database

Add the new system to the Storage Foundation database repository using the following procedure.

Add the new system to the SFDB repository

1. Add the system using the following sequence of commands:

   ```
   # haconf -makerw
   ```

   ```
   # hagrp -modify Sfua_Base SystemList -add saturn
   ```

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

2. Copy the /etc/vx/vxdbed/ .odbc.ini file from and existing node to the new system. For example:

   ```
   # rcp /etc/vx/vxdbed/.odbc.ini saturn:/etc/vx/vxdbed
   ```

3. Run the following command:

   ```
   # dbed_update
   ```

Chapter 13

Removing a node from SF Oracle RAC clusters

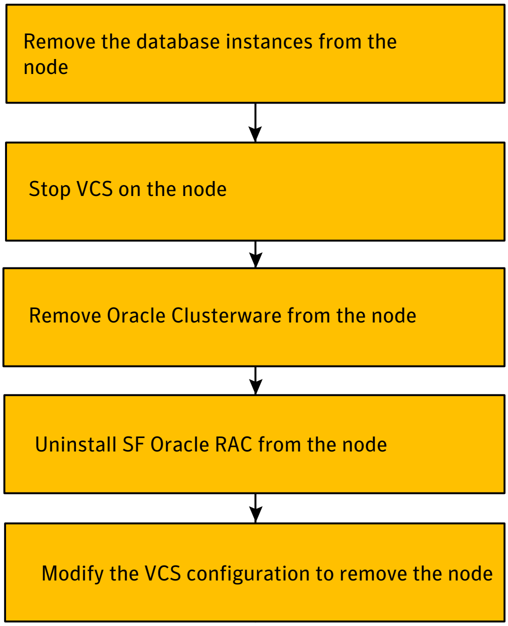
This chapter includes the following topics:

About removing nodes from an SF Oracle RAC 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.

Figure 13-1 illustrates the steps required to remove nodes from an SF Oracle RAC cluster.

Figure 13-1 Removing a node from an SF Oracle RAC cluster flowchart



Removing nodes from an SF Oracle RAC cluster

Perform the following steps to remove a node from an SF Oracle RAC cluster.

To remove a node from an SF Oracle RAC 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 under 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 [-rsh] 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 277.

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.

For an example main.cf:

See “Sample main.cf files for adding and removing nodes” on page 407.

The process involves:

- Editing the /etc/llthosts file
- Editing the /etc/gabtab file
- Modifying the VCS configuration to remove the node

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 te 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
- Use the command line interface

The following procedure uses the command line interface and modifies the sample group `group1` to remove references to the deleted node.

To modify the VCS configuration

1. Change the cluster configuration to read-write mode:

   ```
   # haconf -makerw
   ```

2. Back up the `/etc/VRTSvcs/conf/config/main.cf` file.

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

   ```
   # cp main.cf main.cf.3node.bak
   ```

3 Remove the node from the AutoStartList attribute of the service group by specifying the remaining nodes in the desired order:

```
# hagrp -modify group1 AutoStartList galaxy nebula
```

4 Remove the node from the SystemList attribute of the service group:

```
# hagrp -modify group1 Systemlist -delete saturn
```

5 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 3 and step 4 for each of them.

6 After deleting the removed node from all service groups in the configuration, delete the node from the cluster system list:

```
# hasys -delete saturn
```

7 Save the new configuration to disk:

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

Section 5

Configuring for disaster recovery

Chapter 14

Configuring a campus cluster for disaster recovery

This chapter includes the following topics:

About SF Oracle RAC campus cluster setup 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:

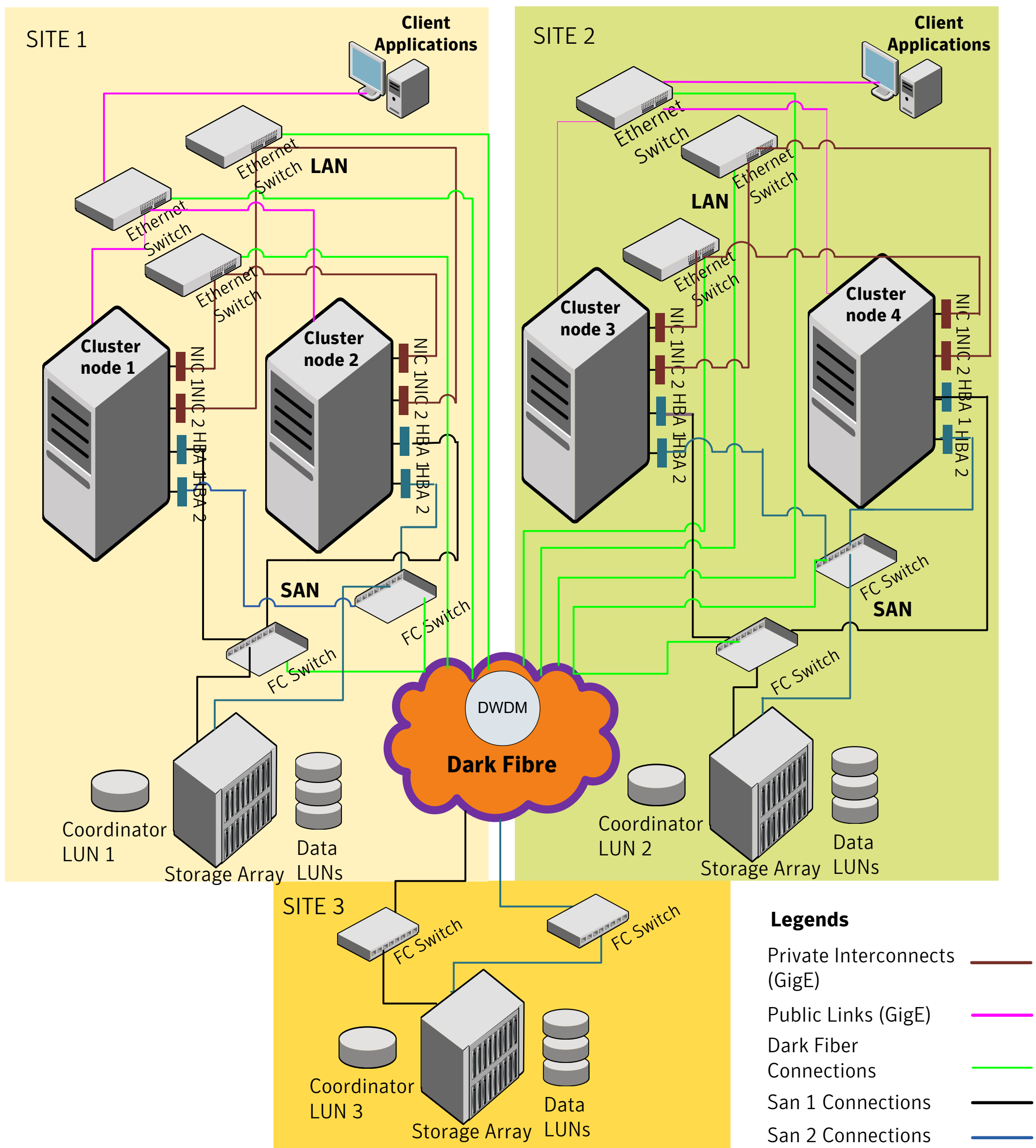
Latency challenges	An SF Oracle RAC campus cluster handles latency challenges in keeping mirrors synchronized while ensuring the efficient recovery in case of site failures for both data and VxVM metadata.

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. You can not use VCS firedrill on SF Oracle RAC campus clusters.

Figure 2-5 illustrates a basic campus cluster setup.

Figure 14-1 Basic campus cluster setup



About I/O fencing for campus clusters

You must configure I/O fencing to prevent corruption of shared data in the event of a network partition.

See "About membership arbitration" on page 286.

See "About data protection" on page 287.

In a campus cluster, the chances of network partition are high and it is essential to prevent data corruption with a robust I/O fencing implementation. There are two options:

- Two coordinator disks at one site and one coordinator disk at the other site.
  In this case, the site that has two coordinator disks has a higher probability to win the race. The disadvantage with this configuration is that if the site that has two coordinator disks encounters a site failure, then the other site also commits suicide.
- One coordinator disk at each of the two sites and a third coordinator disk at a third site.
  This configuration ensures that I/O fencing works even if one of the sites becomes unavailable. A coordinator disk in a third site allows at least one of the sub clusters to continue operations in the event of a site failure in a campus cluster. The site that can access the coordinator disk in the third site in addition to its local coordinator disk wins the race. However, if both the sites of the campus cluster are unable to access the disk at the third site, each site gains one vote and the nodes at both the sites commit suicide. With redundant network connectivity, this risk can be reduced significantly. Starting in release 5.0.1, SF Oracle RAC supports iSCSI LUNs as coordinator disks which provide a cheaper option for the coordinator disk at the third site, avoiding the need to extend the fiber connection to the third site.

The second configuration is recommended for an SF Oracle RAC campus cluster, as it ensures high availability of applications in the event of split brain scenarios.

About membership arbitration

Membership arbitration is necessary on a perceived membership change because systems may falsely appear to be down. When LLT on a system no longer receives heartbeat messages from another system on any configured LLT interface, GAB marks the system as DOWN. However, if the cluster interconnect network failed, a system can appear to be failed when it actually is not. In most environments when this happens, it is caused by an insufficient cluster interconnect network infrastructure, usually one that routes all communication links through a single point of failure.

If all the cluster interconnect links fail, it is possible for one cluster to separate into two subclusters, each of which does not know about the other subcluster. The two subclusters could each carry out recovery actions for the departed systems. This is termed split brain.

In a split brain condition, two systems could try to import the same shared storage and cause data corruption, have an IP address up in two places, or mistakenly run an application in two places at once.

Membership arbitration guarantees against such split brain conditions. The components of membership arbitration consist of:

- Fencing module
- Coordinator disks

About data protection

Membership arbitration by itself is inadequate for complete data protection because it assumes that all systems will either participate in the arbitration or are already down.

Rare situations can arise which must also be protected against. Some examples are:

- A system hang causes the kernel to stop processing for a period of time.
- The system resources were so busy that the heartbeat signal was not sent.
- A break and resume function is supported by the hardware and executed. Dropping the system to a system controller level with a break command can result in the heartbeat signal timeout.

In these types of situations, the systems are not actually down, and may return to the cluster after cluster membership has been recalculated. This could result in data corruption as a system could potentially write to disk before it determines it should no longer be in the cluster.

Combining membership arbitration with data protection of the shared storage eliminates all of the above possibilities for data corruption.

Data protection fences off (removes access to) the shared data storage from any system that is not a current and verified member of the cluster. Access is blocked by the use of SCSI-3 persistent reservations.

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 32.
- License requirements: in addition to SF Oracle RAC with HA/DR, you will need:
  - FlashSnap license
  - Site awareness license for consistent mirror detach.

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 5.0.1 on HP-UX.

Table 14-1 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

Table 14-1 Sample setup for campus cluster *(continued)*

Site	Hardware description
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 ust 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
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 preparing to install and configure SF Oracle RAC" on page 59.

   See "Installing SF Oracle RAC" on page 81.

   See "About configuring SF Oracle RAC" on page 87.

   In the sample setup, install and configure SF Oracle RAC 5.0.1 on all four nodes.

Configuring I/O fencing to prevent data corruption

Perform the following tasks to configure I/O fencing to prevent data corruption in the event of a communication failure.

To configure I/O fencing to prevent data corruption

1. After installing and configuring SF Oracle RAC, continue with configuring I/O fencing for data integrity.

   See "About configuring SF Oracle RAC clusters for data integrity" on page 117.

   See "About I/O fencing for campus clusters" on page 286.

2. Set up the storage at a third site.

   You can extend the DWDM to the third site to have FC SAN connectivity to the storage at the third site. You can also use iSCSI targets as the coordinator disks at the third site.

   For example:

   Enable I/O fencing by using the coordinator disks from all the three sites.

```
# vxdisksetup -i disk04 format=cdsdisk

# vxdisksetup -i disk09 format=cdsdisk
# vxdisksetup -i disk10 format=cdsdisk
# hastop -all
# vxdg init fencedg disk10 disk04 disk09
# vxdg -g fencedg set coordinator=on
# vxdg deport fencedg
# vxdg -t import fencedg
# vxdg deport fencedg
```

   Edit the main.cf to add "UseFence = SCSI3"

```
# vi /etc/VRTSvcs/conf/config/main.cf
# more /etc/vxfendg
fencedg
# more /etc/vxfentab
/dev/vx/rdmp/disk10
/dev/vx/rdmp/disk04
/dev/vx/rdmp/disk09
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfemode
# /sbin/init.d/vxfen stop
# /sbin/init.d/vxfen start
Starting vxfen..
Checking for /etc/vxfendg
Starting vxfen.. Done
```

   On all nodes, start VCS:

```
# hastart
```

Set the site name for each host.

```
# site=SFRAC1
# vxdctl set site=SFRAC2
# vxdctl set site=SFRAC2
```

3 Start I/O fencing by using the disks from all three sites.

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
# vxdctl set site= SFRAC1
```

On the nodes at second site:

```
# vxdctl set site= SFRAC2
# 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 to tag 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=SFRAC1 disk05
# vxdisk settag site=SFRAC2 disk06
# vxdisk settag site=SFRAC2 disk07
# 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
disk05           site                             SFRAC1
disk06           site                             SFRAC2
disk07           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
```

7 Enable site-based allocation on the disk groups for each site.

8 # **vxdg -g *ocrvotedg* addsite *SFRAC1***

vxdg -g *ocrvotedg* addsite *SFRAC2*

vxdg -g *ocrvotedg* addsite *SFRAC1*

vxdg -g *ocrvotedg* addsite *SFRAC2*

9 Set site consistency on the disk groups.

vxdg -g *ocrvotedg* set siteconsistent=on

vxdg -g *oradatadg* set siteconsistent=on

10 Set activation on the disk groups.

```
# vxdg -g ocrvotedg set activation=sw
# vxdg -g oradatadg set activation=sw
```

11 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.

12 From tthe CVM master, start the volumes for all the disk groups.

```
# vxvol -g ocrvotedg startall
# vxvol -g oradatadg startall
```

13 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 -F vxfs -o cluster /dev/vx/dsk/oradatadg/oradatavol /oradata
```

14 Touch two files, one for OCR and another for Vote Disk.

```
# touch /ocr/ocr /ocr/vote
```

Installing Oracle RAC Clusterware and database binaries

After configuring the disk groups and volumes for a campus cluster, install Oracle RAC.

See "About installing Oracle RAC" on page 215.

Configuring VCS service groups for a campus cluster

Follow the procedure below to configure the disk groups under SF Oracle RAC control and set up the VCS attributes to define parallel applications in campus clusters. The CVM and Oracle service groups can be configured by editing the VCS configuration file, the main.cf, to define the service groups.For a sample configuration file:

See "Sample main.cf for a four-node SF Oracle RAC campus cluster " on page 418.

To configure the VCS service groups

1. Configure the disk groups under SF Oracle RAC control and set up the VCS attributes to define parallel applications in campus clusters. The CVM and Oracle service groups can be configured by editing the VCS configuration file, main.cf, to define the service groups.
2. Configure the SystemZones attribute in the service group definition as explained previously.

   See "Configuring VxVM disk groups for Oracle RAC on a campus cluster" on page 291.

3 Group the hosts at each physical site into a single logical SystemZone. This will enable the failover applications to try to come up on local nodes before they try to come up on a remote site.

Not all SF Oracle RAC service groups are parallel. In the sample configuration file, hosts galaxy and nebula should be configured in zone 0 and hosts mercury and jupiter in zone 1. In the event of a failure, this setting instructs VCS to failover the group first within the same site and then across the sites.

4 After configuring your service groups and before putting your configuration into production, you can verify your configuration resilience by means of testing various failure scenarios.

See "Verification of failure scenarios and recovery" on page 295.

Verification of failure scenarios and recovery

Simulating the failure scenarios in an SF Oracle RAC campus cluster is recommended for evaluating the resilience of the cluster in the event of a disaster before putting it into production. Some of the most commonly seen failure scenarios and their resolution in SF Oracle RAC campus clusters are:

- Partial storage failure
- Complete storage failure
- Private interconnects failure
- Failure of a single node in a site
- Failure of all nodes at a site
- Site failure

About failure and recovery in an SF Oracle RAC campus cluster

The following table depicts various failure scenarios and the subsequent recovery, highlighting the advantages of site consistency feature in a SF Oracle RAC campus cluster.

Table 14-2 Expected failure and recovery scenarios

Event	Without site consistency enabled	With site consistency enabled	Reattach/recovery behavior
Partial storage failure (a few disks fail)	Only the mirror that encountered the error is detached. If an entire disk is faulty, then all the mirrors that reside on that disk will be detached. The vxrelocd will try to relocate the failed disk and bring back all detached mirrors on the relocated disk.	If each site contains multiple mirrors for a given volume and at least one valid mirror is available, then site detach is not done. Otherwise, the entire site is detached to ensure data consistency.	Reattach of mirrors is done when the disks are brought back. Recovery of volumes starts automatically.
Complete storage failure (all the disks at a site fail)	Only the mirror that encountered the error is detached. If the entire disk is faulty, then all the mirrors that reside on that disk will be detached.	Entire site is detached.	If the entire site's storage is back online, then mirror reattach and recovery is done automatically. If only some of the storage is back online and vxrelocd is running, then reattach is done after relocating the failed disks to available disks.

Table 14-2 Expected failure and recovery scenarios *(continued)*

Event	Without site consistency enabled	With site consistency enabled	Reattach/recovery behavior
Private interconnects failure (communication links are down)	If only the failure is limited to cluster heartbeats and storage is accessible, then VxVM takes no action. Otherwise, the behaviour is akin to one of the above cases. Due to VCS I/O fencing, in both the cases above, one of the sub-clusters will survive and the other sub-cluster commits suicide.	If only the failure is limited to cluster heartbeats and storage is accessible, then VxVM takes no action. Otherwise, the entire site will be detached. Due to VCS I/O fencing, in both the cases above, one of the sub-clusters will survive and the other sub-cluster commits suicide.	If the sub-cluster that lost the race comes back, it may find itself in a pre-existing split-brain scenario. Administrative intervention is needed to rejoin the nodes. Please refer to Veritas Cluster Server Administrators Guide for instructions on how to clear a pre-existing split-brain scenario.
Failure of a single node in a site (a node is down or too busy to respond)	A new cluster membership is formed following the reconfiguration. VCS I/O fencing removes the keys corresponding to the failed nodes from the coordinator disks. No action is taken by VxVM since the storage is still visible to the cluster.	A new cluster membership is formed following the reconfiguration. VCS I/O fencing removes the keys corresponding to the failed nodes from the coordinator disks. No action is taken by VxVM since the storage is still visible to the cluster.	When the failed node rejoins, it is allowed to join the cluster.
Failure of all nodes at a site (all the nodes are down or too busy to respond)	The behavior is same as when there is private interconnect failure between sites. VCS I/O fencing removes the keys corresponding to the failed node from the coordinator disks.	The behavior is same as when there is private interconnect failure between sites. VCS I/O fencing removes the keys corresponding to the failed node from the coordinator disks.	No action is taken by VxVM since the storage is still visible to the cluster. When the failed node rejoins, it is allowed to join the cluster.

Table 14-2 Expected failure and recovery scenarios *(continued)*

Event	Without site consistency enabled	With site consistency enabled	Reattach/recovery behavior
Site failure (all the nodes and storage fail)	Mirrors that encounter I/O error will be detached. Due to VCS I/O fencing, the surviving site wins the race on the local coordination point and also the one at the third site. It also removes the keys corresponding to the failed nodes.	All the mirrors on the failed site will be detached. Due to VCS I/O fencing, the surviving site wins the race on the local coordination point and also the one at the third site. It also removes the keys corresponding to the failed nodes.	When the site is restored and reconnected, disks will be automatically re-attached and resynchronized. The nodes will rejoin the cluster after reboot. Due to VCS I/O fencing, the possibility of serial split brain is avoided.

Testing partial storage failure and recovery

To test partial storage failure and recovery

1. Disable the path of one of the data LUNs from 2nd site, using vxdmpadm(1M) to simulate partial storage failure.
2. After 10 minutes, enable the path to imitate storage restoration.

   For example:

```
# vxdmpadm -f disable path=disk06
# vxdisk listtag
DEVICE          NAME                          VALUE
disk01           site                          SFRAC1
disk02           site                          SFRAC1
disk03           site                          SFRAC1
disk05           site                          SFRAC1
disk07           site                          SFRAC2
disk08           site                          SFRAC2

# vxprint -p
Disk group: ocrvote
TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
pl ocrvotevol-01 ocrvotevol  ENABLED  921600   -        ACTIVE   -       -
pl ocrvotevol-01 ocrvotevol  ENABLED  921600   -        ACTIVE   -       -
pl ocrvotevol_dcl -01 ocrvotevol_dcl ENABLED 1712 -      ACTIVE   -       -
```

```
pl ocrvotevol_dcl -01 ocrvotevol_dcl ENABLED 1712 -      ACTIVE   -       -

Disk group: oradatadg
TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
pl oradatavol-01 oradatavol  ENABLED  20889600 -        ACTIVE   -       -
pl oradatavol-02 oradatavol  DISABLED 20889600 -        NODEVICE -       -
pl oradatavol_dcl-01 oradatavol_dcl ENABLED 1712 -      ACTIVE   -       -
pl oradatavol_dcl-02 oradatavol_dcl DISABLED 1712 -     NODEVICE -       -

# vxdmpadm -f enable path= disk06

# vxprint -p
Disk group: ocrvote
TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
pl ocrvotevol-01 ocrvotevol  ENABLED  921600   -        ACTIVE   -       -
pl ocrvotevol-01 ocrvotevol  ENABLED  921600   -        ACTIVE   -       -
pl ocrvotevol_dcl -01 ocrvotevol_dcl ENABLED 1712 -      ACTIVE   -       -
pl ocrvotevol_dcl -01 ocrvotevol_dcl ENABLED 1712 -      ACTIVE   -       -
Disk group: oradatadg
TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
pl oradatavol-01 oradatavol  ENABLED  20889600 -        ACTIVE   -       -
pl oradatavol-02 oradatavol  ENABLED  20889600 -        ACTIVE-       -
pl oradatavol_dcl-01 oradatavol_dcl ENABLED 1712 -      ACTIVE   -       -
pl oradatavol_dcl-02 oradatavol_dcl ENABLED 1712 -      ACTIVE -       -
```

In the example above, the disk is detached from the site automatically. The mirror that resides on this disk is disabled, as seen by vxprint (1M). Once the path is enabled, the site is reattached and recovery is started automatically.

Testing complete storage failure and recovery

To test complete storage failure and recovery

1. Disable the paths of all the LUNs from 2nd site by using vxdmpadm(1M) to simulate full storage failure.
2. After 10 minutes, enable the path to imitate storage restoration.

   For example:

   ```
   # vxdmpadm -f disable path=disk06,disk07,disk08,disk09,disk11
   # vxdmpadm -f disable path=disk06,disk07,disk08,disk09,disk11
   # vxdisk -o alldgs list
   # vxdisk listtag
   DEVICE          NAME                           VALUE
   disk01          site                           SFRAC1
   disk02           site                           SFRAC1
   disk03           site                           SFRAC1
   disk05           site                           SFRAC1
   ```

3. Observe the error messages for the disk group getting disabled.

   For example:

   ```
   # vxprint -p
   # vxdmpadm -f enable path=disk06,disk07,disk08,disk09,disk11
   # vxdmpadm -f enablepath=disk06,disk07,disk08,disk09,disk11
   ```

   Immediately after re-enabling the paths, the volumes are seen to be recovering.

   For example:

```
# vxprint -p
Disk group: ocrvote
TY NAME          ASSOC         KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
pl ocrvotevol-01 ocrvotevol  ENABLED  921600   -        ACTIVE   -       -
Disk group: oradatadg
TY NAME          ASSOC         KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
pl oradatavol-01 oradatavol  ENABLED  20889600 -        ACTIVE   -       -
pl oradatavol-02 oradatavol  DISABLED 20889600 -        RECOVER  -       -
pl oradatavol_dcl-01 oradatavol_dcl ENABLED 1712 -      ACTIVE   -       -
pl oradatavol_dcl-02 oradatavol_dcl DISABLED 1712 -     RECOVER  -       -
```

   Immediately after the paths are disabled, all the disks are detached from the site. After the paths are enabled, the site is reattached and recovery of volumes is started automatically.

Testing private interconnects failure and recovery

To test private interconnects failure and recovery

- Disable both the LLT links by physically disconnecting them.

  After the LLT links were disabled, the nodes on one of the sites reboot and re-join the cluster.

Testing the failure of a single node in a site

To test the failure and recovery of a single node in a site

- Reboot a node at one site.

  For example:

  ```
  # reboot
  ```

  The node that was rebooted was able to rejoin the cluster successfully.

Failure of all nodes at a site

To test failure and recovery of all nodes at a site

- Reboot all the nodes at a site.

  For example:

  ```
  # reboot
  # reboot
  ```

  The rebooted nodes were able to re-join the cluster successfully.

Testing site failure and recovery

To test site failure and recovery

1. Disable the paths of all the LUN’s of 2nd site from one of the nodes at the first site, to simulate complete storage failure.
2. Reboot the nodes of the 2nd site to simulate a complete site failure.

3 Enable the paths of LUNs of 2nd site from one of the nodes at the 1st site.

For example:

```
# vxdmpadm -f disable path=disk06,disk07,disk08,disk09,disk11
# vxdmpadm -f disable path=disk06,disk07,disk08,disk09,disk11
# reboot
# reboot
```

4 After completion of reboot, enable the paths of LUNs.

For example:

```
# vxdmpadm -f enable path=disk06,disk07,disk08,disk09,disk11
# vxdmpadm -f enable path=disk06,disk07,disk08,disk09,disk11
```

After the site failure, the nodes that were rebooted were able to join the cluster successfully. After the paths were enabled, the mirrors were attached and recovered automatically.

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.

Chapter 15

Setting up a replicated SF Oracle RAC global cluster

This chapter includes the following topics:

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 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.

Requirements for SF Oracle RAC global clusters

Review the requirements information to make sure your configuration is supported for SF Oracle RAC.

Supported software and hardware for SF Oracle RAC

For supported hardware and software:

- See "Installation requirements" on page 32.
- 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 15-1 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
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

Table 15-1 Supported replication options for SF Oracle RAC global clusters *(continued)*

Replication technology	Supported modes	Supported software
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 MirrowView Installation and Configuration Guide*
- Technical Support TechNote for the latest updates or software issues for replication agents:
  http://entsupport.symantec.com/docs/282004htm

Configuring 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:

See “Installation requirements” on page 32.

For sample primary and secondary cluster configuration files:

See “Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)” on page 388.

See “Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)” on page 393.

Configuring an SF Oracle RAC 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 "Important preinstallation information" on page 31.

See "Global cluster information" on page 430.

See "Sample main.cf files for Oracle replication configurations" on page 388.

If you have an existing SF Oracle RAC cluster, and you want to set up a global cluster, skip the steps below and proceed to configure your secondary cluster.

If you are setting up an SF Oracle RAC global cluster from the beginning, follow the steps below.

To set up 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. Install and configure SF Oracle RAC. Prepare for your installation according to your configuration needs.

   For requirements:

   See "Installation requirements" on page 32.

   For preparation:

   See "About preparing to install and configure SF Oracle RAC" on page 59.

   For installation:

   After verifying a successful SF Oracle RAC installation:

   Verify the CVM group is online on all nodes in the primary cluster:

   ```
   # hagrp -state cvm
   ```

4. 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

5 Install and configure the Oracle RAC binaries:

See "About preparing to install Oracle RAC" on page 181.

See "About installing Oracle RAC" on page 215.

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
```

6 Identify the disks that will be replicated, create the required CVM disk group, volume, and file system. Create the database on that file system.

7 Configure the VCS service groups for the database:

8 Verify that all VCS service groups are online.

Configuring an SF Oracle RAC cluster at the secondary site

You can set up a multi-node or single-node cluster on the secondary site. 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.

To set up the 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 Install and configure SF Oracle RAC. Prepare for your installation according to your configuration needs.

For requirements:

See "Installation requirements" on page 32.

For preparation:

See "About preparing to install and configure SF Oracle RAC" on page 59.

For installation:

After verifying a successful SF Oracle RAC installation:

Verify the CVM group is online on all nodes in the primary cluster:

```
# hagrp -state cvm
```

4 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 setting up I/O fencing" on page 118.

5 For a single-node cluster, do not enable I/O fencing. Fencing will run in disabled mode.

6 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

7 Install and configure the Oracle RAC binaries:

See "About preparing to install Oracle RAC" on page 181.

See "About installing Oracle RAC" on page 215.

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
```

8 Do not create the database, the disk group, or volumes. 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.

9 Copy the init file from $ORACLE_HOME/dbs at the primary to $ORACLE_HOME/dbs at the secondary.

10 Create the following subdirectories as on the primary site:

For Oracle RAC 10g

```
$ mkdir $ORACLE_HOME/admin
$ mkdir $ORACLE_HOME/admin/$DB_NAME
$ cd $ORACLE_HOME/admin/$DB_NAME
$ mkdir bdump  cdump create hdump pfile udump
```

For Oracle RAC 11g there is no need to create the subdirectories since they are created automatically by Oracle RAC 11g when the database starts.

11 On Secondary make sure that CRS is up, add listener resource using netca. Make changes to tnsnames.ora.

Example `tnsnames.ora` (Here vrts is the database name)

```
 LISTENERS_VRTS =
     (ADDRESS_LIST =
         (ADDRESS = (PROTOCOL = TCP)(HOST = mercury-vip)(PORT =
 1521))
         (ADDRESS = (PROTOCOL = TCP)(HOST = jupiter-vip)(PORT =
1521))
    )

VRTS2 =
    (DESCRIPTION =
        (ADDRESS = (PROTOCOL = TCP)(HOST = jupiter-vip)(PORT =
1521))
        (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = vrts)
            (INSTANCE_NAME = vrts2)
         )
      )

VRTS1 =
    (DESCRIPTION =
        (ADDRESS = (PROTOCOL = TCP)(HOST = mercury-vip)(PORT =
1521))
        (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = vrts)
            (INSTANCE_NAME = vrts1)
         )
     )
VRTS =
    (DESCRIPTION =
        (ADDRESS = (PROTOCOL = TCP)(HOST = mercury-vip)(PORT =
1521))
        (ADDRESS = (PROTOCOL = TCP)(HOST = jupiter-vip)(PORT =
1521))
        (LOAD_BALANCE = yes)
        (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = vrts)
```

```
        )
    )
```

12 On the secondary, register the database using `srvctl` command.

```
$ srvctl add database -d <database_name> -o <oracle_home> -p <spfile-on-shareddisk>
```

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
```

13 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>
```

14 Configure the VCS service groups for the database:

Verify that all VCS service groups are online.

For sample configurations:

See "Sample main.cf files for Oracle replication configurations" on page 388.

Note: The database service group will be ONLINE only at one site at a time. Hence if it is ONLINE on the primary site, it will be OFFLINE on secondary site and vice versa.

Configuring replication on clusters at both sites

You must configure replication for the database files at both the primary and secondary site. 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. 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 "Preparing clusters for replication using VVR" on page 318.

   For Hardware-based replication:

   See your hardware documentation for details on setting up replication between the two sites.
3. Start replication between the sites.

   See your hardware documentation for the appropriate procedures.
4. Test the replication between sites.

To test replication between sites

1. Create some sample files at the primary site on the replicated storage.
2. When replication is complete, split or suspend the replication.
3. Import the required disk groups, mount the corresponding file system, and verify that the sample files exist at the secondary site.
4. Unmount the file system, deport the disk group, and establish replication.

Configuring VCS service groups for global clusters

You have configured VCS service groups for 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.

If you are using VVR for replication, configure VCS service groups after installing Oracle on the secondary site, and before establishing replication.

If you did not configure the ClusterService group when you installed SF Oracle RAC on the secondary site, configure it when you configure global clustering.

Configure a global cluster by setting:

- Heartbeat
- Wide area cluster (wac)

- GCO IP (gcoip)
- remote cluster resources

For sample main.cf files for global cluster configurations:

See "Sample main.cf files for Oracle replication configurations" on page 388.

To configure VCS service groups for global clusters

1. Configure and enable global groups for databases and resources.
    - Configure VCS service groups at the secondary site and test local failover at that site (assuming more than one node in the cluster at the secondary site).
    - Configure the replication agent at both sites.
    - Make the RAC service group a global service group, enabling failover across clusters.
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.
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 MirrowView 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*.

Testing a global cluster configuration

Symantec recommends testing before putting a clobal cluster configuration into production.

To test a planned failover

1. Offline the VCS service group for the Oracle RAC database on the cluster at the primary site.
2. Online the VCS service group for the Oracle RAC database on the cluster at the secondary site.

To test distaster recovery at the recovery site

1. Plan downtime to test the disaster recovery configuration.
2. Simulate a disaster at the primary site.

   For example:

   Shut down the hosts and storage arrays at the primary. If you can not shut down the storage arrays, disconnect the replication link between the sites.
3. Use VCS to fail over the Oracle RAC database to the cluster at the secondary site.

To test failback on the primary site

1. Offline the VCS service group for the Oracle RAC database on the cluster at the secondary site.
2. Restart the nodes and the storage array at the primary site.
3. Reconnect the replication link if it was broken.
4. Resynchronize the data from the secondary to make sure the data at the primary site is current.
5. Bring the VCS service group online at the primary site.

Chapter 16

Configuring a global cluster using VVR

This chapter includes the following topics:

About configuring global clustering using VVR

After setting up a secondary cluster running SF Oracle RAC, you can configure a global cluster environment. 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.
- Setting up replication on both clusters.
- Starting replication of the database.
- Configuring VCS on the primary site for replication.
- Configuring VCS on the secondary site for replication.

For sample primary and secondary cluster configuration files:

See "Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)" on page 388.

See “Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)” on page 393.

Preparing clusters for replication using VVR

Before configuring clusters for global clustering, make sure both clusters have the following:

- SF Oracle RAC and Oracle RAC installed and configured
- License keys installed for VVR
- VVR and global clustering enabled

For global clustering and VVR licensing information:

See “Obtaining and installing license keys for a global cluster” on page 79.

To verify VVR and global clustering licenses are enabled on all nodes

1 On all nodes of the primary and secondary clusters, enter:

```
# vxlicrep |grep -i global
   Global Cluster Option#VERITAS Cluster Server = Enabled
   Global Cluster Option                        = Enabled
```

2 On both primary and secondary clusters, enter:

```
# vxlicrep |grep -i vvr
   VVR#VERITAS Volume Manager           = Enabled
   VVR                                  = Enabled
```

The example procedures in the following topics assume rac_cluster101 as the local cluster with nodes galaxy and nebula, and rac_cluster102 as the remote cluster on the secondary site with nodes mercury and jupiter.

To view sample configuration files

1 Navigate to the directory containing sample configuration files:

```
# cd /etc/VRTSvcs/conf/sample_rac
```

2 List the SF Oracle RAC CVM/VVR sample main.cf examples:

```
# ls *cvmvvr*

cvmvvr_primary_main.cf*    cvmvvr_secondary_main.cf*
```

These main.cf examples are for CVM/VVR primary and secondary configurations and will help guide you through the following sections.

For sample primary and secondary cluster configuration files:

See "Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)" on page 388.

See "Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)" on page 393.

Preparing clusters for replication in both sites requires:

- Adding the VVR resource types to the VCS configuration
- Configuring global clustering using VVR
- Defining the remote cluster and heartbeat Cluster Objects

Adding the VVR resource types to the VCS configuration

After SF Oracle RAC is installed on two clusters and fencing is configured, add the VVR types to the VCS configuration.

To add VVR types to the VCS configuration on each cluster perform the tasks described in the procedure below. In the procedure below and as an example, there is a local cluster and a remote cluster with the following names:

```
LOCAL_CLUSTER NAME: rac_cluster101 (galaxy,nebula)
REMOTE_CLUSTER_NAME: rac_cluster102 (mercury.jupiter)
```

The primary site is rac_cluster101 and the secondary site is rac_cluster102. A virtual IP address of 10.10.10.101 is associated with rac_cluster101 and a second virtual IP address of 10.11.10.102 is associated with rac_cluster102.

Adding VVR Types to the VCS Configuration

1. On the first cluster, make sure that CVM is up.
2. Make sure you have installed VVR license keys with "VVR" enabled.

   See "Obtaining SF Oracle RAC license keys" on page 77.
3. Run the script to add definitions for VVR types:

   ```
   # cd /etc/VRTSvcs/conf/sample_vvr
   ```

   ```
   # ./addVVRTypes.sh
   ```

When you run the script "addVVRTypes.sh" for adding VVR resource definitions to the VCS configuration, the following warning messages are displayed:

```
VCS WARNING V-16-1-10421
Non static attribute does not exist 'Primary' (RVG)
VCS WARNING V-16-1-10421
Non static attribute does not exist 'SRL' (RVG)
VCS WARNING V-16-1-10421
Non static attribute does not exist 'RLinks' (RVG)
```

These warnings may be ignored.

4 Perform the previous steps on the second cluster, `rac_cluster102`.

Configuring global clustering using VVR

You can configure global clustering on SF Oracle RAC clusters by editing the configuration files:

See "Modifying the configuration for VVR using the main.cf" on page 321.

Before you configure global clustering, review the following requirements:

- Cluster names on the primary and secondary sites must be unique.
- Node and resource names must be unique within a cluster but not across clusters.
- Each cluster requires a virtual IP address associated with the cluster. The VCS installation and creation of the ClusterService group typically involves defining this IP address. If you did not configure the ClusterService group when you installed SF Oracle RAC, configure it when you configure global clustering.
- One WAN (Wide Area Network) heartbeat must travel between clusters, assuming each cluster has the means to monitor the health of the remote cluster. Configure the heartbeat resource manually.
- All Oracle user and group IDs must be the same on all nodes.
- The Oracle RAC database, which VVR replicates from the storage on the primary site to the secondary site, must be defined in a global group having the same name on each cluster. Each resource in the group may differ from cluster to cluster, but clients redirected to a remote cluster after a wide-area failover must see the same application as the one in the primary cluster.

See the *Veritas Cluster Server User's Guide* for complete details on global clustering.

Modifying the configuration for VVR using the main.cf

To modify the main.cf for VVR

1 Edit the main.cf file to specify the virtual IP address for the local cluster and define the ClusterService group for the local cluster.

The example global clustering configuration shows the rac_cluster101 cluster on the primary site. The additions to the configuration appear in bold text.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "VVRTypes.cf"

cluster rac_cluster101 (
    UserNames = { admin = "cDRpdxPmHpzS." }
    ClusterAddress = "10.10.10.101"
    Administrators = { admin }
    CounterInterval = 5
    UseFence = SCSI3
    )


system galaxy (
    )

system nebula (
    )

group ClusterService (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoStartList = { galaxy,nebula }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )
    Application wac (
        StartProgram = "/opt/VRTSvcs/bin/wacstart"
        StopProgram = "/opt/VRTSvcs/bin/wacstop"
        MonitorProcesses = {"/opt/VRTSvcs/bin/wac" }
        RestartLimit = 3
        )

    IP gcoip (
```

```
            Device = lan0
            Address = "10.10.10.101"
            NetMask = "255.255.255.0"
            )

    NIC csgnic (
            Device = lan0
            NetworkHosts = { "10.10.8.1" }
            )

        gcoip requires csgnic
        wac requires gcoip

    .
    .
    .

    group cvm (
    .
    .
    .
```

2. Edit the main.cf file for the secondary cluster as illustrated in the previous step using configuration values that will be appropriate for the secondary cluster.
3. Wait for port 'h' to close on all systems.

   On one of the nodes enter:

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

4. On all nodes enter:

   ```
   # hastart
   ```

Defining the remote cluster and heartbeat Cluster Objects

After configuring global clustering, add the remote cluster 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 through step 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.

Setting up replication using VVR

Setting up replication with VVR in a global cluster environment involves the following tasks:

- Create a disk group on the storage on the primary site (if you have not already done so).
  See "Planning the storage for Oracle RAC " on page 42.
- Creating the Storage Replicator Log (SRL) in the disk group for the database.
  See "Creating the SRL volume on the primary site" on page 325.
- Creating the Replicated Volume Group (RVG) on the primary site.
  See "Setting up replication objects on the primary site" on page 326.
- Setting up replication objects on the secondary site.
  See "Configuring replication for the secondary site" on page 327.
- See "Starting replication of Oracle RAC database volume" on page 331.

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.
  See "Configuring an SF Oracle RAC cluster at the secondary site" on page 308.
- 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 replication objects 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.

3 Check that the CVM group is online.

4 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).

Configuring replication for 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:

- Create a disk group on the storage with the same name as the equivalent disk group on the primary site (if you have not already done so).
  See "Planning the storage for Oracle RAC " on page 42.
- Create volumes for the database and SRL on the secondary site.
  See "Creating the data and SRL volumes on the secondary site" on page 327.
- Edit the /etc/vx/vras/.rdg file on the secondary site.
  See "Editing the /etc/vx/vras/.rdg files" on page 328.
- 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 328.
- Create the replication objects on the secondary site.
  See "Setting up the disk group on secondary site for replication" on page 329.

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 volume 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 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 the 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 the 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_suster101_priv has IP address 10.10.9.101
   - rac_suster102_priv has IP address 10.10.9.101

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 on 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: oradatadg
- 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: 10.10.9.101 or rac_suster101_priv
- sec_host is the virtual IP address or resolvable virtual host name of the cluster on the secondary site. For example: 10.11.9.102 or rac_cluster102_priv

#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
- 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: oradatadg
datavol_cnt: 1
vset_cnt: 0
srl: rac1_srl
RLinks:
name=rlk_10.11.9.102_ 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_10.10.9.101_ rac1_rvg, detached=on,
synchronous=off
```

Note: Once the replication is started the value off 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_clus102_priv
```

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_clus102_priv
```

2 To start replication after full synchronization, enter the following command:

```
# vradmin -g oradatadg -c rac1_ckpt startrep rac1_rvg
rac_clus102_priv
```

Verifying replication status

Verify that replication is properly functioning.

To verify replication status

1 Use the vxprint command on the primary site:

```
vxprint -g diskgroup -l rlink_name
```

2 Review the `flags` output for the status. The output may appear as `connected` and `consistent`. For example:

```
# vxprint -g oradatadg -l rlk_10.182.13.221_oradatadg
  Rlink: rlk_10.182.13.221_oradatadg
  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.

The following sample main.cf files illustrate the VCS configuration changes after setting up an existing Oracle RAC database for replication:

See "Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)" on page 388.

See "Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)" on page 393.

To view the sample main.cf files on your system, enter the following commands:

```
# pwd

/etc/VRTSvcs/conf/sample_rac

# ls cvmvvr*

cvmvvr_primary_main.cf    cvmvvr_secondary_main.cf
```

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:

See "Configuration examples before and after modification" on page 336.

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 491.

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

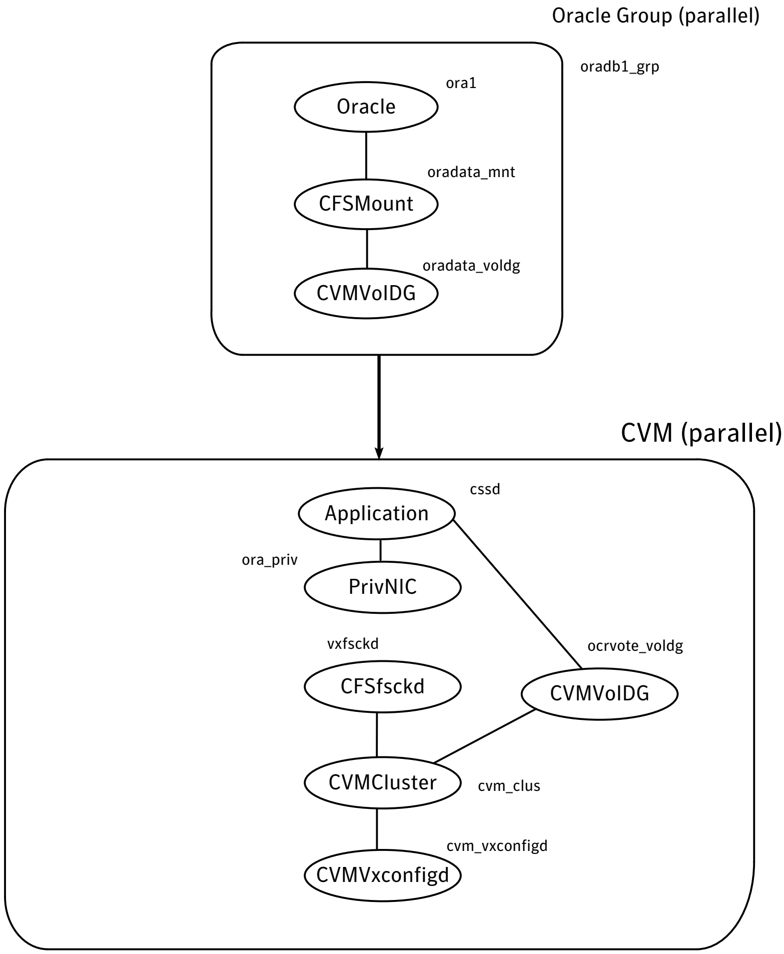
Review the following illustrations that display the changes to the VCS configuration, after setting up replication on the existing Oracle RAC database.

- Configuration before modification:
  Figure 16-1
- Configuration after modification:
  Figure 16-2

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.

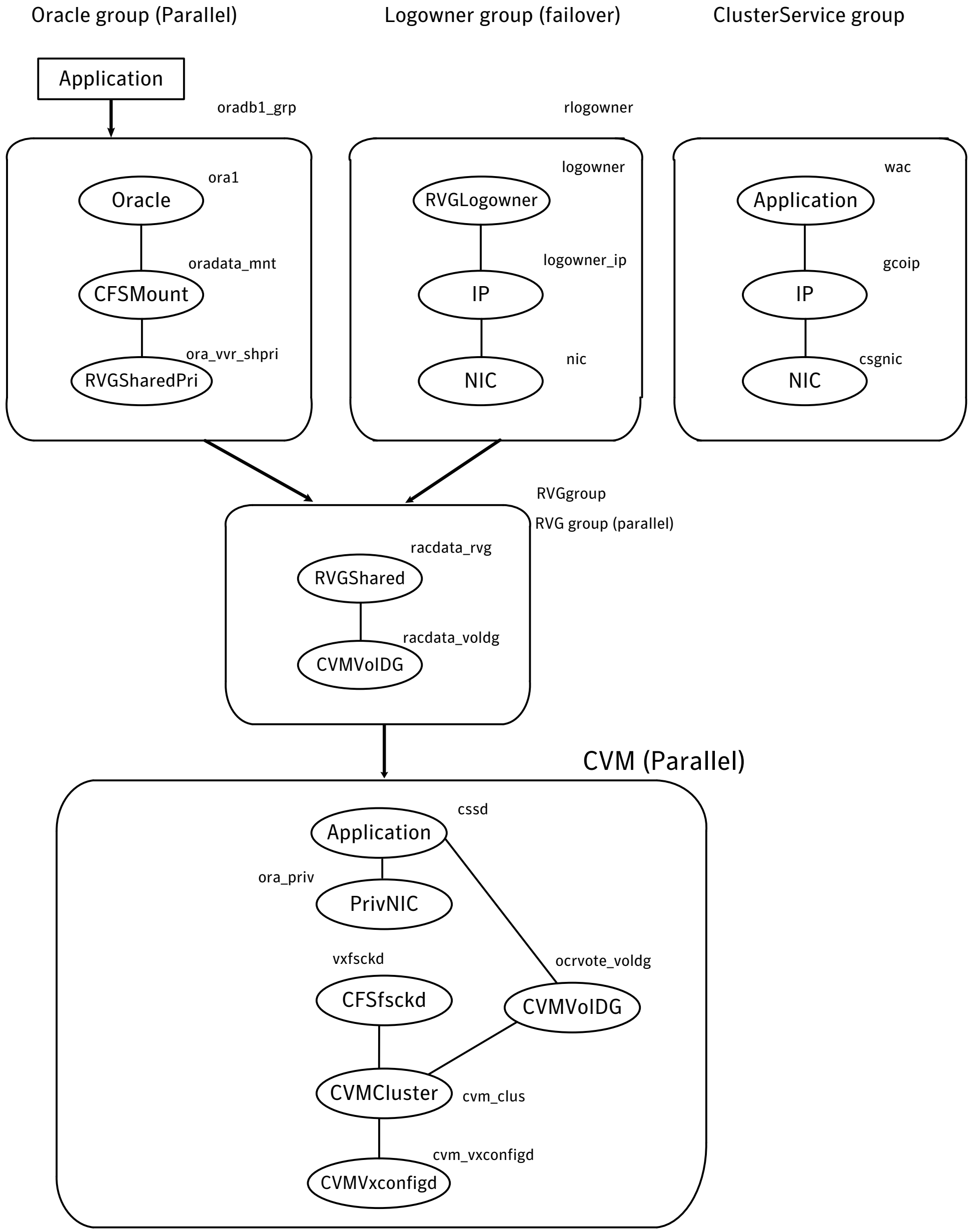
Configuration before modification for replication:

Figure 16-1 Illustration of dependencies before modification for replication (Oracle RAC 10g)



Configuration after modification for replication:

Figure 16-2 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 RVGShared service 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.

   See "Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)" on page 388.

   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 Oracle RAC 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 Oracle RAC 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 oradb1_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
    MonScript = "./bin/Oracle/SqlTest.pl"
    )
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.

   See "Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)" on page 393.

   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, oradb1_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 oradb1_grp (
    SystemList = { mercury = 0, jupiter = 1 }
    ClusterList = { rac_cluster102 = 0, rac_cluster101 = 1 }
    Parallel = 1
    OnlineRegryInterval = 300
    ClusterFailOverPolicy = Manual
    Authority = 1
    AutoStartList = { mercury, jupiter }
    )

    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 @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
          MonScript = "./bin/Oracle/SqlTest.pl"
          )

     requires group RVGgroup online local firm
     oradata_mnt requires ora_vvr_shpri
     rac_db requires oradata_mnt

         StartUpOpt = SRVCTLSTART
          ShutDownOpt = SRVCTLSTOP
          MonScript = "./bin/Oracle/SqlTest.pl"
          )

     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
```

Starting VCS on all nodes in both clusters

After modifying the main.cf files for replication on the primary and secondary clusters, start VCS on both clusters.

To start VCS on all nodes in both clusters

1. From the primary site, use the following command to start the VCS engine on one node:

   ```
   # hastart
   ```

2. Next, enter the following command:

   ```
   # hastatus
   ```

3. When LOCAL_BUILD or RUNNING is listed in the message column, use the following command to start VCS on the other node:

   ```
   # hastart
   ```

4. 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.

5. On the secondary site, start VCS from one node using the following command:

   ```
   # hastart
   ```

6. Next, enter the following command:

   ```
   # hastatus
   ```

7. When LOCAL_BUILD or RUNNING is listed in the message column, use the following command to start VCS on the other node:

   ```
   # hastart
   ```

8. 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.

For information on the VCS commands for global clusters:

See the *Veritas Cluster Server User'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 remote 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 Oracle RAC database service group, `oradb1_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 oradb1_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 oradatadg status rlk_rac_clus102_priv_rac1_rvg
   ```

   Where rlk_rac_clus102_priv_rac1_rvg is the RLINK.

3. On the secondary site, bring the Oracle service group online on all nodes:

   ```
   # hagrp -online oradb1_grp -any
   ```

4. Make sure that all CRS resources are online, and switch back the group oradb1_grp to the primary site.

   - Issue the following command on the remote site:

     ```
     # hagrp -offline oradb1_grp -any
     ```

   - Make sure that oradb1_grp is offline on the primary site. Then, execute the following command on the primary site to bring the oradb1_grp online:

     ```
     # hagrp -online oradb1_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). See the *Veritas Volume Replicator Administrator's Guide* for detailed description of concepts of taking over the primary role.

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 351.

See "Replica" on page 351.

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 oradb1_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 oradatadg and the RVG is rac1_rvg, type:

```
# vxrvg -g oradatadg -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 oradatadg 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 oradatadg snaprestore rac1_rvg
  ```

Troubleshooting CVR

The following topic headings indicate either probable symptoms of a problem, or the procedures required for a solution.

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 6

Uninstalling SF Oracle RAC

Chapter 17

Uninstalling SF Oracle RAC from a cluster

This chapter includes the following topics:

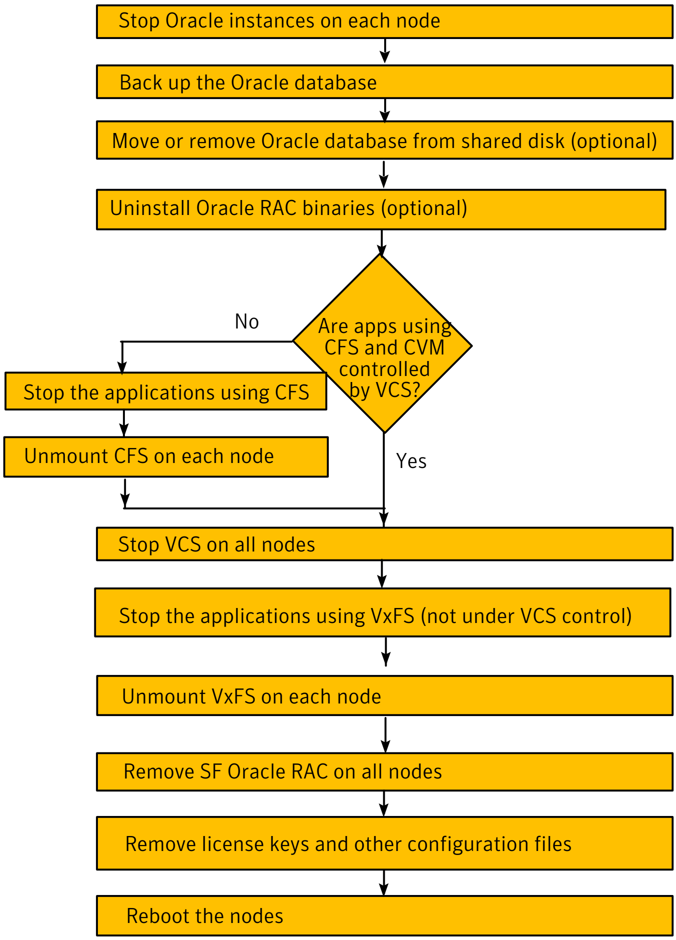
About uninstalling SF Oracle RAC from a cluster

You can uninstall SF Oracle RAC using the uninstallsfrac program 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 17-1 illustrates the steps that are required to uninstall SF Oracle RAC from a cluster.

Figure 17-1 SF Oracle RAC uninstallation



Preparing to uninstall SF Oracle RAC from a cluster

Perform the following steps before you uninstall SF Oracle RAC from a cluster:

- Stopping Oracle instances
- Backing up the Oracle database

- Uninstalling Oracle RAC (optional)
- Removing the database storage management repository
- Stopping the applications that use CFS (outside of VCS control)
- Unmounting CFS file systems (outside of VCS control)
- Stopping the applications that use VxFS (outside of VCS control)
- Unmounting VxFS file systems (outside of VCS control)
- Stopping VCS

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:

   ```
   # /opt/VRTSvcs/bin/hagrp -offline Oracle1 -sys galaxy
   ```

   ```
   # /opt/VRTSvcs/bin/hagrp -offline Oracle1 -sys nebula
   ```

   These commands stop the Oracle resources under VCS control.

   If the database is not under VCS control, stop the Oracle resources as follows:

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

3. Verify that the state of the Oracle and CVM service groups are offline and online respectively.

   ```
   # /opt/VRTSvcs/bin/hagrp -state
   Group      Attribute    System     Value
   Oracle1      State      galaxy     |OFFLINE|
   Oracle1      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.

Uninstalling Oracle RAC (optional)

You cannot use the Oracle database after you uninstall SF Oracle RAC. However, you can continue using Oracle RAC, provided the Oracle Clusterware and database binaries are not installed on VxFS. To continue using Oracle RAC, unlink the SF Oracle RAC libraries from Oracle RAC.

link to unlinking procedure

If you do not plan to use Oracle RAC, you may want to uninstall the software using the Oracle runInstaller utility. Run the utility on any node in the cluster.

For information about the runInstaller utility, see the Oracle documentation.

To uninstall Oracle RAC

1. Log in as the Oracle user.
2. Set the DISPLAY variable. Depending on the shell you use, run the following command:

Bourne Shell (sh or ksh)	`$ DISPLAY=host:0.0;export DISPLAY`
C Shell (csh or tcsh)	`$ setenv DISPLAY host:0.0`

3. Run the runInstaller utility:

```
$ /cdrom/Disk1/runInstaller
```

4. Select the option to uninstall Oracle RAC.

Removing the database storage management repository

Make sure that you have superuser (root) privileges to remove the repository database.

To remove the database storage management repository

1. Remove the sfua_db resource from the VCS configuration:

```
# /opt/VRTS/bin/sfua_db_config -o unconfig_cluster
```

2. Import the database storage management repository disk group:

```
# vxdg import <name_of_disk_group>
```

3. Mount the database storage management repository volume:

```
# /sbin/init.d/sfua_rep_mount start
```

4. Drop the database storage management repository. This step deletes the database storage management repository files.

```
# /opt/VRTS/bin/sfua_db_config -o dropdb
```

5. Unmount the database storage management repository mount point.

```
# /sbin/init.d/sfua_rep_mount stop
```

Stopping the applications that use CFS (outside of VCS control)

You need to stop the applications that use CFS mount points not controlled by VCS.

To stop the applications that use CFS (outside of VCS control)

1. Using native application commands, stop the applications that use a CFS mount point.
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 the applications that use VxFS (outside of VCS control)

You need to stop all applications that use VxFS mount points not under VCS control.

To stop the applications that use VxFS (outside of VCS control)

1. Using native application commands, stop the applications that use a VxFS mount point.
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 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:

   ```
   # /opt/VRTSvcs/bin/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.

   ```
   # /sbin/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
   ```

Removing SF Oracle RAC from a cluster

You can remove the SF Oracle RAC packages 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.

Removing SF Oracle RAC from a cluster involves the following tasks:

- Removing the SF Oracle RAC packages
- Removing other configuration files (optional)

Removing the SF Oracle RAC packages

The installer offers the option to remove Veritas Volume Manager and Veritas Volume Replicator packages. The uninstallsfrac program can remove these packages 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 packages.
- Removes the language packages, if installed.

To remove the SF Oracle RAC packages

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 and VVR installed, indicate whether or not you want to remove VxVM and VVR packages from all nodes in the cluster. Enter **y** only if the root disk is outside of VxVM control.

   The uninstallsfrac program performs the following task:

   - Checks the operating system on each node
   - Verifies the system-to-system communication
   - Verifies the licenses

- Checks for the SF Oracle RAC packages installed on the nodes. This process involves identifying system uninstallation requirements and dependencies between packages to determine the safety and order of uninstalling packages.

5 Confirm to uninstall SF Oracle RAC.

```
All SFRAC processes that are currently running must be stopped.
Do you want to stop SFRAC 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 packages
- 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
```

Rebooting the nodes

Reboot each node after you uninstall SF Oracle RAC:

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

Section 7

Reference

Sample configuration files

This appendix includes the following topics:

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 types files for VCS (types.cf), CFS (CFSTypes.cf), CVM (CVMTypes.cf), PrivNIC (PrivNIC.cf), MultiPrivNIC (MultiPrivNIC.cf), Oracle Enterprise agent (OracleTypes.cf), and Oracle ASM (OracleASMTypes.cf). The files are located in the /etc/VRTSvcs/conf/config directory. These files define the agents that control the resources in the cluster.
  - The VCS types file (types.cf) includes all agents that are bundled with VCS. Refer to the *Veritas Cluster Server Bundled Agents Reference Guide* for information about VCS agents.
  - The CFS types file (CFSTypes.cf) includes the CFSMount agent and CFSfsckd types.
    The CFSMount agent mounts and unmounts the shared volume file systems.

The CFSfsckd types are defined for cluster file system daemons and do not require user configuration.

- The CVM types file (CVMTypes.cf) includes definitions for the CVMCluster agent, CVMVxconfigd agent, and the CVMVolDg agent.

CVMCluster agent	The CVMCluster agent is automatically configured during installation. The agent performs the following tasks: ■ Starts CVM in the cluster by automatically importing shared disk groups ■ Controls the node membership in the cluster ■ Defines how nodes communicate the state of volumes
CVMVxconfigd agent	The CVMVxconfigd agent starts and monitors the vxconfigd daemon. The daemon performs the following tasks: ■ Maintains the disk and the disk group configurations ■ Communicates the configuration changes to the kernel ■ Modifies the configuration information that is stored on disks See “ CVMVxconfigd agent” on page 489.
CVMVolDg agent	The CVMVolDg agent starts the volumes in a shared disk group, sets activation modes, and monitors specified critical volumes. See “ CVMVolDg agent” on page 491.

- The PrivNIC types file (PrivNIC.cf) includes definitions for the PrivNIC agent. The PrivNIC agent queries LLT to count the number of visible nodes on each of the LLT Ethernet interfaces.
- The MultiPrivNIC types file (MultiPrivNIC.cf) includes definitions for the MultiPrivNIC agent. The MultiPrivNIC agent provides resources for UDP/IP support for Oracle RAC 11g cache fusion capabilities.
- The Oracle Enterprise agent types file (OracleTypes.cf) includes definitions for the Oracle agent and the Netlsnr agent. The Oracle agent monitors the resources for an Oracle database and the Netlsnr agent manages the resources for the listener process.

- The Oracle ASM types file (OracleASMTypes.cf) includes definitions for the ASM Instance agent and the ASM DG agent.

ASM Instance agent	The ASM Instance agent monitors the ASM instance, brings the ASM instance online, and takes it offline.
ASM DG agent	The ASM DG agent mounts, unmounts, and monitors the ASM disk groups that are required for ASM-enabled databases.

- 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 I/O fencing" on page 126.
- 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.

Sample main.cf file after SF Oracle RAC installation

The following are the configuration details for this sample main.cf:

- Name of the cluster: rac_cluster101
- Nodes in the cluster: galaxy and nebula
- Has only one parallel service group: cvm

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "PrivNIC.cf"
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "OracleASMTypes.cf"

cluster rac_cluster101 (
    UserNames = { admin = bopHo }
    Administrators = { admin }
    UseFence = SCSI3
```

```
    )

system galaxy (
    )

system nebula (
    )

group cvm (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { galaxy, nebula }
    )
    CFSfsckd vxfsckd (
    )

CVMCluster cvm_clus (
    CVMClustName = rac_cluster101
    CVMNodeId = { galaxy = 0, nebula = 1 }
    CVMTransport = gab
    CVMTimeout = 200
    )

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
    )

vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Sample main.cf files for Oracle configurations

Sample main.cf file examples are provided for the following Oracle configurations:

- Sample main.cf for Oracle RAC 10g without Oracle agent
- Sample main.cf for Oracle RAC 10g with Oracle agent
- Sample main.cf for Oracle RAC 10g without the Oracle agent and with VxSS
- Sample main.cf for Oracle RAC 11g without Oracle agent
- Sample main.cf for Oracle RAC 11g with Oracle agent

Note: After an SF Oracle RAC installation, several sample main.cf file types can be viewed in the following directory: `/etc/VRTSvcs/conf/sample_rac`

Sample main.cf for Oracle RAC 10g without Oracle agent

The following are the configuration details for this Oracle RAC 10g sample main.cf:

- Configuration file name: 10g_simple_main.cf
- Use for single Oracle RAC 10g database only
- Has only one parallel service group: cvm
- cvm group includes PrivNIC and Application resource for CSSD

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "PrivNIC.cf"

cluster rac_cluster101 (
        UserNames = { admin = bopHo}
        Administrators = { admin }
        UseFence = SCSI3
        )

system galaxy (
        )

system nebula (
        )

group cvm (
      SystemList = { galaxy = 0, nebula = 1 }
      AutoFailOver = 0
      Parallel = 1
      AutoStartList = { galaxy, nebula }
      )

      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
                )


        CVMVolDg ocrvote_voldg (
                Critical = 0
                CVMDiskGroup = ocrvotedg
                CVMVolume = { ocrvol, votevol }
                CVMActivation = sw
                )



        CFSMount oradata_mnt (
                Critical = 0
                MountPoint = "/oradata"
                BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
                )

        CVMVolDg oradata_voldg (
                Critical = 0
                CVMDiskGroup = oradatadg
                CVMVolume = { oradatavol }
                CVMActivation = sw
                )

        CFSfsckd vxfsckd (
                )


       CVMCluster cvm_clus (
                 CVMClustName = rac_cluster101
                 CVMNodeId = { galaxy = 0, nebula = 1 }
                 CVMTransport = gab
                 CVMTimeout = 200
                  )



        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )
```

```
      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 = "255.255.240.0"
              )


cssd requires ocrvote_voldg
cssd requires oradata_mnt
cssd requires ora_priv

oradata_mnt requires oradata_voldg
oradata_mnt requires vxfsckd

oradata_voldg requires cvm_clus
ocrvote_voldg requires cvm_clus

cvm_clus requires cvm_vxconfigd
```

Sample main.cf for Oracle RAC 10g with Oracle agent

The following are the configuration details for this Oracle RAC 10g sample main.cf:

- Configuration file name: 10g_main.cf
- For multiple Oracle databases
- Has two parallel service groups: cvm and oradb1_grp
- oradb1_grp depends on cvm
- oradb1_grp has Oracle and oradata mount resource

Note: Set the database startup mode to manual in CRS.

```
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 (
        )

group oradb1_grp (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )

        Oracle ora1 (
                Critical = 0
                Sid @galaxy = vrts1
                Sid @nebula = vrts2
                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

group cvm (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )

        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
                 )


     CVMVolDg ocrvote_voldg (
             Critical = 0
             CVMDiskGroup = ocrvotedg
             CVMVolume = { ocrvol, votevol }
             CVMActivation = sw
             )

    CFSfsckd vxfsckd (
            )




    CVMCluster cvm_clus (
            CVMClustName = rac_cluster101
            CVMNodeId = { galaxy = 0, nebula = 1 }
            CVMTransport = gab
            CVMTimeout = 200
            )



    CVMVxconfigd cvm_vxconfigd (
```

```
             Critical = 0
             CVMVxconfigdArgs = { syslog }
             )


    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 = "255.255.240.0"
            )


cssd requires ocrvote_voldg
cssd requires ora_priv
ocrvote_voldg requires cvm_clus
vxfsckd requires cvm_clus
cvm_clus requires cvm_vxconfigd
```

Sample main.cf for Oracle RAC 10g without the Oracle agent and with VxSS

The following is a sample main.cf for Oracle RAC 10g without the Oracle agent and with the VxSS group.

```
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 (
        )


group VxSS (
        SystemList = { galaxy = 0, nebula = 1 }
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        OnlineRetryLimit = 3
        OnlineRetryInterval = 120
        )

        Phantom phantom_vxss (
                )

        ProcessOnOnly vxatd (
                IgnoreArgs = 1
                PathName = "/opt/VRTSat/bin/vxatd"
                )



 // resource dependency tree
 //
 // group VxSS
 // {
 // Phantom phantom_vxss
 // ProcessOnOnly vxatd
 // }


group cvm (
      SystemList = { galaxy = 0, nebula = 1 }
      AutoFailOver = 0
      Parallel = 1
      AutoStartList = { galaxy, nebula }
      )

      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
        )


CVMVolDg ocrvote_voldg (
        Critical = 0
        CVMDiskGroup = ocrvotedg
        CVMVolume = { ocrvol, votevol }
        CVMActivation = sw
        )



CFSMount oradata_mnt (
        Critical = 0
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
        )

CVMVolDg oradata_voldg (
        Critical = 0
        CVMDiskGroup = oradatadg
        CVMVolume = { oradatavol }
        CVMActivation = sw
        )

CFSfsckd vxfsckd (
        )


CVMCluster cvm_clus (
         CVMClustName = rac_cluster101
         CVMNodeId = { galaxy = 0, nebula = 1 }
         CVMTransport = gab
         CVMTimeout = 200
          )



CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )
```

```
        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 = "255.255.240.0"
                )


cssd requires ocrvote_voldg
cssd requires oradata_mnt
cssd requires ora_priv
oradata_mnt requires oradata_voldg
oradata_voldg requires cvm_clus
ocrvote_voldg requires cvm_clus
oradata_mnt requires vxfsckd
cvm_clus requires cvm_vxconfigd


// resource dependency tree
 //
 // group cvm
 // {
 // Application cssd
 //     {
 //     CFSMount ocrvote_mnt
 //         {
 //         CVMVolDg ocrvote_voldg
 //             {
 //             CFSMount oradata_mnt
 //                 {
 //                 CMVVolDg oradata_voldg
 //                 }
 //             }
 //         CFSfsckd vxfsckd
 //             {
 //             CVMCluster cvm_clus
 //                 {
 //                 CVMVxconfigd cvm_vxconfigd
 //                 }
 //             }
 //         }
 //     PrivNIC ora_priv
```

```
//      }
// }
```

Sample main.cf for Oracle RAC 11g without Oracle agent

The following are the configuration details for this Oracle RAC 11g sample main.cf:

- Configuration file name: 11g_simple_main.cf
- To be used for single 11g+ Oracle database only
- Has only one service group: cvm
- cvm group includes PrivNIC and Application resource for CSSD

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "MultiPrivNIC.cf"
include "PrivNIC.cf"

cluster rac_cluster101 (
        UserNames = { admin = bopHo}
        Administrators = { admin }
        UseFence = SCSI3
        )

system galaxy (
        )

system nebula (
        )

group cvm (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )

        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
                      )



 CVMVolDg ocrvote_voldg (
         Critical = 0
         CVMDiskGroup = ocrvotedg
         CVMVolume = { ocrvol, votevol }
         CVMActivation = sw
         )

CFSMount oradata_mnt (
        Critical = 0
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
        )

CVMVolDg oradata_voldg (
        Critical = 0
        CVMDiskGroup = oradatadg
        CVMVolume = { oradatavol }
        CVMActivation = sw
        )

CFSfsckd vxfsckd (
        )



                  CVMCluster cvm_clus (
                           CVMClustName = rac_cluster101
                           CVMNodeId = { galaxy = 0, nebula = 1 }
                           CVMTransport = gab
                           CVMTimeout = 200
                           )


                   CVMVxconfigd cvm_vxconfigd (
                          Critical = 0
                          CVMVxconfigdArgs = { syslog }
                          )
```

```
        MultiPrivNIC multi_priv (
              Critical = 0
              Device@galaxy = { lan1 = 0, lan2 = 1}
              Device@nebula = { lan1 = 0, lan2 = 1}
              Address@galaxy = { "192.168.1.1" = 0, "192.168.1.2" = 0, "192.168.2.1" = 1 }
              Address@nebula = { "192.168.1.3" = 0, "192.168.1.4" = 0, "192.168.2.2" = 1 }
              NetMask = "255.255.240.0"
              )


                    cssd requires ocrvote_voldg
                    cssd requires oradata_mnt
                    cssd requires multi_priv

                    oradata_mnt requires oradata_voldg

                    oradata_voldg requires cvm_clus
                    ocrvote_voldg requires cvm_clus
                    oradata_mnt requires vxfsckd
                    vxfsckd requires cvm_clus
                    cvm_clus requires cvm_vxconfigd
```

Sample main.cf for Oracle RAC 11g with Oracle agent

The following are the configuration details for this Oracle RAC 11g sample main.cf:

- Configuration file name: 11g_main.cf
- More general purpose, can have multiple Oracle databases
- Has three service groups: cvm, oradb1_grp and oradb2_grp
- oradb1_grp depends on cvm
- oradb1_grp has Oracle and oradata mount resource
- oradb2_grp depends on cvm
- oradb2_grp has Oracle and oradata mount resource

Note: Set the database startup mode to manual in CRS .

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
```

```
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"

cluster rac_cluster101 (
        UserNames = { admin = bopHo }
        Administrators = { admin }
        UseFence = SCSI3
        )

system galaxy (
        )

system nebula (
        )

group cvm (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
         )

       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
           )



      CVMVolDg ocrvote_voldg (
              Critical = 0
              CVMDiskGroup = ocrvotedg
              CVMVolume = { ocrvotevol }
              CVMActivation = sw
              )

       CFSfsckd vxfsckd (
              )
```

```
                    CVMCluster cvm_clus (
                            CVMClustName = rac_cluster101
                            CVMNodeId = { galaxy = 0, nebula = 1 }
                            CVMTransport = gab
                            CVMTimeout = 200
                            )


                    CVMVxconfigd cvm_vxconfigd (
                            Critical = 0
                            CVMVxconfigdArgs = { syslog }
                            )



MultiPrivNIC multi_priv (
        Critical = 0
        Device@galaxy = { lan1 = 0, lan2 = 1}
        Device@nebula = { lan1 = 0, lan2 = 1}
        Address@galaxy = { "192.168.1.1" = 0, "192.168.1.2" = 0, "192.168.2.1" = 1 }
        Address@nebula = { "192.168.1.3" = 0, "192.168.1.4" = 0, "192.168.2.2" = 1 }
        NetMask = "255.255.240.0"
        )


             cssd requires ocrvote_voldg
             cssd requires multi_priv
             ocrvote_voldg requires cvm_clus
             vxfsckd requires cvm_clus
             cvm_clus requires cvm_vxconfigd




             group oradb1_grp (
                     SystemList = { galaxy = 0, nebula = 1 }
                     AutoFailOver = 0
                     Parallel = 1
                     AutoStartList = { galaxy, nebula }
                     )
```

```
        Oracle ora1 (
                Critical = 0
                Sid @galaxy = vrts1
                Sid @nebula = vrts2
                Owner = oracle
                Home = "/app/oracle/orahome"
                StartUpOpt = "SRVCTLSTART"
                ShutDownOpt = "SRVCTLSTOP"
                )

       CFSMount oradata1_mnt (
               Critical = 0
               MountPoint = "/oradata1"
               BlockDevice = "/dev/vx/dsk/oradata1_dg/oradatavol"
               )

      CVMVolDg oradata1_voldg (
              CVMDiskGroup = oradata1_dg
              CVMVolume = { oradatavol }
              CVMActivation = sw
              )

     requires group cvm online local firm
     ora1 requires oradata1_mnt
     oradata1_mnt requires oradata1_voldg


group oradb2_grp (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )

        Oracle ora2 (
                Critical = 0
                Sid @galaxy = hr1
                Sid @nebula = hr2
                Owner = oracle
                Home = "/app/oracle/orahome"
                StartUpOpt = "SRVCTLSTART"
                ShutDownOpt = "SRVCTLSTOP"
                )
```

```
CFSMount oradata2_mnt (
        Critical = 0
        MountPoint = "/oradata2"
        BlockDevice = "/dev/vx/dsk/oradata2_dg/oradatavol"
        )

CVMVolDg oradata2_voldg (
        CVMDiskGroup = oradata2_dg
        CVMVolume = { oradatavol }
        CVMActivation = sw
        )

requires group cvm online local firm
ora2 requires oradata2_mnt
oradata2_mnt requires oradata2_voldg
```

Sample main.cf files for Oracle replication configurations

This section displays the sample main.cf files for Oracle replication configurations.

Sample main.cf file examples are provided for the following Oracle replication configurations:

- Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)
- Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)
- Sample main.cf for Oracle RAC 10g for hardware-based replication primary site
- Sample main.cf for Oracle RAC 10g for hardware-based replication secondary site

---

Note: After an SF Oracle RAC installation, several sample main.cf file types can be viewed in the following directory: `/etc/VRTSvcs/conf/sample_rac`

Sample main.cf for Oracle RAC 10g and CVM/VVR (primary replication site)

The following are the configuration details for this Oracle RAC 10g sample main.cf:

- Named: cvmvvr_primary_main.cf

- More general purpose, can have multiple Oracle databases
- Path to file: /etc/VRTSvcs/conf/sample_rac/cvmvvr_primary_main.cf

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf
include "/etc/VRTSvcs/conf/config/VVRTypes.cf"

cluster rac_cluster101 (
    UserNames = { admin = bopHo }
    ClusterAddress = "10.10.10.101"
    Administrators = { admin }
    UseFence = SCSI3
    )

remotecluster rac_cluster102 (
    ClusterAddress = "10.11.10.102"
    )

heartbeat Icmp (
    ClusterList = { rac_cluster102 }
    Arguments @rac_cluster102 = { "10.11.10.102" }
    )

system galaxy (
    )

system nebula (
    )

group ClusterService (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoStartList = { galaxy, nebula }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

Application wac (
        StartProgram = "/opt/VRTSvcs/bin/wacstart"
        StopProgram = "/opt/VRTSvcs/bin/wacstop"
        MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
        RestartLimit = 3
        )
```

```
    IP gcoip (
        Device = lan0
        Address = "10.10.10.101"
        NetMask = "255.255.240.0"
        )

    NIC csgnic (
       Device = lan0
       NetworkHosts = { "10.10.12.2", "10.10.12.3" }
       )

    gcoip requires csgnic
    wac requires gcoip

group RVGgroup (
    SystemList = { galaxy = 0, nebula = 1 }
    Parallel = 1
    AutoStartList = { galaxy, nebula }
    )

    CVMVolDg racdata_voldg (
        CVMDiskGroup = oradatadg
        CVMActivation = sw
        )

    RVGShared racdata_rvg (
        RVG = rac1_rvg
        DiskGroup = oradatadg
        )

    requires group cvm online local firm
    racdata_rvg requires racdata_voldg

group cvm (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { galaxy, nebula }
    )

    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
        )

    CFSfsckd vxfsckd (
        )

    CVMCluster cvm_clus (
        CVMClustName = rac_cluster101
        CVMNodeId = { galaxy = 0, nebula = 1 }
        CVMTransport = gab
        CVMTimeout = 200
        )

CVMVolDg ocrvote_voldg (
    Critical = 0
    CVMDiskGroup = ocrvotedg
    CVMVolume = { ocrvol, votevol }
    CVMActivation = sw
    )

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
    )

PrivNIC ora_priv (
    Critical = 0
    Device = { lan1 = 0, lan2 = 1}
    Address@galaxy = "192.168.12.1"
    Address@nebula = "192.168.12.2"
    NetMask = "255.255.240.0"
    )


    cssd requires ocrvote_voldg
    cssd requires ora_priv
    cssd requires ora_priv
    ocrvote_voldg requires cvm_clus
    vxfsckd requires cvm_clus
    cvm_clus requires cvm_vxconfigd

group oradb1_grp (
    SystemList = { galaxy = 0, nebula = 1 }
    Parallel = 1
    ClusterList = { rac_cluster101 = 0, rac_cluster102 = 1 }
```

```
    OnlineRetryInterval = 300
    ClusterFailOverPolicy = Manual
    AutoStartList = { galaxy, nebula }
    )

CFSMount oradata_mnt (
    MountPoint = "/oradata"
    BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
    )

Oracle ora1 (
     Critical = 0
    Sid @galaxy = vrts1
    Sid @nebula = vrts2
    Owner = oracle
    Home = "/app/oracle/orahome"
    StartUpOpt = SRVCTLSTART
    ShutDownOpt = SRVCTLSTOP
    )

RVGSharedPri ora_vvr_sharedpri (
    RvgResourceName = racdata_rvg
    OnlineRetryLimit = 0
    )

requires group RVGgroup online local firm
 ora1 requires oradata_mnt
 oradata_mnt requires ora_vvr_sharedpri

group rlogowner (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoStartList = { galaxy, nebula }
    OnlineRetryLimit = 2
    )

    IP logowner_ip (
        Device = lan0
        Address = "10.10.9.101"
        NetMask = "255.255.240.0"
        )

    NIC nic (
        Device = lan0
        NetworkHosts = { "10.10.12.2", "10.10.12.3" }
        )
```

```
RVGLogowner logowner (
    RVG = rac1_rvg
    DiskGroup = oradatadg
    )

    requires group RVGgroup online local firm
    logowner requires logowner_ip
    logowner_ip requires nic
```

Sample main.cf for Oracle RAC 10g and CVM/VVR (secondary replication site)

The following are the configuration details for this Oracle RAC 10g sample main.cf:

- Named: cvmvvr_secondary_main.cf
- More general purpose, can have multiple Oracle databases
- Path to file: /etc/VRTSvcs/conf/sample_rac/cvmvvr_secondary_main.cf

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf
include "/etc/VRTSvcs/conf/config/VVRTypes.cf"

cluster rac_cluster102 (
    UserNames = { admin = bopHo }
    ClusterAddress = "10.11.10.102"
    Administrators = { admin }
    UseFence = SCSI3
    )

remotecluster rac_cluster101 (
    ClusterAddress = "10.10.10.101"
    )

heartbeat Icmp (
    ClusterList = { rac_cluster101 }
    Arguments @rac_cluster101 = { "10.10.10.101" }
    )

system mercury (
    )
```

```
system jupiter (
    )

group ClusterService (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoStartList = { mercury, jupiter }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Application wac (
        StartProgram = "/opt/VRTSvcs/bin/wacstart"
        StopProgram = "/opt/VRTSvcs/bin/wacstop"
        MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
        RestartLimit = 3
        )

    IP gcoip (
        Device = lan0
        Address = "10.11.10.102"
        NetMask = "255.255.240.0"
        )

    NIC csgnic (
        Device = lan0
        NetworkHosts = { "10.10.12.2", "10.10.12.3" }
        )

    gcoip requires csgnic
    wac requires gcoip

group RVGgroup (
    SystemList = { mercury = 0, jupiter = 1 }
    Parallel = 1
    AutoStartList = { mercury, jupiter }
    )

    CVMVolDg racdata_voldg (
        CVMDiskGroup = oradatadg
        CVMActivation = sw
        )

    RVGShared racdata_rvg (
        RVG = rac1_rvg
        DiskGroup = oradatadg
        )
```

```
    requires group cvm online local firm
    racdata_rvg requires racdata_voldg

group cvm (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { mercury, jupiter }
    )

    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
        )

    CFSfsckd vxfsckd (
        )

    CVMCluster cvm_clus (
        CVMClustName = rac_cluster102
        CVMNodeId = { mercury = 0, jupiter = 1 }
        CVMTransport = gab
        CVMTimeout = 200
        )

    CVMVolDg ocrvote_voldg (
        Critical = 0
        CVMDiskGroup = ocrvotedg
        CVMVolume = { ocrvol, votevol }
        CVMActivation = sw
        )

    CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )

    PrivNIC ora_privnic (
        Critical = 0
        Device = { lan1 = 0, lan2 = 1}
        Address@galaxy = "192.168.12.1"
```

```
            Address@nebula = "192.168.12.2"
            NetMask = "255.255.240.0"
            )

        cssd requires ocrvote_voldg
        cssd requires ora_priv
        ocrvote_voldg requires cvm_clus
        vxfsckd requires cvm_clus
        cvm_clus requires cvm_vxconfigd

    group oradb1_grp (
        SystemList = { mercury = 0, jupiter = 1 }
        Parallel = 1
        ClusterList = { rac_cluster101 = 0, rac_cluster102 = 1 }
        OnlineRetryInterval = 300
        ClusterFailOverPolicy = Manual
        Authority = 1
        AutoStartList = { mercury, jupiter }
        )

        CFSMount oradata_mnt (
            MountPoint = "/oradata"
            BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
            )

        Oracle ora1 (
            Critical = 0
            Sid @mercury = vrts1
            Sid @jupiter = vrts2
            Owner = oracle
            Home = "/app/oracle/orahome"
            StartUpOpt = SRVCTLSTART
            ShutDownOpt = SRVCTLSTOP
            )

        RVGSharedPri ora_vvr_sharedpri (
            RvgResourceName = racdata_rvg
            OnlineRetryLimit = 0
            )

        requires group RVGgroup online local firm
        ora1 requires oradata_mnt
        oradata_mnt requires ora_vvr_sharedpri
```

```
group rlogowner (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoStartList = { mercury, jupiter }
    OnlineRetryLimit = 2
    )

    IP logowner_ip (
        Device = lan0
        Address = "10.11.9.102"
        NetMask = "255.255.240.0"
        )

    NIC nic (
        Device = lan0
        NetworkHosts = { "10.10.12.2", "10.10.12.3" }
        )

    RVGLogowner logowner (
        RVG = rac1_rvg
        DiskGroup = oradatadg
        )

requires group RVGgroup online local firm
    logowner requires logowner_ip
    logowner_ip requires nic
```

Sample main.cf for Oracle RAC 10g for hardware-based replication primary site

The following are the configuration details for this Oracle RAC 10g sample main.cf:

- Configuration file name: srdf_primary_main.cf
- More general purpose, can have multiple Oracle databases
- While this sample is based on SRDF, this template is valid for other supported hardware-based replication options.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"
include "SRDFTypes.cf"
```

```
cluster rac_cluster101 (
    UserNames = { admin = bopHo }
    ClusterAddress = "10.11.10.101"
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    )

remotecluster rac_cluster102 (
    ClusterAddress = "10.11.10.102"
    )

heartbeat Icmp (
    ClusterList = { rac_cluster102 }
    Arguments @rac_cluster101 = { "10.11.10.102" }
    )

system galaxy (
    )

system nebula (
    )

group ClusterService (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoStartList = { galaxy, nebula }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Application wac (
        StartProgram = "/opt/VRTSvcs/bin/wacstart"
        StopProgram = "/opt/VRTSvcs/bin/wacstop"
        MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
        RestartLimit = 3
        )

    IP gcoip (
        Device = lan0
        Address = "10.11.10.101"
        NetMask = "255.255.240.0"
        )

    NIC csgnic (
        Device = lan0
        NetworkHosts = { "10.10.12.2", "10.10.12.3" }
        )
```

```
    gcoip requires csgnic
    wac requires gcoip

    // resource dependency tree
    //
    //      group ClusterService
    //      {
    //      Application wac
    //          {
    //          IP gcoip
    //              {
    //              NIC csgnic
    //              }
    //          }
    //      }

group Async_ReplicatedDataGroup (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoStart = 0
    Parallel = 1
    ClusterList = { rac_cluster101 = 1, rac_cluster102 = 0 }
    AutoStartList = { galaxy, nebula }
    ClusterFailOverPolicy = Auto
    )

    CFSMount oradataa_cfs (
        MountPoint = "/oradataa"
        BlockDevice = "/dev/vx/dsk/oradataa_dg_galaxy_nebula/oradataa_vol"
        )

    CVMVolDg oradataa_vol (
        Critical = 0
        CVMDiskGroup = oradataa_dg_galaxy_nebula
        CVMVolume = { oradataa_vol }
        CVMActivation = sw
        )


               Oracle Oracle2 (
                       Critical = 0
                       Sid @galaxy = vrts1
                       Sid @nebula = vrts2
                       Owner = oracle
                       Home = "/app/oracle/orahome"
```

```
                        StartUpOpt = SRVCTLSTART
                        ShutDownOpt = SRVCTLSTOP

    SRDF SRDFASync_Group_1 (
        GrpName = RAC_Async
        Mode = Asynchronous
        )

    requires group cvm online local firm
    Oracle2 requires oradataa_cfs
    oradataa_cfs requires oradataa_vol
    oradataa_vol requires SRDFASync_Group_1

    // resource dependency tree
    //
    //      group Async_ReplicatedDataGroup
    //      {
    //      Oracle Oracle2
    //          {
    //          CFSMount oradataa_cfs
    //              {
    //              CVMVolDg oradataa_vol
    //                  {
    //                  SRDF SRDFASync_Group_1
    //                  }
    //              }
    //          }
    //      }

group cvm (
    SystemList = { galaxy = 0, nebula = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { galaxy, nebula }
    )

                    Application cssd (
                        Critical = 0
                        StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
                        StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline stopcrs"
                        CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
                        MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
                        )
```

```
CFSMount ocrvote_cfs (
  Critical = 0
  MountPoint @galaxy = "/ocrvote"
  MountPoint @nebula = "/ocrvote"
  BlockDevice @galaxy = "/dev/vx/dsk/ocrvote_dg_galaxy_nebula/ocrvote_vol"
  BlockDevice @nebula = "/dev/vx/dsk/ocrvote_dg_galaxy_nebula/ocrvote_vol"
  )

CFSfsckd vxfsckd (
    )

CVMCluster cvm_clus (
    CVMClustName = rac_cluster101
    CVMNodeId = { galaxy = 0, nebula = 1 }
    CVMTransport = gab
    CVMTimeout = 200
    )

CVMVolDg ocrvote_vol (
    Critical = 0
    CVMDiskGroup @galaxy = ocrvote_dg_galaxy_nebula
    CVMDiskGroup @nebula = ocrvote_dg_galaxy_nebula
    CVMVolume @galaxy = { ocrvote_vol }
    CVMVolume @nebula = { ocrvote_vol }
    CVMActivation @galaxy = sw
    CVMActivation @nebula = sw
    )

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
    )

PrivNIC ora_privnic (
    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 = "255.255.240.0"
    )

cssd requires ocrvote_cf
cssd requires ora_priv
cvm_clus requires cvm_vxconfigd
```

```
    ocrvote_cfs requires ocrvote_vol
    ocrvote_vol requires vxfsckd
    vxfsckd requires cvm_clus

                        // resource dependency tree
                        //
                        //      group cvm
                        //      {
                        //      Application cssd
                        //          {
                        //          CFSMount ocrvote_cfs
                        //              {
                        //              CVMVolDg ocrvote_vol
                        //                  {
                        //                  CFSfsckd vxfsckd
                        //                      {
                        //                      CVMCluster cvm_clus
                        //                          {
                        //                          CVMVxconfigd cvm_vxconfigd
                        //                          }
                        //                      }
                        //                  }
                        //              }
                        //          PrivNIC ora_priv
                        //          }
                        //      }
```

Sample main.cf for Oracle RAC 10g for hardware-based replication secondary site

The following are the configuration details for this Oracle RAC 10g sample main.cf:

- Configuration file name: srdf_secondary_main.cf
- More general purpose, can have multiple Oracle databases

The following file is a placeholder, it needs editing.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"
include "SRDFTypes.cf"
```

```
cluster rac_cluster102 (
    UserNames = { admin = bopHo }
    ClusterAddress = "10.11.10.102"
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    )

remotecluster rac_cluster101 (
    ClusterAddress = "10.11.10.101"
    )

heartbeat Icmp (
    ClusterList = { rac_cluster101 }
    Arguments @rac_cluster101 = { "10.11.10.101" }
    )

system mercury (
    )

system jupiter (
    )

group ClusterService (
    SystemList = { mercury = 0, jupiter = 0 }
    AutoStartList = { mercury, jupiter }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Application wac (
        StartProgram = "/opt/VRTSvcs/bin/wacstart"
        StopProgram = "/opt/VRTSvcs/bin/wacstop"
        MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
        RestartLimit = 3
        )

                       IP gcoip (
                           Device = lan0
                           Address = "10.11.10.102"
                           NetMask = "255.255.240.0"
                           )

    NIC csgnic (
        Device = lan0
        NetworkHosts = { "10.10.12.2", "10.10.12.3" }
        )
```

```
    gcoip requires csgnic
    wac requires gcoip

    // resource dependency tree
    //
    //      group ClusterService
    //      {
    //      Application wac
    //          {
    //          IP gcoip
    //              {
    //              NIC csgnic
    //              }
    //          }
    //      }

group Async_ReplicatedDataGroup (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoStart = 0
    Parallel = 1
    ClusterList = { rac_cluster102 = 1, rac_cluster101 = 0 }
    AutoStartList = { mercury, jupiter }
    ClusterFailOverPolicy = Auto
    )

    CFSMount oradataa_cfs (
        MountPoint = "/oradataa"
        BlockDevice = "/dev/vx/dsk/oradataa_dg_mercury_jupiter/oradataa_vol"
        )

                   CVMVolDg oradataa_vol (
                       Critical = 0
                       CVMDiskGroup = oradataa_dg_mercury_jupiter
                       CVMVolume = { oradataa_vol }
                       CVMActivation = sw
                       )


               Oracle Oracle2 (
                       Critical = 0
                       Sid @mercury = vrts1
                       Sid @jupiter = vrts2
                       Owner = oracle
                       Home = "/app/oracle/orahome"
```

```
                        StartUpOpt = SRVCTLSTART
                        ShutDownOpt = SRVCTLSTOP

    SRDF SRDFASync_Group_1 (
        GrpName = RAC_Async
        Mode = Asynchronous
        )

    requires group cvm online local firm
    Oracle2 requires oradataa_cfs
    oradataa_cfs requires oradataa_vol
    oradataa_vol requires SRDFASync_Group_1

    // resource dependency tree
    //
    //      group Async_ReplicatedDataGroup
    //      {
    //      Oracle Oracle2
    //          {
    //          CFSMount oradataa_cfs
    //              {
    //              CVMVolDg oradataa_vol
    //                  {
    //                  SRDF SRDFASync_Group_1
    //                  }
    //              }
    //          }
    //      }

group cvm (
    SystemList = { mercury = 0, jupiter = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { mercury, jupiter }
    )

    Application cssd (
        Critical = 0
        StartProgram = "/opt/VRTSvcs/rac/bin/cssd-online"
        StopProgram = "/opt/VRTSvcs/rac/bin/cssd-offline stopcrs"
        CleanProgram = "/opt/VRTSvcs/rac/bin/cssd-clean"
        MonitorProgram = "/opt/VRTSvcs/rac/bin/cssd-monitor"
        )
```

```
CFSMount ocrvote_cfs (
    Critical = 0
    MountPoint @mercury = "/ocrvote"
    MountPoint @jupiter = "/ocrvote"
    BlockDevice @mercury = "/dev/vx/dsk/ocrvote_dg_mercury_jupiter/ocrvote_vol"
    BlockDevice @jupiter = "/dev/vx/dsk/ocrvote_dg_mercury_jupiter/ocrvote_vol"
    )

CFSfsckd vxfsckd (
    )

CVMCluster cvm_clus (
    CVMClustName = rac_cluster102
    CVMNodeId = { mercury = 0, jupiter = 1 }
    CVMTransport = gab
    CVMTimeout = 200
    )

CVMVolDg ocrvote_vol (
    Critical = 0
    CVMDiskGroup @mercury = ocrvote_dg_mercury_jupiter
    CVMDiskGroup @jupiter = ocrvote_dg_mercury_jupiter
    CVMVolume @mercury = { ocrvote_vol }
    CVMVolume @jupiter = { ocrvote_vol }
    CVMActivation @mercury = sw
    CVMActivation @jupiter = sw
    )

CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
    )

PrivNIC ora_privnic (
    Critical = 0
    Device @mercury = { lan1 = 0, lan2 = 1}
    Device @jupiter = { lan1 = 0, lan2 = 1}
    Address@mercury = "192.168.12.3"
    Address@jupiter = "192.168.12.4"
    NetMask = "255.255.240.0"
    )

cssd requires ocrvote_cf
cssd requires ora_priv
cvm_clus requires cvm_vxconfigd
```

```
ocrvote_cfs requires ocrvote_vol
ocrvote_vol requires vxfsckd
vxfsckd requires cvm_clus

// resource dependency tree
//
//      group cvm
//      {
//      Application cssd
//          {
//          CFSMount ocrvote_cfs
//              {
//              CVMVolDg ocrvote_vol
//                  {
//                  CFSfsckd vxfsckd
//                      {
//                      CVMCluster cvm_clus
//                          {
//                          CVMVxconfigd cvm_vxconfigd
//                          }
//                      }
//                  }
//              }
//          PrivNIC ora_priv
//          }
//      }
```

Sample main.cf files for adding and removing nodes

This section displays sample main.cf files for adding and removing nodes.

The following sample main.cf file examples are provided for adding and removing nodes in a configuration:

- Sample main.cf for adding an Oracle RAC 10g node
- Sample main.cf for removing an Oracle RAC 10g node
- Sample main.cf for adding an Oracle RAC 11g node
- Sample main.cf for removing an Oracle RAC 11g node

Note: After an SF Oracle RAC installation, several sample main.cf file types can be viewed in the following directory: `/etc/VRTSvcs/conf/sample_rac`

Sample main.cf for adding an Oracle RAC 10g node

Changes to the Oracle RAC 10g sample main.cf for adding a node are highlighted in bold for the saturn node.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"

cluster ora_cluster (
        UserNames = { admin = dOPhOJoLPkPPnXPjOM }
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        CounterInterval = 5
        UseFence = SCSI3
        )

system galaxy (
        )

system nebula (
        )

system saturn (
        )

group cvm (
        SystemList = { galaxy = 0, nebula = 1, saturn = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

Note: In the group cvm section of this main.cf, the saturn node has been added.

```
        CFSMount oradata_mnt (
                Critical = 0
                MountPoint = "/oradata"
                BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
                )
```

```
CVMVolDg oradata_voldg (
        Critical = 0
        CVMDiskGroup = oradatadg
        CVMVolume = { oradatavol }
        CVMActivation = sw
        )

CVMVolDg orabin_voldg (
        Critical = 0
        CVMDiskGroup = orabindg
        CVMVolume = { orabinvol }
        CVMActivation = sw
        )


CVMVolDg ocrvote_voldg (
        Critical = 0
        CVMDiskGroup = ocrvotedg
        CVMActivation = sw
         )


CFSfsckd vxfsckd (
        )



CVMCluster cvm_clus (
        CVMClustName = ora_cluster
        CVMNodeId = { galaxy = 0, nebula = 1, saturn = 2 }
        CVMTransport = gab
        CVMTimeout = 200
        )
```

Note: In the CVMCluster cvm_clus section for the main.cf, the saturn node has been added.

```
CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )
```

```
        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 = "192.168.12.58"
               Address@nebula = "192.168.12.59"
               Address@saturn = "192.168.12.60"
               NetMask = "255.255.240.0"
               )
```

Note: In the PrivNIC ora_priv section for the main.cf, the saturn node has been added.

```
cvm_clus requires cvm_vxconfigd

oradata_voldg requires cvm_clus
ocrvote_voldg requires cvm_clus

ocrvote_mnt requires vxfsckd
oradata_mnt requires vxfsckd
oradata_mnt requires oradata_voldg
```

Sample main.cf for removing an Oracle RAC 10g node

Changes to the Oracle RAC 10g sample main.cf for adding a node are highlighted in bold for the saturn node.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"

cluster ora_cluster (
        UserNames = { admin = dOPhOJoLPkPPnXPjOM }
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        CounterInterval = 5
        UseFence = SCSI3
```

```
        )

system galaxy (
        )

system nebula (
        )

system saturn (
        )

group cvm (
        SystemList = { galaxy = 0, nebula = 1, saturn = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

Note: In the group cvm section of this main.cf, the saturn node should be removed.

```
       CFSMount oradata_mnt (
                Critical = 0
                MountPoint = "/oradata"
                BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
                )

       CVMVolDg oradata_voldg (
                Critical = 0
                CVMDiskGroup = oradatadg
                CVMVolume = { oradatavol }
                CVMActivation = sw
                )

       CVMVolDg orabin_voldg (
                Critical = 0
                CVMDiskGroup = orabindg
                CVMVolume = { orabinvol }
                CVMActivation = sw
                )

CFSfsckd vxfsckd (
                )
```

```
        CVMCluster cvm_clus (
                 CVMClustName = ora_cluster
                 CVMNodeId = { galaxy = 0, nebula = 1, saturn = 2 }
                 CVMTransport = gab
                 CVMTimeout = 200
                 )

        CVMVxconfigd cvm_vxconfigd (
                 Critical = 0
                 CVMVxconfigdArgs = { syslog }
                 )
```

Note: In the group CVMCluster cvm_clus section for the main.cf, the saturn node should 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 = "192.168.12.58"
                Address@nebula = "192.168.12.59"
                Address@saturn = "192.168.12.60"
                NetMask = "255.255.240.0"
                )
```

Note: In the group PrivNIC ora_priv section for the main.cf, the saturn node information should be removed.

```
 cvm_clus requires cvm_vxconfigd

 oradata_voldg requires cvm_clus
 ocrvote_voldg requires cvm_clus

 ocrvote_mnt requires vxfsckd
 oradata_mnt requires vxfsckd
oradata_mnt requires oradata_voldg
```

Sample main.cf for adding an Oracle RAC 11g node

Changes to the sample main.cf for adding a node are highlighted in bold for the saturn node.

```
include "types.cf"
include "CFSTypes.cf"
include "MultiPrivNIC.cf"
include "CVMTypes.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"

cluster ora_cluster (
        UserNames = { admin = dOPhOJoLPkPPnXPjOM }
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        CounterInterval = 5
        UseFence = SCSI3
        )


system galaxy (
        )

system nebula (
        )

system saturn (
        )


group cvm (
        SystemList = { galaxy = 0, nebula = 1, saturn = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

Note: In the group cvm section of this main.cf, the saturn node has been added.

```
     CFSMount oradata_mnt (
              Critical = 0
```

```
            MountPoint = "/oradata"
            BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
            )
   CVMVolDg oradata_voldg (
            Critical = 0
            CVMDiskGroup = oradatadg
            CVMVolume = { oradatavol }
            CVMActivation = sw
             )
  CVMVolDg orabin_voldg (
          Critical = 0
          CVMDiskGroup = orabindg
          CVMVolume = { orabinvol }
          CVMActivation = sw
          )


  CVMVolDg ocrvote_voldg (
          Critical = 0
          CVMDiskGroup = ocrvotedg
          Sample configuration files 63
          Sample main.cf files for adding and removing nodes
          CVMActivation = sw
          )


                      CFSfsckd vxfsckd (
                              )


                      CVMCluster cvm_clus (
                               CVMClustName = ora_cluster
                               CVMNodeId = { galaxy = 0, nebula = 1, saturn = 2 }
                               CVMTransport = gab
                               CVMTimeout = 200
                               )
```

Note: In the group CVMCluster cvm_clus section of this main.cf, the saturn node has been added.

```
   CVMVxconfigd cvm_vxconfigd (
              Critical = 0
```

```
            CVMVxconfigdArgs = { syslog }
            )

    MultiPrivNIC multi_priv (
          Critical = 0
          Device@galaxy = { lan1 = 0, lan2 = 1}
          Device@nebula = { lan1 = 0, lan2 = 1}
          Device@saturn = { lan1 = 0, lan2 = 1}
          Address@galaxy = { "192.168.1.1" = 0, "192.168.1.2" = 0, "192.168.2.1" = 1 }
          Address@nebula = { "192.168.1.3" = 0, "192.168.1.4" = 0, "192.168.2.2" = 1 }
          Address@saturn = { "192.168.1.5" = 0, "192.168.1.6" = 0, "192.168.2.3" = 1}
          NetMask = "255.255.255.0"
               )
```

Note: In the group MultiPrivNIC multi_priv section of this main.cf, the saturn node has been added.

```
cvm_clus requires cvm_vxconfigd

oradata_voldg requires cvm_clus
ocrvote_voldg requires cvm_clus

ocrvote_mnt requires vxfsckd
oradata_mnt requires vxfsckd
oradata_mnt requires oradata_voldg
cssd requires multi_priv
```

Sample main.cf for removing an Oracle RAC 11g node

Changes to the sample main.cf for removing a node are highlighted in bold for the saturn node. Note that any saturn node associated references in the following sample main.cf need to be removed. Refer to the two following sample Oracle RAC 11g main.cfs after editing:

See “Sample main.cf for Oracle RAC 11g without Oracle agent” on page 382.

See “Sample main.cf for Oracle RAC 11g with Oracle agent” on page 384.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
```

```
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"


cluster ora_cluster (
        UserNames = { admin = dOPhOJoLPkPPnXPjOM }
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        CounterInterval = 5
        UseFence = SCSI3
        )

system galaxy (
        )

system nebula (
        )

system saturn (
        )

group cvm (
        SystemList = { galaxy = 0, nebula = 1, saturn = 2 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula, saturn }
        )
```

Note: In the group_cvm section for the main.cf, the saturn node should be removed.

```
        CFSMount oradata_mnt (
                Critical = 0
                MountPoint = "/oradata"
                BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
                )

       CVMVolDg oradata_voldg (
                Critical = 0
                CVMDiskGroup = oradatadg
                CVMVolume = { oradatavol }
```

```
            CVMActivation = sw
            )

    CVMVolDg orabin_voldg (
            Critical = 0
            CVMDiskGroup = orabindg
            CVMVolume = { orabinvol }
            CVMActivation = sw
            )



    CFSfsckd vxfsckd (
            )

    CVMCluster cvm_clus (
            CVMClustName = ora_cluster
            CVMNodeId = { galaxy = 1, nebula = 2, saturn = 3 }
            CVMTransport = gab
            CVMTimeout = 200
            )
```

Note: In the group CVMCluster cvm_clus section for the main.cf, the saturn node should be removed.

```
        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                 )


MultiPrivNIC multi_priv (
       Critical = 0
       Device@galaxy = { lan1 = 0, lan2 = 1}
       Device@nebula = { lan1 = 0, lan2 = 1}
       Device@saturn = { lan1 = 0, lan2 = 1}
       Address@galaxy = { "192.168.1.1" = 0, "192.168.1.2" = 0, "192.168.2.1" = 1 }
       Address@nebula = { "192.168.1.3" = 0, "192.168.1.4" = 0, "192.168.2.2" = 1 }
       Address@saturn = { "192.168.1.5" = 0, "192.168.1.6" = 0, "192.168.2.3" = 1 }
       NetMask = "255.255.255.0"
       )
```

Note: In the group MultiPrivNIC multi_priv section for the main.cf, the saturn node should be removed.

```
cvm_clus requires cvm_vxconfigd

oradata_voldg requires cvm_clus
ocrvote_voldg requires cvm_clus

ocrvote_mnt requires vxfsckd
oradata_mnt requires vxfsckd
oradata_mnt requires oradata_voldg
```

Sample main.cf for a four-node SF Oracle RAC campus cluster

The following are the configuration details for a four-node SF Oracle RAC campus cluster:

- Nodes galaxy and nebula are located on one site
- Nodes mercury and jupiter are located on another site
- Has two parallel service groups: cvm and oradb1_grp
- oradb1_grp depends on cvm
- oradb1_grp has Oracle and oradata mount resource

```
include "OracleASMTypes.cf"
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"

cluster rac_cluster101 (
    UserNames = { admin = bopHo }
    Administrators = { admin }
    UseFence = SCSI3
    HacliUserLevel = COMMANDROOT
    )
```

```
system galaxy (
    )

system nebula (
    )

system mercury (
    )

system jupiter (
    )

group cvm (
    SystemList = { galaxy = 0, nebula = 1, mercury = 2, jupiter = 3 }
    AutoFailOver = 2
    Parallel = 1
    AutoStartList = { galaxy, nebula, mercury, jupiter }
    SystemZones = { galaxy = 0, nebula = 0, mercury = 1, jupiter = 1 }
    )

    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
         )


      CFSfsckd vxfsckd (
      )


      CVMCluster cvm_clus (
           CVMClustName = rac_cluster101
           CVMNodeId = { galaxy = 0, nebula = 1, mercury = 2, jupiter = 3 }
           CVMTransport = gab
           CVMTimeout = 200
           )


      CVMVolDg ocrvote_voldg (
          Critical = 0
```

```
    CVMDiskGroup = ocrvotedg
    CVMVolume = { ocrvol, votevol }
    CVMActivation = sw
    )


CVMVxconfigd cvm_vxconfigd (
    Critical = 0
    CVMVxconfigdArgs = { syslog }
    )


PrivNIC ora_priv (
    Critical = 0
    Device@galaxy = { lan1 = 0, lan2 = 1}
    Device@nebula = { lan1 = 0, lan2 = 1}
    Device@mercury = { lan1 = 0, lan2 = 1}
    Device@jupiter = { lan1 = 0, lan2 = 1}
    Address@galaxy = "192.168.12.1"
    Address@nebula = "192.168.12.2"
    Address@mercury = "192.168.12.3"
    Address@jupiter = "192.168.12.4"
    NetMask = "255.255.240.0"
    )


cssd requires ocrvote_voldg
cssd requires ora_priv
cvm_clus requires cvm_vxconfigd
ocrvote_mnt requires ocrvote_voldg
ocrvote_voldg requires vxfsckd
vxfsckd requires cvm_clus


// resource dependency tree
//
// group cvm
// {
// Application cssd
//  {
//   CFSMount ocr_mnt
//    {
//     CVMVolDg ocr_voldg
//      {
```

```
        //       CFSfsckd vxfsckd
        //        {
        //         CVMCluster cvm_clus
        //          {
        //           CVMVxconfigd cvm_vxconfigd
        //          }
        //        }
        //      }
        //    }
        //   PrivNIC ora_priv
        //   }
        //  }


group oradb1_grp (
    SystemList = { galaxy = 0, nebula = 1, mercury = 2, jupiter = 3 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { galaxy, nebula, mercury, jupiter }
    )

    CFSMount oradata_mnt (
        Critical = 0
        MountPoint = "/oradata"
        BlockDevice = "/dev/vx/dsk/oradatadg/oradatavol"
        )

    CVMVolDg oradata_voldg (
        Critical = 0
        CVMDiskGroup = oradatadg
        CVMVolume = { oradatavol }
        CVMActivation = sw
        )

    Oracle ora1 (
        Critical = 0
        Sid @galaxy = vrts1
        Sid @nebula = vrts2
        Sid @mercury = vrts3
        Sid @jupiter = vrts4

        Owner = oracle
        Home = "/app/oracle/orahome"
```

```
            StartUpOpt = "SRVCTLSTART"
            ShutDownOpt = "SRVCTLSTOP"
            )

        requires group cvm online local firm
        ora1 requires oradata_mnt
        oradata_mnt requires oradata_voldg

        // resource dependency tree
        //
        // group oradb1_grp
        // {
        // Oracle ora1
        //  {
        //   CFSMount oradata_mnt
        //   {
        //    CVMVolDg oradata_voldg
        //   }
        //  }
        // }
    group oradb1_grp (
    SystemList = { galaxy = 0, nebula = 1, mercury = 2, jupiter = 3 }
    AutoFailOver = 2
    Parallel = 1
    AutoStartList = { galaxy, nebula, mercury, jupiter }
    SystemZones = { galaxy = 0, nebula = 0, mercury = 1, jupiter = 1 }
    )
```

Appendix B

SF Oracle RAC installation and configuration sample values

This appendix includes the following topics:

Installation and configuration worksheets

The SF Oracle RAC installation and configuration program prompts you for information about SF Oracle RAC. It also provides default values for some information which you can choose to use. The worksheets provide sample values that you can use as examples of the information required for an SF Oracle RAC installation and configuration.

Symantec recommends using the worksheets to record values for your systems before you begin the installation and configuration process.

- Worksheet for installing SF Oracle RAC, its component products, and features:
  See "SF Oracle RAC worksheet" on page 424.
- Worksheet for installing Oracle RAC:
  See "Oracle RAC Worksheets" on page 432.
- Worksheet for replicated clusters using VVR:
  See "Replicated cluster using VVR worksheet" on page 437.
- Worksheet for replicated clusters using SRDF:
  See "Replicated cluster using SRDF worksheet" on page 438.

SF Oracle RAC worksheet

This section provides worksheets for installing and configuring SF Oracle RAC, its component products, and features.

Table B-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 B-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.	

Table B-1 SF Oracle RAC worksheet *(continued)*

Installation information	Sample value	Assigned value
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. See "Obtaining SF Oracle RAC license keys" on page 77. **Note:** You can choose between SF Oracle RAC and SF Oracle RAC Disaster Recovery and High Availability options for license keys.	
Do you want to install required SF Oracle RAC packages or all SF Oracle RAC packages?	Install only the required packages if you do not want to configure any optional components or features. Default option is to install all packages.	
Primary cluster name	rac_cluster101	
Primary cluster ID number	101	
Private network links		
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	

Table B-1 SF Oracle RAC worksheet *(continued)*

Installation information	Sample value	Assigned value
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	
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	

Table B-1 SF Oracle RAC worksheet *(continued)*

Installation information	Sample value	Assigned value
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	
Vxfen disks	disk01, disk02, disk03	
Vxfen disk group	vxfencoordg	

I/O fencing information

Table B-2 displays the information that is required to configure I/O fencing.

Table B-2 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	

Veritas Cluster Server component information

Table B-3 displays the information that is required to configure the Veritas Cluster Server component.

Table B-3 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	
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: Do not use the network interface card that is used for the public network, which is typically lan0.	

Cluster Volume Manager information

Table B-4 displays the information that is required to configure the Cluster Volume Manager.

Table B-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 B-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 B-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.	
Host name of the Symantec Product Authentication Service Root Broker System	Example: venus	

SF Oracle RAC add user information

Table B-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 B-6 SF Oracle RAC add user information

Information	Examples	Assigned values
User name	smith	
User password	Enter 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 B-7 displays the information that is required to configure global clusters.

Note: Global clusters are an optional feature that requires a license.

Table B-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 B-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 B-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.	

Table B-8 Veritas Volume Replicator information *(continued)*

Information	Examples	Assigned values
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 Worksheets

This section provides worksheets for installing and configuring Oracle RAC.

Table B-9 displays examples of information required for installing Oracle RAC.

Table B-9 Required information for installing Oracle RAC

Information	Sample value	Assigned value
Oracle user name	oracle Default is oracle.	
Oracle user id	100	
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.	
Oracle group id	For inventory group as primary group: 1000 For dba group as secondary group: 1001	
Oracle user home directory	/home/oracle	

Table B-9 Required information for installing Oracle RAC *(continued)*

Information	Sample value	Assigned value
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.	

Table B-10 displays the information to configure the private IP addresses for Oracle RAC. Private IP addresses for both the PrivNIC and MultiPrivNIC agents are displayed.

Table B-10 Information required to configure private IP addresses for Oracle RAC

Information	Sample value	Assigned value
Private IP addresses for each node (PrivNIC)	■ On galaxy: 192.168.12.1 ■ On nebula: 192.168.12.2 The PrivNIC resource does not accept leading zeros in the private IP addresses. Make sure that the private IP addresses have a format as displayed in the above examples for galaxy and nebula. Private IP address formats similar to the following are not acceptable and will fail: ■ On galaxy: 192.168.12.01 ■ On nebula: 192.168.12.02	
Private hostnames (set in /etc/hosts)	galaxy-priv, nebula-priv	
VCS resource name for PrivNIC	ora-priv	
Virtual IP address	On galaxy: 10.10.11.1 On nebula: 10.10.11.2	
Virtual hostnames (set in /etc/hosts)	galaxy-vip, nebula-vip	

Table B-10 Information required to configure private IP addresses for Oracle RAC *(continued)*

Information	Sample value	Assigned value
Private IP addresses for each node (MultiPrivNIC)	On galaxy: ■ 192.168.1.1 (Oracle Clusterware) ■ 192.168.1.2 (First UDP to use for the CLUSTER_INTERCONNECT parameter) ■ 192.168.2.1 (Second UDP to use for the CLUSTER_INTERCONNECT parameter) On nebula: ■ 192.168.1.3 (Oracle Clusterware) ■ 192.168.1.4 (First UDP to use for for the CLUSTER_INTERCONNECT parameter) ■ 192.168.2.2 (Second UDP to use for the CLUSTER_INTERCONNECT parameter) One private IP address is to be used for Oracle Clusterware and the other two private IP addresses are to be used for cluster_interconnects (UDP). Symantec also 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 B-10 Information required to configure private IP addresses 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 }	
Netmask for cluster	255.255.255.0	

Table B-11 displays the required information for $CRS_HOME and $ORACLE_HOME on each system.

Table B-11 Required information for $CRS_HOME and $ORACLE_HOME on each system

Information	Sample value	Assigned value
Disk for each node that contains the Oracle Clusterware and database binaries	c1t1d0	
Disk group on each local storage	■ On galaxy: orabindg_galaxy ■ On nebula: orabindg_nebula	
Volume for each local disk group	■ On galaxy: orabinvol_galaxy ■ On nebula: orabinvol_nebula	
File system on each local volume	■ On galaxy: /dev/vx/dsk/orabindg_galaxy/ orabinvol_galaxy ■ On nebula: /dev/vx/dsk/orabindg_nebula/ orabinvol_nebula	
Mount point for each (non-shared) file system	/app (non-shared)	
Directory to install Oracle Clusterware	/app/crshome	
Absolute path of Oracle Clusterware installer	/var/Oracle/clusterware/Disk1	
Absolute path of Oracle database installer	/var/Oracle/database/Disk1	
Directory for Oracle base (ORACLE_BASE)	/app/oracle	
Directory to install Oracle (ORACLE_HOME):	/app/oracle/orahome	
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)	

Table B-11 Required information for $CRS_HOME and $ORACLE_HOME on each system *(continued)*

Information	Sample value	Assigned value
VCS resource names for Oracle Database	oradata_voldg, oradata_mnt	
Global Database Name	vrts.veritas.com (database name.domain)	
SID prefix	ora1	

Table B-12 displays information to create OCR and VOTE-disk volumes and file systems.

Table B-12 Information to create OCR and Voting Disk directories on CFS or raw volumes

Information	Sample value	Assigned value
Shared disk	c2t1d0	
Shared disk group	ocrvotedg	
Volume for shared disk group	ocrvotevol If separate: ocrvol and votevol	
File system on shared volume	/dev/vx/rdsk/ocrvotedg/ocrvotevol	
Volume options OCR and Votedisk	nmirror=3	
Mount point for shared file system	/ocrvote	
Directory for OCR files	/ocrvote/ocr	
Directory for Voting Disk files	/ocrvote/vote	
VCS resource names for Votedisk and OCR	ocrvote_voldg, ocrvote_mnt	
Mount point for archive logs	/oradata	

Replicated cluster using VVR worksheet

Table B-13 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 B-13 Replicated cluster using VVR 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 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 B-13 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 B-14 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 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	

Appendix C

Response Files

This appendix includes the following topics:

- About response files
- Response file installation procedures
- Response file syntax
- Install-only response file example
- Configuration response file example
- Response file variable definitions

About response files

Use response files to standardize and automate installations on multiple clusters.

You can reuse or customize the response files and use them for future installation or configuration activities by invoking the installation script with the `responsefile` option. The response file passes arguments to the installation script to automate the installation.

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.
  For example:
  An install-only response file can be identified by the following string:

  ```
  $CPI::CFG{OPT}{INSTALLONLY}=1;
  ```

  A configure-only response file can be identified by the following string:

```
$CPI::CFG{OPT}{CONFIGURE}=1;
```

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*.

Response file installation procedures

Running the installsfrac program program with the -responsefile option enables you to install and configue SF Oracle RAC within a secure environment, and perform installations on other clusters. You can use the response files that are generated during the installation to reinstall SF Oracle RAC on that cluster, or on other clusters.

To install SF Oracle RAC on other clusters using response files, copy the file to a system in another cluster and manually edit the file as needed.

This section describes the following procedures:

- Re-installation procedure using the response files
- Installation procedure using the response files on other clusters

Re-installation using the response files

When you perform an interactive installation of SF Oracle RAC using the installer, response files are automatically generated in the following directory:

```
/opt/VRTS/install/logs/installsfrac-<installernumber>/ \
installsfrac-<installernumber>.response file
```

The response file name is generated as installsfrac-<installernumber>.response, where the number is random. You can use the response files for future installations on the same machine.

Perform the following steps for a response file re-installation.

Response file re-installation

1. Follow the directions in the SF Oracle RAC installation and configuration chapters to perform a single installation on a single cluster (nodes and their coordination points).

   After you perform a single installation on a single cluster, the following types of response files are created:

- An install-only response file
- A configure response file

2 Locate the response files in the /opt/VRTS/install/logs directory. Identify the install-only response file and the configure response file as described in the following step.

Note: If the directory contains many response files that are generated from earlier installations, determine the response files that you want to use. Then, proceed to identify the install-only response file and the configure response file as described in the following step.

---

3 The install-only response file is created during the SF Oracle RAC installation process. The configure response file is created after an installation reboot and during the subsequent configuration process.

To determine whether the response file is an install-only response file, use the `grep` command on the response file to search for the following string:

```
$CPI::CFG{OPT}{INSTALLONLY}=1;
```

If the string appears in the `grep` command output, the response file is an install-only response file.

To determine whether the response file is a configure response file, use the `grep` command on the response file to search for the following string:

```
$CPI::CFG{OPT}{CONFIGURE}=1;
```

If the string appears in the `grep` command output, the response file is a configure response file.

Note: Both the install-only response file and the configure response file are used for this procedure.

---

4 Use the generated install-only response file to automatically run the cluster installation. The installation is based on the settings in the generated response file.

To start the installsfrac script, enter the following command on that cluster:

```
# installsfrac -responsefile /opt/VRTS/install/logs/ \
installsfrac-<installernumber>/installsfrac-<installernumber>.response
```

Note: The installsfrac-<installernumber>.response is the install-only response file in this step.

By default, the installsfrac program uses SSH for remote communication. To use RSH, specify the -rsh option with the installsfrac program by using the following command:

```
# installsfrac -rsh -responsefile /opt/VRTS/install/logs/ \
installsfrac-<installernumber>/installsfrac-<installernumber>.response
```

Additionally, you must edit the response file to include "$CPI::CFG{OPT}{RSH}=1". Using the vi or another text editor, edit the response file and add the following line. For additional information about response file syntax:

See "Response file syntax" on page 448.

5 After the system reboots, use the configure response file to automatically run the cluster configuration. The configuration is based on the settings in the configure response file. Enter the following command on that cluster:

```
# installsfrac -responsefile /opt/VRTS/install/logs/\
installsfrac-<installernumber>/installsfrac-<installernumber>.response
```

Note: The installsfrac-<installernumber>.response is the configure response file in this step.

By default, the installsfrac program uses SSH for remote communication.

To use RSH, specify the -rsh option with the installsfrac program by using the following command:

```
# installsfrac -rsh -responsefile /opt/VRTS/install/logs/\
installsfrac-<installernumber>/installsfrac-<installernumber>.response
```

Installation using the response file on other clusters

When you perform an interactive installation of SF Oracle RAC using the installer, response files are automatically generated in the following directory:

```
/opt/VRTS/install/logs/installsfrac-<installernumber>/ \
installsfrac-<installernumber>.response file
```

The response file name is generated as installsfrac program-<installernumber>.response, where the installernumber is random. You can use this response file for future installations on other clusters.

Perform the following steps for a response file installation on other clusters:

Response file installation on other clusters

1. Follow the directions in the SF Oracle RAC installation and configuration chapters to perform a single installation on the first cluster using the wanted settings.

   After you perform a single installation on a single cluster, you have the following two response file types:

   - An install-only response file
   - A configure response file

   The install-only response file is created during the SF Oracle RAC installation process. The configure response file is created after an installation reboot and during the subsequent configuration process.

   Note: Both the install-only response file and the configure response file are used for this procedure.

   ---

2. After the installation on the first cluster is complete, review the log and summary files to ensure an error-free installation.

   The installer stores these files within the /opt/VRTS/install/logs directory.

3 Proceed to review the response files located at:

```
/opt/VRTS/install/logs/\
installsfrac-<installernumber>/\
installsfrac-<installernumber>.response
```

Determine which response file is the install-only response file and which response file is the configure response file within this directory.

To determine whether the response file is an install-only response file, use the grep command on the response file to search for the following string:

```
$CPI::CFG{OPT}{INSTALLONLY}=1;
```

If the string appears in the `grep` command output, the response file is an install-only response file.

To determine whether the response file is a configure response file, use the grep command on the response file to search for the following string:

```
$CPI::CFG{OPT}{CONFIGURE}=1;
```

If the string appears in the `grep` command output, the response file is a configure response file.

Note: If the directory contains many response files that are generated from earlier installations, determine the response files that you want to use. Then, proceed to identify the install-only response file and the configure response file as described in the following step.

---

4 Place a copy of both response file types in a directory such as /tmp on the next cluster to install SF Oracle RAC.

5 On the next cluster, edit the copied response files using a text editor (vi).

In particular, modify the hostnames in the response file to the hostnames that are used in the new cluster.

Note: The response files themselves contain information about the variables within them. This information is helpful in understanding the response file variables variables that may require editing.

---

6 For demo or site licenses, the license key in the response file need not be changed. When license keys are “node-locked” to specific cluster nodes, you must edit the license key.

7 Change the permissions on the file to 700.

8 Use the edited install-only response file to automatically run the next cluster installation. The installation is based on the settings in the edited install-only response file.

To start the installsfrac program, enter the following command on that cluster:

```
# installsfrac -responsefile /opt/VRTS/install/logs/\
installsfrac-<installernumber>/\
installsfrac-<installernumber>.response
```

Note: The installsfrac program-<installernumber>.response is the edited install-only response file in this step.

By default, the installsfrac program uses SSH for remote communication. To use RSH, specify the -rsh option with the installsfrac program by using the following command:

```
# installsfrac -rsh -responsefile /opt/VRTS/install/logs/\
installsfrac-<installernumber>/\
installsfrac-<installernumber>.response
```

Additionally, you must edit the response file to include "$CPI::CFG{OPT}{RSH}=1" . Using the vi or another text editor, edit the response file and add the following line. For additional information about response file syntax:

See “Response file syntax” on page 448.

9 After the system reboots, use the edited configure response file to automatically run the next cluster configuration. The configuration is based on the settings in the edited configure response file.

Enter the following command on that cluster:

```
# installsfrac -responsefile /opt/VRTS/install/logs/\
installsfrac-<installernumber>/\
installsfrac-<installernumber>.response
```

Note: The installsfrac-<installernumber>.response is the edited configure response file in this step.

---

10 By default, the installsfrac program uses SSH for remote communication. To use RSH, specify the -rsh option with the installsfrac program by using the following command:

```
# installsfrac -rsh -responsefile /opt/VRTS/install/logs/\
installsfrac-<installernumber>/\
installsfrac-<installernumber>.response
```

11 Repeat steps 2 through 10 for each new cluster installation.

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"];
```

Install-only response file example

The following is an example of an install-only response file with some of its variable definitions:

```
#
# installsfrac configuration values:
#
$CPI::CFG{OBC_IGNOREWARNINGS}=0;
$CPI::CFG{OBC_MODE}="STANDALONE";
$CPI::CFG{OPT}{INSTALLONLY}=1;
$CPI::CFG{OPT}{NOEXTRAPKGS}=1;
$CPI::CFG{OPT}{RSH}=1;
$CPI::CFG{SYSTEMS}=[ qw(galaxy nebula) ];
$CPI::CFG{UPI}="SFRAC";
$CPI::CFG{VCS_ALLOWCOMMS}="Y";
$CPI::CFG{VM_HP_INSTALL_IT}=1;
```

```
1;
# # $CPI::CFG{DONOTINSTALL} is an optional one dimensional list variable.
# This variable defines a list of optional depots not to be
# installed on the systems.
#
# $CPI::CFG{DONOTREMOVE} is an optional one dimensional list variable.
# This variable defines a list of depots not to be removed from the
# systems during uninstall.
#
.
.
.
```

Note: A user can modify the hostnames in the example, (galaxy and nebula) in this response file, to other hostnames. The user can then use this modified response file for installation on another system.

Note: The variables in the response file are defined in Table C-1. The VCS variables in the response file are defined in the Veritas Cluster Server Installation Guide.

Configuration response file example

The following is an example of a configuration response file with some of its variable definitions:

```
#
# installsfrac configuration values:
#
$CPI::CFG{OBC_IGNOREWARNINGS}=0;
$CPI::CFG{OBC_MODE}="STANDALONE";
$CPI::CFG{OPT}{CONFIGURE}=1;
$CPI::CFG{OPT}{RSH}=1;
$CPI::CFG{SFRAC_CONFIG_SFRAC_OPT}=1;
$CPI::CFG{SFRAC_MAIN_MENU_OPT}=2;
$CPI::CFG{SYSTEMS}=[ qw(galaxy nebula) ];
$CPI::CFG{UPI}="SFRAC";
$CPI::CFG{VCS_ALLOWCOMMS}="Y";
$CPI::CFG{VCS_CLUSTERID}=894;
$CPI::CFG{VCS_CLUSTERNAME}="rac_cluster101";
$CPI::CFG{VCS_LLTLINK1}{galaxy}="lan1";
```

```
$CPI::CFG{VCS_LLTLINK1}{nebula}="lan1";
$CPI::CFG{VCS_LLTLINK2}{galaxy}="lan2";
$CPI::CFG{VCS_LLTLINK2}{nebula}="lan2";
$CPI::CFG{VCS_USERENPW}=[ qw(fopHojOlpKppNxpJom) ];
$CPI::CFG{VCS_USERNAME}=[ qw(admin) ];
$CPI::CFG{VCS_USERPRIV}=[ qw(Administrators) ];
$CPI::CFG{VM_NEWNAMES_FILE}{galaxy}=0;
$CPI::CFG{VM_NEWNAMES_FILE}{nebula}=0;

1;
# # $CPI::CFG{DONOTINSTALL} is an optional one dimensional list variable.
# This variable defines a list of optional depots not to be installed
# on the systems.
#
# $CPI::CFG{DONOTREMOVE} is an optional one dimensional list variable.
# This variable defines a list of depots not to be removed from the
# systems during uninstall.
#
.
.
.
```

Note: A user can modify the hostnames, (galaxy and nebula) in this response file, to other hostnames. The user can then use this modified response file for installation on another system.

Note: The variables in the response file are defined in Table C-1. The VCS variables in the response file are defined in Veritas Cluster Server Installation Guide.

Response file variable definitions

Table C-1 lists the variables that are used for installing and configuring SF Oracle RAC.

Variables may be required or optional. However, if some of the optional variables are used, it is necessary to define other optional variables too.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration

Variable	List or Scalar	Description
$CPI::CFG{DONOTINSTALL}	List	Optional This variable defines a list of optional packages not to be installed on the systems.
$CPI::CFG{DONOTREMOVE}	List	Optional This variable defines a list of packages not to be removed from the systems during uninstall.
$CPI::CFG{KEYS}{<SYSTEM>}	List	Optional This variable defines a list of license keys to be registered on the systems during install.
$CPI::CFG{OPT_LOGPATH}	Scalar	Optional This variable defines the location where log files are copied to following an install. The default location is /opt/VRTS/install/logs.
$CPI::CFG{OPT}{CONFIGURE}	Scalar	Optional This variable performs configuration and startup of a product that has previously been installed using the -installonly option.
$CPI::CFG{OPT}{INSTALL}	Scalar	Optional This variable designates a standard installation including licensing, installation, configuration, and startup.
$CPI::CFG{OPT}{INSTALLONLY}	Scalar	Optional This variable installs packages but does not configure or start the product.
$CPI::CFG{OPT}{KEYFILE}	Scalar	Optional This variable defines the location of a ssh keyfile used to communicate with all remote systems.
$CPI::CFG{OPT}{LICENSE}	Scalar	Optional This variable licenses the product only.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration *(continued)*

Variable	List or Scalar	Description
$CPI::CFG{OPT}{NOLIC}	Scalar	Optional This variable installs the product without requiring the entry of a license key.
$CPI::CFG{OPT}{PATCHPATH}	Scalar	Optional This variable defines a location from which all remote systems can install product patches. Typically, the location is an NFS mount.The location must be accessible from all target systems.
$CPI::CFG{OPT}{PKGPATH}	Scalar	Optional This variable defines a location from which all remote systems can install product packages. Typically, the location is an NFS mount.The location must be accessible from all target systems.
$CPI::CFG{OPT}{RSH}	Scalar	Optional This variable uses rsh instead of ssh as the communication method between systems.
$CPI::CFG{OPT}{TMPPATH}	Scalar	Optional This variable defines the location where a working directory is created to store the temporary files and the packages that are needed during the installation. The default location is /var/tmp.
$CPI::CFG{OPT}{UNINSTALL}	Scalar	Optional This variable uninstalls the product.
$CPI::CFG{STOPFAIL_ALLOW}	Scalar	Optional This variable decides whether or not the installer proceeds with the installation when it encounters errors in stopping processes or unloading drivers.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration *(continued)*

Variable	List or Scalar	Description
$CPI::CFG{SYSTEMS}	List	Required This variable defines the list of systems on which the product is to be installed, uninstalled, or configured.
$CPI::CFG{SYSTEMSCFG}	List	Optional This variable defines the list of systems to be recognized for configuration when a secure environment prevents all systems from being installed at once.
$CPI::CFG{UPI}	Scalar	This variable is an abbreviation that defines the product to be installed, uninstalled, or configured.
$CPI::CFG{AT_ROOTDOMAIN}	List	Optional This variable defines the name of the system where the root broker is installed.
$CPI:: CFG{SFRAC_CONFIG_SFRAC_OPT}	Scalar	Required This variable defines the option that needs to be chosen after you choose to configure SF Oracle RAC.
$CPI:: CFG{SFRAC_MAIN_MENU_OPT}	Scalar	Required This variable defines the option that needs to be chosen in the main menu of SF Oracle RAC.
$CPI::CFG{VCS_CLUSTERID}	Scalar	Required This variable is an integer between 0 and 65535, which uniquely identifies the cluster.
$CPI::CFG{VCS_CLUSTERNAME}	Scalar	Required This variable defines the name of the cluster.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration *(continued)*

Variable	List or Scalar	Description
$CPI::CFG{VCS_CSGNETMASK}	Variable	Optional This variable defines the netmask of the virtual IP address to be used by the Cluster Manager (Web Console).
$CPI::CFG{VCS_CSGNIC}	Scalar	Optional This variable defines the virtual IP address to be used by the Cluster Manager (Web Console).
$CPI::CFG{VCS_GCONETMASK}	Scalar	Optional This variable defines the Netmask of the virtual IP address to be used by the Global Cluster Option).
$CPI:: CFG{VCS_GCONIC}{<SYSTEM>}	Scalar	Optional This variable defines the NIC for the Virtual IP used for the Global Cluster Option. 'ALL' can be entered as a system value if the same NIC is used on all systems.
$CPI::CFG{VCS_GCOVIP}	Scalar	Optional This variable defines the virtual IP address to be used by the Global Cluster Option.
$CPI:: CFG{VCS_LLTLINK#}{<SYSTEM>}	Variable	Required This variable defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (LLTLINK1 and LLTLINK2). Up to four LLT links can be configured.
$CPI:: CFG{VCS_LLTLINKLOWPRI}{<SYSTEM>}	Variable	Optional This variable defines a low priority heartbeat link. Typically, LLTLINKLOWPRI is used on a public network link to provide an additional layer of communication.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration *(continued)*

Variable	List or Scalar	Description
$CPI::CFG{VCS_SMTPRECP}	Variable	Optional This variable defines a list of full email addresses (example: user@yourcompany.com) of SMTP recipients.
$CPI::CFG{VCS_SMTPRSEV}	Variable	Optional This variable defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive.
$CPI::CFG{VCS_SMTPSERVER}	Variable	Optional This variable defines the domain-based hostname (example: smtp.yourcompany.com) of the SMTP server to be used for Web notification.
$CPI::CFG{VCS_SNMPCONS}	Variable	Optional This variable defines a list of SNMP console system names.
$CPI::CFG{VCS_SNMPCSEV}	Variable	Optional This variable defines the minimum severity level of messages (Information, Waring, Error, SevereError) that listed SNMP consoles are to receive.
$CPI::CFG{VCS_SNMPPORT}	Variable	Optional This variable defines the SNMP trap daemon port (default=162).
$CPI::CFG{VCS_USERENPW}	Variable	Optional This variable defines an encrypted password for each VCS user.
$CPI::CFG{VCS_USERNAME}	Variable	Optional This variable defines a list of VCS user names.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration *(continued)*

Variable	List or Scalar	Description
$CPI::CFG{VCS_USERPRIV}	Variable	Optional This variable defines each user's VCS privileges.
$CPI:: CFG{VM_DEFAULTDG}{<SYSTEM>}	Variable	Required This variable defines the name of the default disk group.
$CPI::CFG{VM_NO_OPEN_VOLS}	Variable	Required This variable indicates that the user should not be asked if there are any open volumes when vxconfigd is not enabled. Such prompts are asked during uninstallations. (1: affirms there are no open volumes on the system)
$CPI::CFG{VOL_MAX_NMPOOL_SZ}	Variable	Optional This variable defines the vol_max_nmpool_sz tunable.
$CPI::CFG{VOL_MAX_RDBACK_SZ}	Variable	Optional This variable defines the vol_max_rdback_sz tunable.
$CPI::CFG{VOL_MIN_LOWMEM_SZ	Variable	Optional This variable defines the vol_min_lowmem_sz tunable
$CPI::CFG{VOL_RVIO_MAXPOOL_SZ}	Variable	Optional This variable defines the vol_rvio_maxpool_sz tunable.
$CPI::CFG{VRAS_STATS_FREQUENCY}	Variable	Optional This variable defines the frequency for VVR stats collection.
$CPI::CFG{VVR_DATA_PORTS}	Variable	Optional This variable defines the port that is used by VVR for replication.

Table C-1 Response file variables for basic SF Oracle RAC installation and configuration *(continued)*

Variable	List or Scalar	Description
$CPI::CFG{VVR_HB_PORT}	Variable	Optional This variable defines the port that is used for VVR heartbeating.
$CPI:: CFG{VVR_VRADMIND_PORT}	Variable	Optional This variable defines the port that is used for vradmind heartbeating.
$CPI:: CFG{VVR_VXRSYNCD_PORT}	Variable	Optional This variable defines the port that is used by vxrsyncd daemon.

Appendix D

Automatic Storage Management

This appendix includes the following topics:

About ASM

ASM provides an integrated cluster file system and volume management capabilities for Oracle database files. ASM can be configured with the Veritas Volume Manager (VM) or Cluster Volume Manager (CVM) to take advantage of the volume management and DMP multipathing features in the Veritas Storage Foundation for Oracle RAC.

Veritas CVM and ASM integration

ASM can be configured with Veritas Cluster Volume Manager (CVM) to take advantage of the volume management and DMP multipathing features in Veritas Storage Foundation for Oracle RAC. CVM provides uniform device names across all the nodes in the cluster. When a new array is added to a configuration, the upper level logical volumes remain the same to the user.

Dynamic MultiPathing

A key element of SF Oracle RAC is Dynamic MultiPathing (DMP). DMP provides multiple parallel I/O paths between servers and storage which improve both the availability and scalability of servers and storage.

Customers who wish to run ASM with Veritas Storage Foundation can benefit significantly from the DMP capabilities built into SF Oracle RAC. DMP provides maximum availability and performance in large heterogeneous SANs. As such, DMP allows users to confidently standardize on SF Oracle RAC to take full advantage of the agility that results from no longer being locked into a specific storage hardware vendor.

ASM on CVM rules

The following rules must be obeyed when running ASM on CVM:

- Do not create any file systems on VxVM volumes which will be used with ASM. Doing so may cause data corruption and/or result in headers getting overwritten.
- Do not include volumes with file systems or raw volumes in the same diskgroup being assigned to ASM. Veritas raw volumes for ASM should be used exclusively by ASM.
- Do not enable ODM when implementing ASM. ODM is only appropriate for data files residing on the Veritas File system (VxFS and/or CFS). If the user chooses to use Veritas Cluster File System for any other purpose, such as archive logs, ODM is not applicable.
- Do not stripe or concatenate the volumes using Veritas Volume Manager. ASM implements an additional layer of striping above hardware RAID configuration.
- It is recommended that the user create 2 Oracle ASM diskgroups (DGs).
  - Diskgroup1: data files, one set of redo logs, and one set of control files
  - Diskgroup2: Flash Recovery Area, archive logs, and a second set of redo logs and control files

---

Note: Please refer to Oracle's ASM best practices paper for more details.

- A VxVM volume should consist of a single disk/LUN as presented to the operating system.
- Do not change ownership or permissions on the DMP meta nodes, as this could prevent access to storage devices under DMP. For example:

  ```
  /dev/vx/dmp/devicename
  ```

  and

  ```
  /dev/vx/rdmp/devicename
  ```

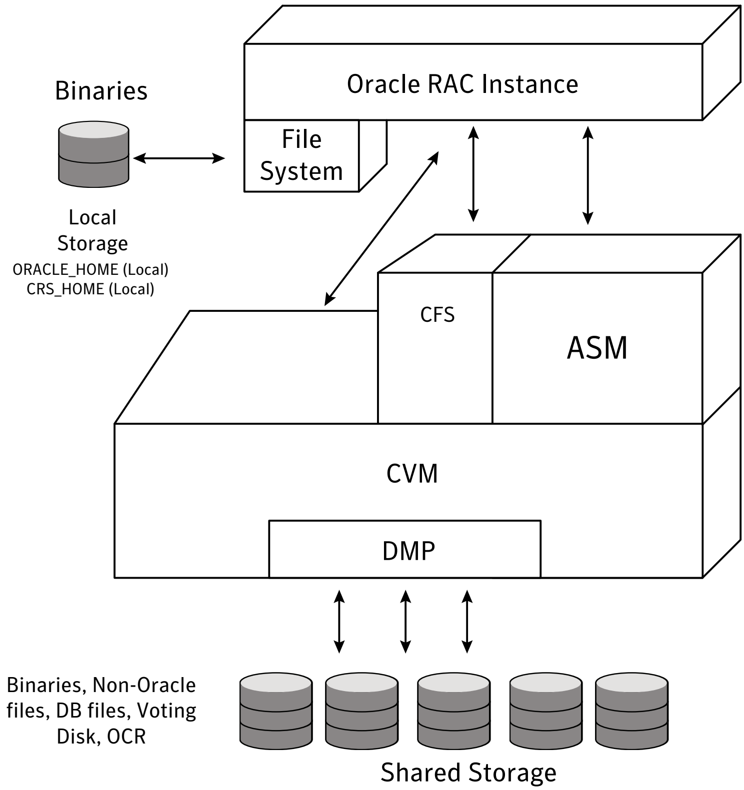
Note: A DMP metanode represents a metadevice, a Veritas Volume Manager abstraction that corresponds to a disk or LUN and all the I/O paths on which it can be accessed.

- Do not attempt to have ASM directly address the DMP meta nodes. All access to DMP meta nodes should be through the appropriate Veritas Volume Manager (clustered or unclustered).
- DMP combined with other multipathing software on the same system is neither allowed nor supported.
- Coordinator disks for I/O fencing cannot be configured under ASM.
- Do not attempt VxVM/CVM virtualization operations, i.e. volume resize, concatenation with LUNs that are under ASM control.
- Volumes presented to a particular ASM diskgroup should be of the same geometry, speed, and type.
- Veritas Storage Foundation commands `vxresize` or `vxassist` are not supported in this configuration.

Supported SF Oracle RAC and ASM configurations

Figure D-1 below shows ASM and Veritas Storage Foundation working together in a clustered (Oracle RAC) configuration. In this figure, clustered versions of the Veritas Volume Manager (CVM) and Veritas File System (CFS) are shown in support of Oracle RAC.

Figure D-1 Supported Oracle RAC configuration



In this Oracle RAC configuration, binaries, clusterware files, and non-Oracle files can be stored in a Cluster File System. Database files are stored and managed by ASM, which can then leverage Storage Foundation Dynamic Multi-pathing (DMP) through Veritas Volume Manager.

Note: For any given host or Oracle RAC cluster only one multipathing solution should be active and managing the underlying devices.

The Oracle RAC Voting Disk and the Oracle Cluster Registry (OCR) (shown at the bottom of the figure) are not managed by ASM in Oracle, but can be stored in Veritas Volume Manager or File System.

Requirements for the supported SF Oracle RAC and ASM configurations

Symantec supports ASM configurations running with the Storage Foundation under the following conditions:

- Support is provided for ASM on any Storage Foundation products that are supported with Oracle 10.2.0.3 and later. Check with Symantec customer support for up to date listings of supported configurations.
- ASM support is provided for configurations that are running over raw logical volumes (VxVM and CVM).

ASM monitoring utilities

ASM offers monitoring utilities, as well as alert log files for troubleshooting. The ASM command line utility (ASMCMD) is useful to administer disk groups and monitor disk space usage.

For any ASM errors, check the corresponding log files for the Oracle instance.

Refer to your Oracle documentation for information about the ASM monitoring utilities and log files.

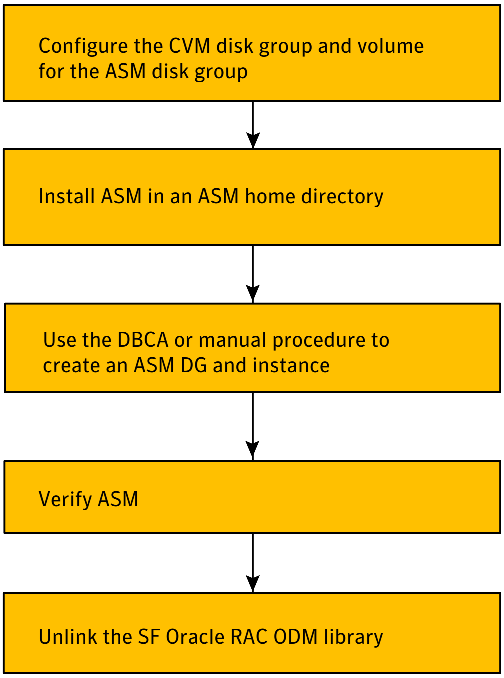
CVM and ASM configuration procedure

The CVM and ASM configuration procedure consists of the following tasks:

- Configure the CVM disk group and volume for the ASM disk group
- Install ASM in an ASM home directory
- Use the DBCA or manual procedure to create an ASM DG and instance
- Verify ASM
- Unlink ODM

Figure D-2 displays a flowchart of the above required tasks.

Figure D-2 CVM and ASM configuration procedure



Warning: Before beginning this process, please review the requirements in See "ASM on CVM rules" on page 460.

Before beginning this process, please review the SF Oracle RAC main.cf file for an Oracle with ASM configuration:

See "Veritas CVM and ASM main.cf file" on page 473.

Configure the CVM disk group and volume for the ASM disk group

As root, configure a CVM disk group using the following commands. The example below illustrates how to create the CVM disk group. This procedure needs to be performed from one node in the case of RAC, but that node must be the CVM master node.

To determine which node is the CVM master node, enter the following command:

```
# vxdctl -c mode
```

Note: This command will only display the CVM master node, if the VxVM cluster feature is enabled.

Configure the CVM disk group and volume for the ASM disk group

1. Enter the following commands for the first disk:

   ```
   galaxy@root# vxdiskunsetup -C c1t12d0
   ```

   ```
   galaxy@root# vxdisksetup -i c1t12d0
   ```

2. Enter the following commands to initialize and configure the disk group:

   ```
   galaxy@root# vxdg -s init ora_asm_dg c1t12d0
   ```

   ```
   galaxy@root# vxassist -g ora_asm_dg make ora_asm_vol 2000M c1t12d0
   ```

   ```
   galaxy@root# vxedit -g ora_asm_dg  \
   set group=dba user=oracle mode=660 ora_asm_vol
   ```

As Oracle user configure ASM using either DBCA or EM. If you do not use either GUI, you will need to manually create the ASM instances and disk groups.

Install Automatic Storage Management in an ASM home directory

Installing ASM in its own home directory enables you to keep the ASM home separate from the database home directory (ORACLE_HOME). With ASM, Oracle recommends that Oracle binaries for the database should be installed in one ORACLE_HOME, and ASM binaries should be installed in a separate, different ORACLE_HOME. By using separate home directories, you can upgrade and patch ASM and the Oracle Database software independently, and you can deinstall Oracle Database software without affecting the ASM instance.

During the installation process, you are asked to configure ASM. You can configure ASM by creating disk groups that become the default location for files created in the database.

When you create a disk group, indicate whether the disk group is a normal redundancy disk group (2-way mirroring for most files by default) or a high-redundancy disk group (3-way mirroring), or an external redundancy disk group (no mirroring by ASM).

The default disk group type is normal redundancy.

To install ASM in an ASM home directory

1. Insert the Oracle CD.
2. Set the DISPLAY variable, mount the CD drive, and run the Oracle installer as Oracle User.

   ```
   # /mnt/cdrom/runInstaller
   ```

3. Read the Welcome screen and click **Next**.

   When you start the Oracle Universal Installer (OUI), the Select a Product to Install window appears.
4. Select the Enterprise Edition for RAC, and then click **Next**.
5. In the Specify Home Details window, specify a name for the ASM home directory, for example, OraASM11g_home. Select a directory that is a subdirectory of your Oracle base directory, for example, /app/oracle/ASM_HOME.

   Click Browse to change the directory in which ASM will be installed.

   After you have specified the ASM home directory, click **Next**. The Specify Hardware Cluster Installation Mode window appears.
6. Click Select All to select all nodes for installation and then click **Next**.

   If your Oracle Clusterware installation was successful, then the Specify Hardware Cluster Mode window lists the nodes that you identified for your cluster, such as galaxy and nebula.

   After you click Next, the Product Specific Prerequisites Checks window appears.

   Follow the OUI wizard instructions for the rest of this procedure.

Use the Oracle DBCA procedure to create ASM disk group and instances

Before performing the Oracle DBCA procedure below, a CVM volume must be created.

See "Configure the CVM disk group and volume for the ASM disk group" on page 464.

Perform the following steps for the Oracle DBCA (Database Creation Assistant) procedure. This procedure can be performed on an Oracle system configuration using either spfiles or pfiles.

Oracle DBCA procedure

1. From the Oracle DBCA interface, select the "Configure ASM Instance" option.
2. Create a default ASM disk group (Eg: DATADG).
3. Choose the appropriate redundancy.
4. Change the Discovery String to “/dev/vx/rdsk/ora_asm_dg/ora_asm*”

   This should list all the VxVM volumes created and available for ASM.
5. Select the disk.

At the completion of this step, the ASM instance should be started and the disk group should be mounted on all nodes of the cluster.

To ensure that the disk group is mounted after a node restart, update the ASM init.ora parameter, asm_diskstring, with the disk group name. If ASM is using a spfile, then this update is done automatically by DBCA.

Verify the disk group status using the following SQL command:

```
SQL>select name, state from v$asm_diskgroup;
```

When using DBCA to create a database, select ASM for storage.

After the ASM disk group is created, all the processes associated with ASM instance start and the init.ora is created for each of the RAC ASM instances. The default ASM instance name is +ASMn where n is the instance number depending on the number of RAC instances.

Verify your ASM installation

Verify that all the database services for ASM are up and running.

To verify that ASM is operational following the installation

1. Change directories to the bin directory in the CRS home directory:

   ```
   cd /app/crshome/bin
   ```

2. Run the following command as the oracle user, where galaxy is the name of the node you want to check:

   ```
   ./srvctl status asm -n galaxy
   ```

   ```
   ASM instance +ASM1 is running on node galaxy
   ```

   The example output shows that there is one ASM instance running on the local node.

3. Repeat the command shown in the step above, substituting nebula for galaxy to verify the successful installation on the other node in your cluster.

Unlinking the SF Oracle RAC ODM library

ODM is only appropriate for data files residing on the Veritas File system. For this reason, do not enable ODM when implementing ASM.

Note: Symantec recommends that in an ASM environment, that the ODM library also be unlinked.

Unlinking the SF Oracle RAC ODM library

1. Log in as the user oracle.
2. Shutdown the instance if it is up:

   ```
   $ srvctl stop asm -n galaxy
   ```

   ```
   $ srvctl stop asm -n nebula
   ```

3. On each node, enter the following command as oracle user:

   ```
   $ cd $ORACLE_HOME/lib
   ```

4 On each node, enter the following command as oracle user.

For Oracle RAC 11g:

```
$ mv $ORACLE_HOME/lib/libodm11.so libodm11.so.veritas
```

For Oracle RAC 10g:

```
$ mv $ORACLE_HOME/lib/libodm10.so libodm10.so.veritas
```

5 On each node, enter the following command as oracle user.

For Oracle RAC 11g:

```
$ ln -s $ORACLE_HOME/lib/libodmd11.so libodm11.so
```

For Oracle RAC 10g:

```
$ ln -s $ORACLE_HOME/lib/libodmd10.so libodm10.so
```

6 Start up the instance:

```
$ srvctl start asm -n galaxy
```

```
$ srvctl start asm -n nebula
```

ASM instance startup and shutdown commands

As user oracle use the following commands for normal startup and shutdown of the ASM instance. These commands can be run from any node of the cluster.

For ASM instance startup, type the following commands:

```
galaxy@oracle> srvctl start asm -n galaxy
```

```
galaxy@oracle> srvctl start asm -n nebula
```

For ASM instance shutdown, type the following command:

```
galaxy@oracle> srvctl stop asm -n galaxy
```

Note: The ASM instance cannot be shut down when database instances which are using ASM are up and running. Use CVM to shut down all database instances that are accessing the ASM instance before shutting down the ASM instance.

Adding additional storage to an ASM disk group with CVM

This section discusses adding additional storage to an ASM disk group with CVM.

Adding additional storage to an ASM disk group with CVM

1 As root user, to add additional storage use the following commands.

```
galaxy@root# vxdiskunsetup -C c1t12d17

galaxy@root# vxdisksetup -i c1t12d17

galaxy@root# vxdg -g ora_asm_dg adddisk c1t12d17

galaxy@root# vxassist -g ora_asm_dg make ora_asm_vol2 2000M
 c1t12d17

galaxy@root# vxedit -g ora_asm_dg set group=dba user=oracle \
mode=660 ora_asm_vol2
```

2 Perform one of the following tasks to either add a disk to an existing ASM disk group or to extend the existing ASM disk size:

- To add a disk to an existing ASM disk group using SQL, enter the following SQL command:

```
SQL>alter diskgroup asm_diskgroup
add disk ora_asm_vol2
```

- To extend the existing ASM disk size, enter the following SQL command as the oracle user:

```
SQL>ALTER DISKGROUP asm_diskgroup
RESIZE DISK ora_asm_vol SIZE 4000M
```

Veritas ASM agents

There are two Veritas ASM agents required for an Oracle ASM configuration with the Veritas Cluster Volume Manager:

- ASMInst agent or ASM Instance agent
- ASMDG agent or ASM DG (disk group) agent

ASMInst agent will online, offline, and monitor the ASM instance.

ASMDG agent will mount, dismount, monitor the ASM disk groups required for ASM enabled databases.

Note: For additional information about these Veritas ASM agents, refer to the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide*.

Veritas CVM and Oracle service group with ASM

A VCS service group is a collection of resources working together to provide application services to clients. A VCS service group typically includes multiple resources that are both hardware and software based.

For additional details on service group dependencies, refer to the *Veritas Cluster Server User's Guide*.

Veritas CVM and an Oracle service group with ASM

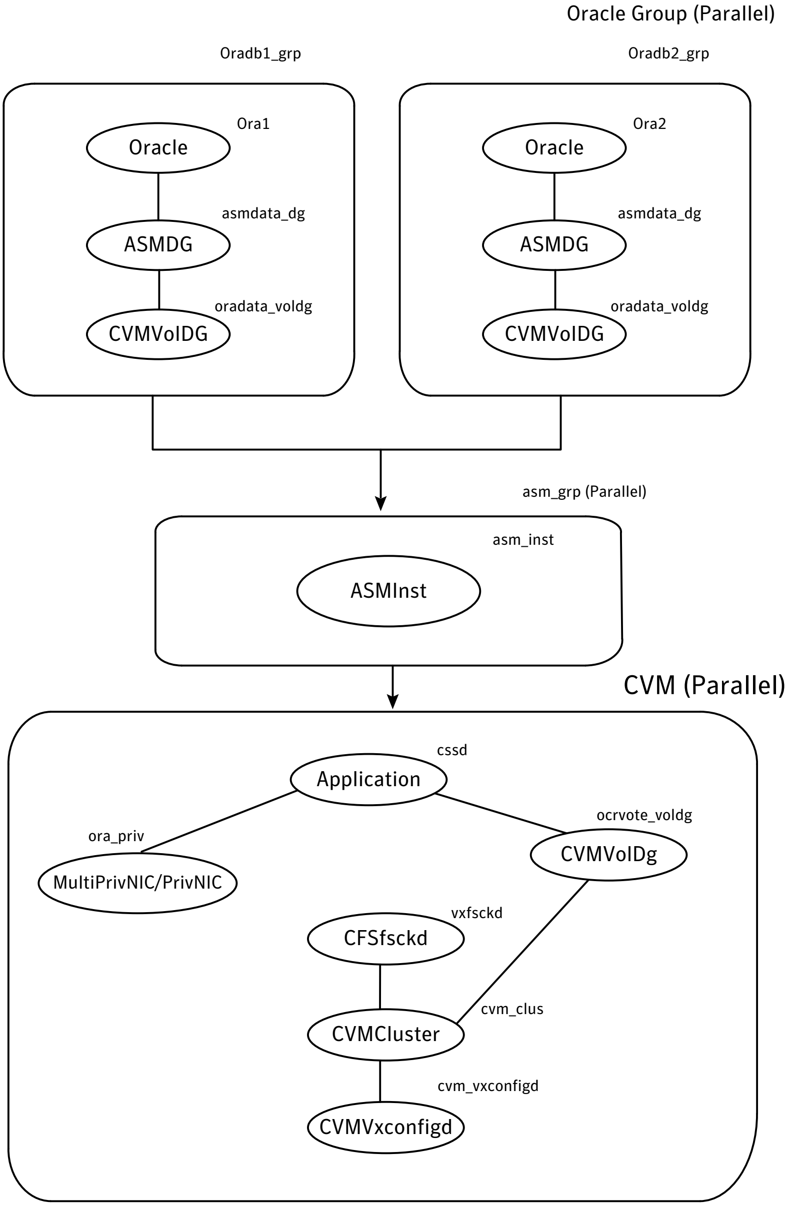
In a configuration with the VCS Oracle agent, VCS controls the Oracle database. An online local firm dependency exists between the Oracle group and the CVM group.

Figure D-3 below shows the VCS configuration for SFRAC with ASM.

The ASMInst agent in the asm_grp service group will online, offline, and monitor the ASM instance. The ASMDG agent in the database service group will mount, dismount, and monitor the ASM disk groups required for ASM enabled databases.

During VCS startup, the ASMDG agent will mount the ASM disk group required for the database, after the CVM volume on which the database resides is started. In case of multiple databases running on one node, it will protect them from each other's failures.

Figure D-3 VCS configuration for SFRAC with Oracle



Veritas CVM and ASM main.cf file

The following is an SF Oracle RAC sample configuration for Oracle RAC 10g with ASM.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"
include "OracleASMTypes.cf"


cluster sfrac_asm (
      UserNames = { admin = bopHo }
      Administrators = { admin }
      UseFence = SCSI3
      HacliUserLevel = COMMANDROOT
      )

system galaxy (
      )

system nebula (
      )


group cvm (
      SystemList = { galaxy = 0, nebula = 1 }
      AutoFailOver = 0
      Parallel = 1
      AutoStartList = { galaxy, nebula }
      )


Application cssd (
      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"
      )
```

```
CFSfsckd vxfsckd (
        )

CVMCluster cvm_clus (
      CVMClustName = sfrac_asm
      CVMNodeId = { galaxy = 0, nebula = 1 }
      CVMTransport = gab
      CVMTimeout = 200
      )


CVMVolDg ocrvoldg (
      Critical = 0
      CVMDiskGroup = ora_crs_shared
      CVMVolume = { crsvol, votevol }
      CVMActivation = sw
      )


CVMVxconfigd cvm_vxconfigd (
      Critical = 0
      CVMVxconfigdArgs = { syslog }
      )


PrivNIC ora_priv (
      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"
      )

cssd requires ocrvoldg
cssd requires ora_priv
cvm_clus requires cvm_vxconfigd
ocrvoldg requires cvm_clus
vxfsckd requires cvm_clus


group asmgrp (
      SystemList = { galaxy = 0, nebula = 1 }
      Parallel = 1
```

```
      AutoStartList = { galaxy, nebula }
      )

ASMInst asm (
      Sid @galaxy = "+ASM1"
      Sid @nebula = "+ASM2"
      Owner = oracle
      Home = "/app/oracle/ASM_HOME"
      )

requires group cvm online local firm


group dbgrp (
      SystemList = { galaxy = 0, nebula = 1 }
      Parallel = 1
      AutoStartList = { galaxy, nebula }
      )

      ASMDG asmdg (
            Sid @galaxy = "+ASM1"
            Sid @nebula = "+ASM2"
            Owner = oracle
            Home = "/app/oracle/ASM_HOME"
            DiskGroups = { ASM_RAC_DG }
            )

     CVMVolDg racvoldg (
           CVMDiskGroup = rac_dg
           CVMVolume = { oradatavol }
           CVMActivation = sw
           )

     Oracle asmdb (
            ResourceOwner = oracle
            Sid @galaxy = vrts1
            Sid @nebula = vrts2
            Owner = oracle
            Home = "/app/oracle/ASM_HOME"
            StartUpOpt = SRVCTLSTART
            ShutDownOpt = SRVCTLSTOP
            )
```

```
requires group asmgrp online local firm
asmdb requires asmdg
asmdg requires racvoldg
```

The following is an SF Oracle RAC sample configuration for Oracle RAC 11g with ASM.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "MultiPrivNIC.cf"
include "OracleTypes.cf"
include "PrivNIC.cf"
include "OracleASMTypes.cf"


cluster sfrac_asm (
      UserNames = { admin = bopHo }
      Administrators = { admin }
      UseFence = SCSI3
      HacliUserLevel = COMMANDROOT
      )

system galaxy (
      )

system nebula (
      )


group cvm (
      SystemList = { galaxy = 0, nebula = 1 }
      AutoFailOver = 0
      Parallel = 1
      AutoStartList = { galaxy, nebula }
      )


Application cssd (
      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"
      )
```

```
                CFSfsckd vxfsckd (
                       )

                CVMCluster cvm_clus (
                      CVMClustName = sfrac_asm
                      CVMNodeId = { galaxy = 0, nebula = 1 }
                      CVMTransport = gab
                      CVMTimeout = 200
                      )


                CVMVolDg ocrvoldg (
                      Critical = 0
                      CVMDiskGroup = ora_crs_shared
                      CVMVolume = { crsvol, votevol }
                      CVMActivation = sw
                      )


                CVMVxconfigd cvm_vxconfigd (
                      Critical = 0
                      CVMVxconfigdArgs = { syslog }
                      )


MultiPrivNIC multi_priv (
            Critical = 0
            Device @galaxy = { lan1= 0, lan2 = 1 }
            Device @nebula = { lan1= 0, lan2 = 1 }
            Address @galaxy = { "192.168.1.1" =0, "192.168.1.2" =0, "192.168.2.1" =1 }
            Address @nebula = { "192.168.1.3" =0, "192.168.1.4" =0, "198.168.2.2" =1 }
            NetMask = "255.255.255.0"
            )



cssd requires ocrvoldg
cssd requires multi_priv
cvm_clus requires cvm_vxconfigd
ocrvoldg requires cvm_clus
vxfsckd requires cvm_clus


group asmgrp (
```

```
        SystemList = { galaxy = 0, nebula = 1 }
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )

ASMInst asm (
        Sid @galaxy = "+ASM1"
        Sid @nebula = "+ASM2"
        Owner = oracle
        Home = "/app/oracle/ASM_HOME"
        )

requires group cvm online local firm


group dbgrp (
        SystemList = { galaxy = 0, nebula = 1 }
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )

        ASMDG asmdg (
                Sid @galaxy = "+ASM1"
                Sid @nebula = "+ASM2"
                Owner = oracle
                Home = "/app/oracle/ASM_HOME"
                DiskGroups = { ASM_RAC_DG }
                )

      CVMVolDg racvoldg (
            CVMDiskGroup = rac_dg
            CVMVolume = { oradatavol }
            CVMActivation = sw
            )

      Oracle asmdb (
              ResourceOwner = oracle
              Sid @galaxy = vrts1
              Sid @nebula = vrts2
              Owner = oracle
              Home = "/app/oracle/ASM_HOME"
              StartUpOpt = SRVCTLSTART
              ShutDownOpt = SRVCTLSTOP
```

```
            )

requires group asmgrp online local firm
asmdb requires asmdg
asmdg requires racvoldg
```

Appendix E

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.

Note: This appendix only discusses the procedures for creating a test database for Oracle RAC 10g and Oracle RAC 11g.

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 CRS, 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 in a shared raw volume or in a cluster file system (CFS). The following sections describe creating database tablespaces for Oracle on either raw volumes or on a file system:

- Creating the database storage on raw volumes
- Creating the database storage on CFS

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 c4t1d2
```

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 c4t2d3
```

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 through step 8.

10 Create the database using the Oracle documentation.

Appendix F

High availability agent information

This appendix includes the following topics:

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 User's Guide*

Other agents included within SF Oracle RAC

SF Oracle RAC includes the following additional agents:

- 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.
- 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.
- ASMInst agent
  The ASMInst agent manages and controls the ASM instance.
- ASMDG agent
  The ASMDG agent mounts and unmounts the ASM disk groups onto an ASM instance.

For more information on the Oracle, Netlsnr, ASMInstance, and ASMDG agents.

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).

Entry points for CVMCluster agent

Table F-1 describes the entry points used by the CVMCluster agent.

Table F-1 CVMCluster agent entry points

Entry Point	Description
Online	Joins a node to the CVM cluster port. Enables the Volume Manager cluster functionality by automatically importing the shared disk groups.
Offline	Removes a node from the CVM cluster port.
Monitor	Monitors the node's CVM cluster membership state.

Attribute definition for CVMCluster agent

Table F-2 describes the user-modifiable attributes of the CVMCluster resource type.

Table F-2 CVMCluster agent attributes

Attribute	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
         )
```

For a more extensive main.cf example that includes the CVMCluster resource:

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.

Entry points for CVMVxconfigd agent

Table F-3 describes the entry points for the CVMVxconfigd agent.

Table F-3 Vxconfigd entry points

Entry Point	Description
Online	Starts the `vxconfigd` daemon
Offline	N/A
Monitor	Monitors whether `vxconfigd` daemon is running

Attribute definition for CVMVxconfigd agent

Table F-4 describes the modifiable attributes of the CVMVxconfigd resource type.

Table F-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.

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 }
        )
```

For a more extensive main.cf that includes the CVMVxconfigd resource:

CVMVolDg agent

The CVMVolDg agent represents and controls CVM diskgroups and CVM volumes within the diskgroups. The global nature of CVM diskgroups and volumes requires importing them only once on the CVM master node.

Configure the CVMVolDg agent for each disk group used by an 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 in the disk group.

Entry points for CVMVolDg agent

Table F-5 describes the entry points used by the CVMVolDg agent.

Table F-5 CVMVolDg agent entry points

Entry Point	Description
Online	Starts all volumes in the shared disk group specified by the CVMVolume attribute. Makes sure that the shared disk groups are imported. Note that the CVMVolDg agent does not import shared disk groups. If the disk group is not imported, the online script returns an error. 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	Sets the diskgroup activation mode to off so that all the volumes in diskgroup are invalid.
Monitor	Monitors specified critical volumes in the diskgroup. The CVMVolume attribute specifies these volumes. SF Oracle RAC requires specifying at least one volume in a diskgroup.
Clean	Cleans up the temporary files created by the online entry point.

Attribute definition for CVMVolDg agent

Table F-6 describes the user-modifiable attributes of the CVMVolDg resource type.

Table F-6 CVMVolDg agent attributes

Attribute	Dimension	Description
CVMDiskGroup	string-scalar	Names the diskgroup.
CVMVolume	string-keylist	Lists critical volumes in the diskgroup. SF Oracle RAC requires specifying at least one volume in the diskgroup.
CVMActivation	string-scalar	Sets the activation mode for the diskgroup. Default = `sw (shared-write)`

CVMVolDg agent type definition

The CVMTypes.cf file includes the CVMVolDg type definition.

```
type CVMVolDg (
        static keylist RegList = { CVMActivation }
        static str ArgList[] = { CVMDiskGroup, CVMVolume,
            CVMActivation }
        str CVMDiskGroup
        keylist CVMVolume[]
        str CVMActivation
        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 (
        CVMDiskGroup = oradatadg
        CVMVolume = { oradata1, oradata2 }
        CVMActivation = sw
         )
```

To see CVMVolDg defined in a more extensive example:

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.

Entry points for CFSMount agent

Table F-7 provides the entry points for the CFSMount agent.

Table F-7 CFSMount agent entry points

Entry Point	Description
Online	Mounts a block device in cluster mode.
Offline	Unmounts the file system, forcing unmount if necessary, and sets primary to secondary if necessary.
Monitor	Determines if the file system is mounted. Checks mount status using the `fsclustadm` command.
Clean	Generates a null operation for a cluster file system mount.

Attribute definition for CFSMount agent

Table F-8 lists user-modifiable attributes of the CFSMount Agent resource type.

Table F-8 CFSMount Agent attributes

Attribute	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 F-8 CFSMount Agent attributes *(continued)*

Attribute	Dimension	Description

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.
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 }
   static int FaultOnMonitorTimeouts = 1

   static int OnlineWaitLimit = 0
   static str ArgList[] = { MountPoint, BlockDevice,
     MountOpt }
   NameRule = resource.MountPoint
   str MountPoint
```

```
str MountType
str BlockDevice
str MountOpt

str Primary

keylist NodeList
keylist Policy
```

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;
        )
```

To see CFSMount defined in a more extensive example:

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.

Note: When you use the PrivNIC agent to provide high availability to a private IP address, do not use the `CLUSTER_INTERCONNECTS` parameter to load balance the interconnect traffic across multiple physical links (by setting multiple IP addresses in the CLUSTER_INTERCONNECTS parameter). Using the parameter for load balancing results in loss of high availability to the private interconnects.

Functions of the PrivNIC agent

Table F-9 describes the PrivNIC agent's monitor entry point.

Note: Because the resource is persistent, only the monitor entry point is required.

Table F-9 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 F-10 describes the user-modifiable attributes of the PrivNIC agent.

Table F-10 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. IP address validation is performed on the numerical private IP address to determine if this is a valid IPv4 address. When configuring private IPv4 addresses for Oracle Clusterware, make sure that there are no leading zeroes in any of the ocetets 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 = "255.255.240.0"`

Optional attributes of the PrivNIC agent

Table F-11 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/llttab` file) differs from the name of the network interface as shown in "ifconfig," then DeviceTag must be specified for that interface.
		For example: in the common case, `/etc/llttab` 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/llttab` 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"`

Table F-11 Optional attributes for PrivNIC agent *(continued)*

Attribute	Dimension	Description
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.
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.

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 = "255.255.240.0"
                )
```

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. Private IP addresses are required by Oracle Clusterware and the Oracle database for communicating between the cluster nodes.

Note: The MultiPrivNIC 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 MultiPrivNIC agent provides a reliable alternative in the following scenarios:

- Operating system limitations prevent you from using NIC bonding to provide increased bandwidth using multiple network interfaces.
- The interconnect traffic needs to be isolated when the cluster is running multiple databases.

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.

Note: When you use the MultiPrivNIC agent to provide high availability to the private IP addresses, do not use the `CLUSTER_INTERCONNECTS` parameter to load balance the interconnect traffic across multiple physical links (by setting multiple IP addresses in the CLUSTER_INTERCONNECTS parameter). Using the parameter for load balancing results in loss of high availability to the private interconnects.

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.

Functions of the MultiPrivNIC agent

Table F-12 below describes the MultiPrivNIC agent's monitor entry point.

Note: Because the resource is persistent, only the monitor entry point is required.

Table F-12 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 MultiPrivNIC agent then applies various filters to this list to determine a most desired failover decision and it 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" device are different, then the MultiPrivNIC agent initiates a failover from the currently active device to the "winner" device.

Attributes of the MultiPrivNIC agent

Table F-13 below describes the user-modifiable attributes of the MultiPrivNIC resource type.

Table F-13 MultiPrivNIC agent attribute definitions

Attribute	Dimension	Description

Device	string-association	The device attribute specifies the network interface device 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 interface with the lower network-id has the higher preference for failover. 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 = {lan0=0, lan1=1, lan2=2}`

Address	string-association	The numerical private IP address and its preferred device.
		
		Checks are performed to determine if this is a valid IP address. When configuring private IP addresses for Oracle Clusterware, ensure that the last 8-bit number in the IPv4 addresses have the format as " X.X.X.1".
		
		The following is an example of an IPv4 address:
		
		`Address @galaxy =`
		`{ "192.168.1.1" =0,`
		`"192.168.1.2" =0,`
		`"192.168.2.1" =1 }`

Netmask	string-association	The netmask attribute is the numerical netmask for the private IP address. For example, Address = "255.255.255.0".

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 MonitorInterval = 20
        static int MonitorTimeout = 300
        static int OfflineMonitorInterval = 20
        static str ArgList[] = {Device, DeviceTag, Address, NetMask, UseVirtualIP,
                                GabPort, UseSystemList, ExcludeNode}
        static str Operations = None
        str Device{}
        str DeviceTag{}
        str Address{}
        str NetMask
        int UseVirtualIP
        str GabPort = o
        int UseSystemList
        int ExcludeNode[]
        )
```

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 = { "192.168.1.1" =0, "192.168.1.2" =0, "192.168.2.1" =1 }
                   Address @nebula = { "192.168.1.3" =0, "192.168.1.4" =0, "192.168.2.2" =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. All links being equal (same number of visible nodes on each of the LLT interfaces), the IP addresses are configured on the preferred interfaces. The MultiPrivNIC agent relies on LLT to monitor the cluster interfaces. The MultiPrivNIC agent 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 which has the maximum nodes. If multiple devices see maximum nodes, the agent considers the current IP traffic on all devices and calculates a "winner" device with lower IP traffic. When the preferred links comes back up again, the IP address corresponding to this link reverts back to it.

Note: The user configures the priority of the devices during SF Oracle RAC installation and configuration.

CSSD agent

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. Using the CSSD agent in SF Oracle RAC installations ensures adequate handling of inter-dependencies and thus prevents the premature startup of Oracle Clusterware, which causes cluster failures.

During system startup, the Oracle Clusterware init scripts invoke the `clsinfo` script provided by Veritas software. The clsinfo script ensures 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.

During system shutdown, the agent stops Oracle Clusterware before the OCR and voting disk resources are taken offline. This ensures that Oracle Clusterware 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.

Functions of the CSSD agent

Table F-14 describes the functions of the CSSD agent.

Table F-14 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 F-15 lists the required attributes of the CSSD agent:

Table F-15 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

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-resource (
    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 506.
  See "Resource type definition for the Oracle agent" on page 512.
- The Netlsnr agent monitors the listener process.
  See "Netlsnr agent functions" on page 517.
  See "Resource type definition for the Netlsnr agent" on page 517.
- The ASMInst agent monitors the Oracle ASM instance.
  See "ASMInst agent functions" on page 521.
  See "Resource type definition for the ASMInst agent" on page 521.
- The ASMDG agent monitors the Oracle ASM disk groups.
  See "ASMDG agent functions" on page 524.
  See "Resource type definition for the ASMDG agent" on page 525.

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 F-16 lists the Oracle agent functions.

Table F-16 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 508.
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 509.

Table F-16 Oracle agent functions *(continued)*

Agent operation	Description
Action	Performs the predefined actions on a resource. See "Action entry point for SF Oracle RAC agent for Oracle" on page 510.

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 the agent must perform basic monitoring in Process check or Health check mode.

Table F-17 describes the basic monitoring options.

Table F-17 Basic monitoring options

Option	Description
0 (Default)	Process check The agent scans the process table for the ora_dbw, ora_smon, ora_pmon, and ora_lgwr processes to verify that Oracle is running.
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.

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 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 F-19 on page 511.

Table F-18 describes the agent's predefined actions.

Table F-18 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.

Table F-18 Predefined agent actions *(continued)*

Action	Description
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 F-19 lists the virtual fire drill actions of the Veritas Cluster Server agent for Oracle lets you run infrastructure checks and fix specific errors.

Table F-19 Predefined virtual fire drill actions

Virtual fire drill action	Description
getid (Oracle agent)	Verifies that the Oracle Owner exists on the node.
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 listener.ora file, 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, EnvFile, AutoEndBkup, DetailMonitor,
        User, Pword, Table, MonScript, AgentDebug, Encoding,
        MonitorOption }
    str Sid
    str Owner
    str Home
    str Pfile
    str StartUpOpt = STARTUP_FORCE
    str ShutDownOpt = IMMEDIATE
    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 int IntentionalOffline = 1

)
```

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 F-20 lists the required attributes. You must assign values to the required attributes.

Table F-20 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, as the defined owner of executables and database files in /etc/passwd.
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 F-21 lists the optional attributes for Oracle agent. You can configure the optional attributes if necessary.

Table F-21 Optional attributes for Oracle agent

Optional Attributes	Type and Dimension	Definition
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.

Table F-21 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
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.
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 Default = 0 See "Monitor options for the Oracle agent" on page 508.

Table F-21 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
DetailMonitor	integer-scalar	Setting this flag to a non-zero enables detail monitoring for Oracle. 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 monitor intervals. **Note:** If you set the AutoEndBkup attribute value to 0, then you must set the DetailMonitor attribute value to 1. 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.
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	string-scalar	Table for update by `User/Pword`.

Table F-21 Optional attributes for Oracle agent *(continued)*

Optional Attributes	Type and Dimension	Definition
Encoding	string-scalar	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default is "".
IntentionalOffline		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 *Veritas Cluster Server User's Guide*.
AgentDebug	boolean-scalar	Additional debug messages are logged when this flag is set. Default = 0

Table F-22 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 F-22 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 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 F-23 lists the Netlsnr agent functions.

Table F-23 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)
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 510.

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 }
    str Owner
    str Home
    str TnsAdmin
    str Listener
    str EnvFile
    str MonScript = "./bin/Netlsnr/LsnrTest.pl"
    str LsnrPwd
    boolean AgentDebug = 0
    str Encoding
    static int 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 F-24 lists the required attributes for Netlsnr agent. You must assign values to the required attributes.

Table F-24 Required attributes for Netlsnr agent

Required attributes	Type and dimension	Definition
Owner	string-scalar	Oracle user, as the defined owner of executables and database files in /etc/passwd.
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 F-25 lists the optional attributes for Netlsnr agent. You can configure the optional attributes if necessary.

Table F-25 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 F-25 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.
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 F-26 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 F-26 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.

ASMInst agent functions

The ASMInst agent monitors the processes of ASM instance.

Table F-27 lists the ASMInst agent operations.

Table F-27 ASMInst agent operations

Agent operation	Description
Monitor	Verifies the status of the ASM instance. The ASMInst agent monitors the ASM instance using the Health check monitoring method. If the Health check monitoring fails, the agent does Process check monitoring. The agent also checks if the ocssd.bin process is running. The agent returns offline for the following conditions: ■ The process is not running. ■ The process is restarted. **Note:** Make sure that the OCSSD process is running. The ASMInst agent only monitors the OCSSD process. The agent does not start or stop the process.
Clean	Forcibly stops the Oracle ASM instance by using the following SQL command: `shutdown abort` If the process does not respond to the `shutdown` command, the agent kills the process using the `SIGTERM` or `SIGKILL` commands.

Resource type definition for the ASMInst agent

The ASMInst agent of the Veritas Cluster Server agent for Oracle is represented by the ASMInst resource type in SF Oracle RAC.

```
type ASMInst (
    static str AgentDirectory = "/opt/VRTSagents/ha/bin/ASMInst"
    static str ArgList[] = { Sid, Owner, Home, Pfile,
    EnvFile, Encoding }
    str Sid
    str Owner
    str Home
    str Pfile
    str EnvFile
    str Encoding
    )
```

Attribute definition for the ASMInst agent

Review the description of the ASMInst agent attributes. The agent attributes are classified as required, optional, and internal.

Table F-28 lists the required attributes. You must assign values to the required attributes.

Table F-28 Required attributes for ASMInst agent

Required attributes	Type and dimension	Definition
Sid	string-scalar	The variable $ORACLE_SID that represents the ASM instance. The Sid is considered case-sensitive by the ASMInst agent.
Owner	string-scalar	The Oracle user, as the defined owner of $ORACLE_HOME of ASM instance and in /etc/passwd.
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 F-29 lists the optional attributes for ASMInst agent. You can configure the optional attributes if necessary.

Table F-29 Optional attributes for ASMInst agent

Optional Attributes	Type and Dimension	Definition
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 of ASM instance 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.
Encoding	string-scalar	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default is "".

Table F-30 lists the internal attribute for ASMInst agent. This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table F-30 Internal attributes for ASMInst agent

Optional Attributes	Type and Dimension	Definition
AgentDirectory	static-string	Specifies the location of binaries, scripts, and other files related to the ASMInst agent. Default is /opt/VRTSagents/ha/bin/ASMInst.

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 DiskGroup attribute of the ASMDG agent.

Table F-31 lists the ASMDG agent operations.

Table F-31 ASMInst 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

Table F-31 ASMInst agent operations *(continued)*

Agent operation	Description
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, DiskGroups,
    EnvFile, Encoding }
    str Sid
    str Owner
    str Home
    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 F-32 lists the required attributes. You must assign values to the required attributes.

Table F-32 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. The Sid is considered case-sensitive by the ASMInst agent.
Owner	string-scalar	The Oracle user, as the defined owner of $ORACLE_HOME of ASM instance and in /etc/passwd.
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 F-33 lists the optional attributes for ASMDG agent. You can configure the optional attributes if necessary.

Table F-33 Optional attributes for ASMDG agent

Optional Attributes	Type and Dimension	Definition
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.

Table F-33 Optional attributes for ASMDG agent *(continued)*

Optional Attributes	Type and Dimension	Definition
Encoding	string-scalar	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default is "".

Table F-34 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 F-34 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.

Appendix G

SF Oracle RAC deployment scenarios

This appendix includes the following topics:

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`

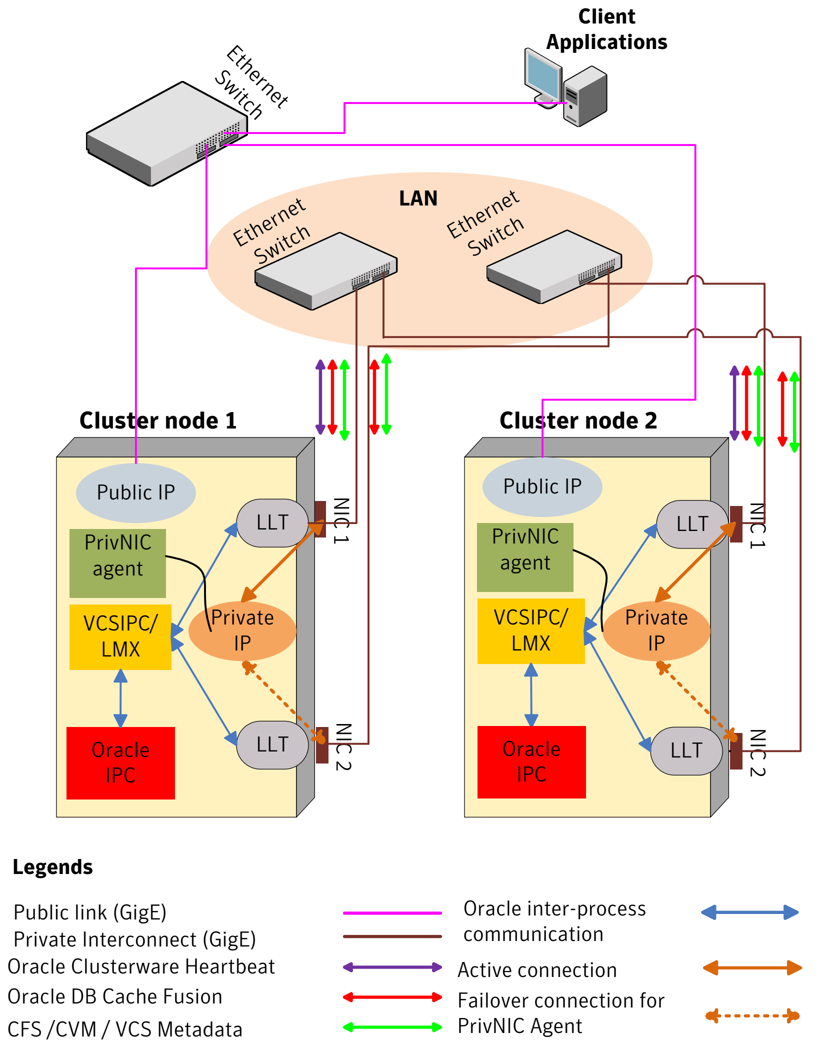
In the illustrated configuration:

- 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 G-1 illustrates the logical view of a two-node SF Oracle RAC cluster with VCS IPC and PrivNIC agent (Oracle RAC 10g).

Figure G-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 10g or Oracle RAC 11g 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:

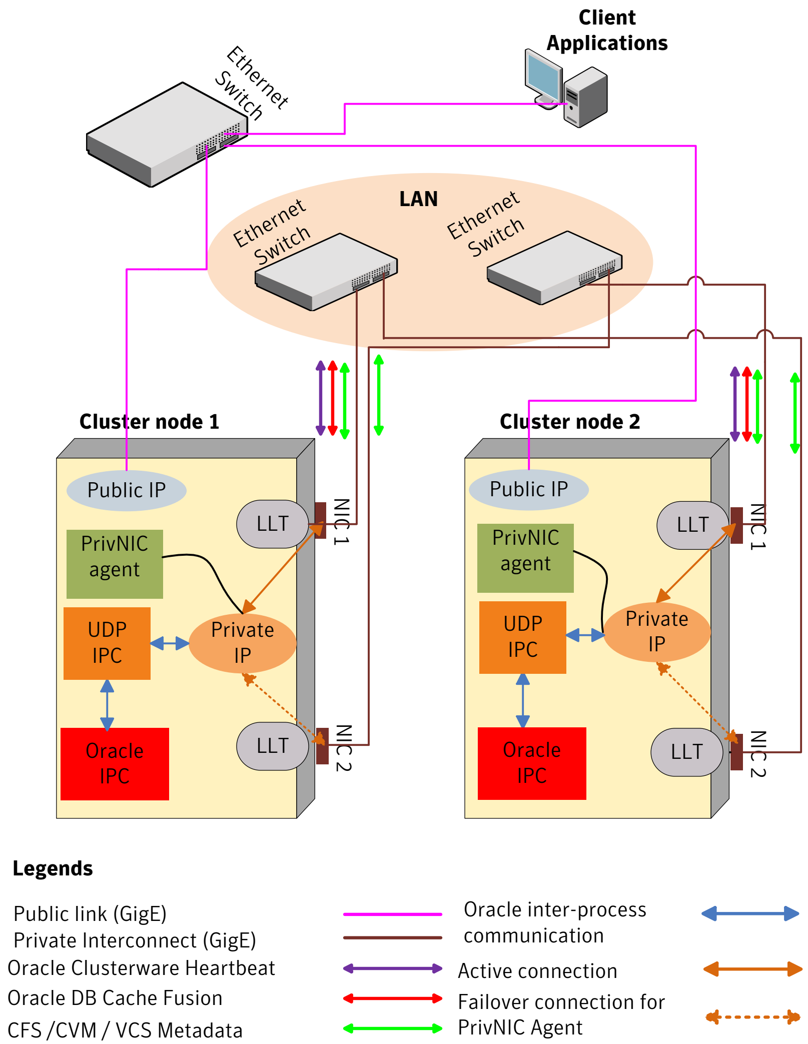
- A common IP address is used for Oracle Clusterware communication and Oracle database cache fusion.

Note: You need to specify the private network IP address used for Oracle database cache fusion in the `CLUSTER_INTERCONNECTS` initialization parameter. Remove the `cluster_interconnect` entry, if it exists in the OCR, using the following command:`$ oifcfg delif`.

- 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 G-2 illustrates the logical view of a two-node SF Oracle RAC cluster with UDP IPC and PrivNIC agent (Oracle RAC 10g/Oracle RAC 11g).

Figure G-2 SF Oracle RAC cluster with UDP IPC and PrivNIC agent (Oracle RAC 10g/Oracle RAC 11g)



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 10g or Oracle RAC 11g 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:

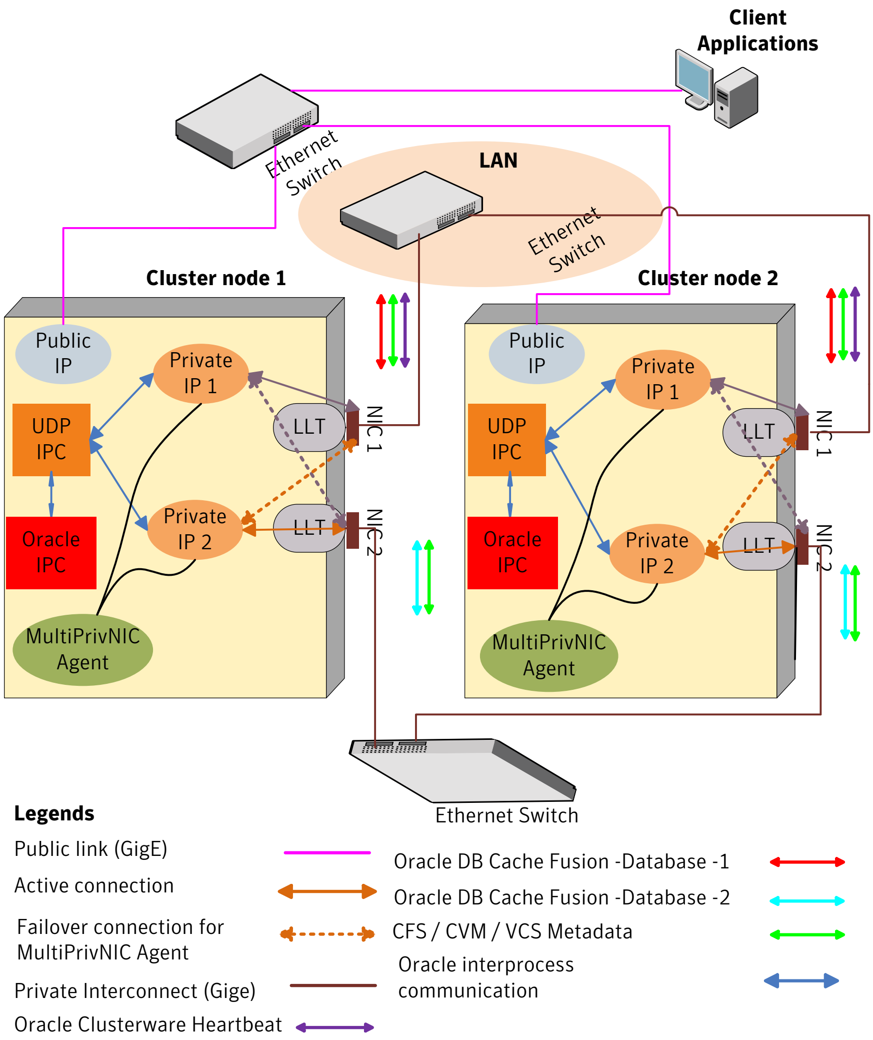
- One private IP address is used for each database for database cache fusion. One of the private IP addresses used for the database cache fusion is shared by Oracle Clusterware communication.

  Note: You need to specify the private network IP address used for Oracle database cache fusion in the `CLUSTER_INTERCONNECTS` initialization parameter for each database. Remove the `cluster_interconnect` entry, if it exists in the OCR, using the following command:`$ oifcfg delif`.

  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 G-3 illustrates the logical view of a two-node SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent (Oracle RAC 10g/Oracle RAC 11g).

Figure G-3 SF Oracle RAC cluster for multiple databases with UDP IPC and MultiPrivNIC agent (Oracle RAC 10g/Oracle RAC 11g)



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 10g or Oracle RAC 11g 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:

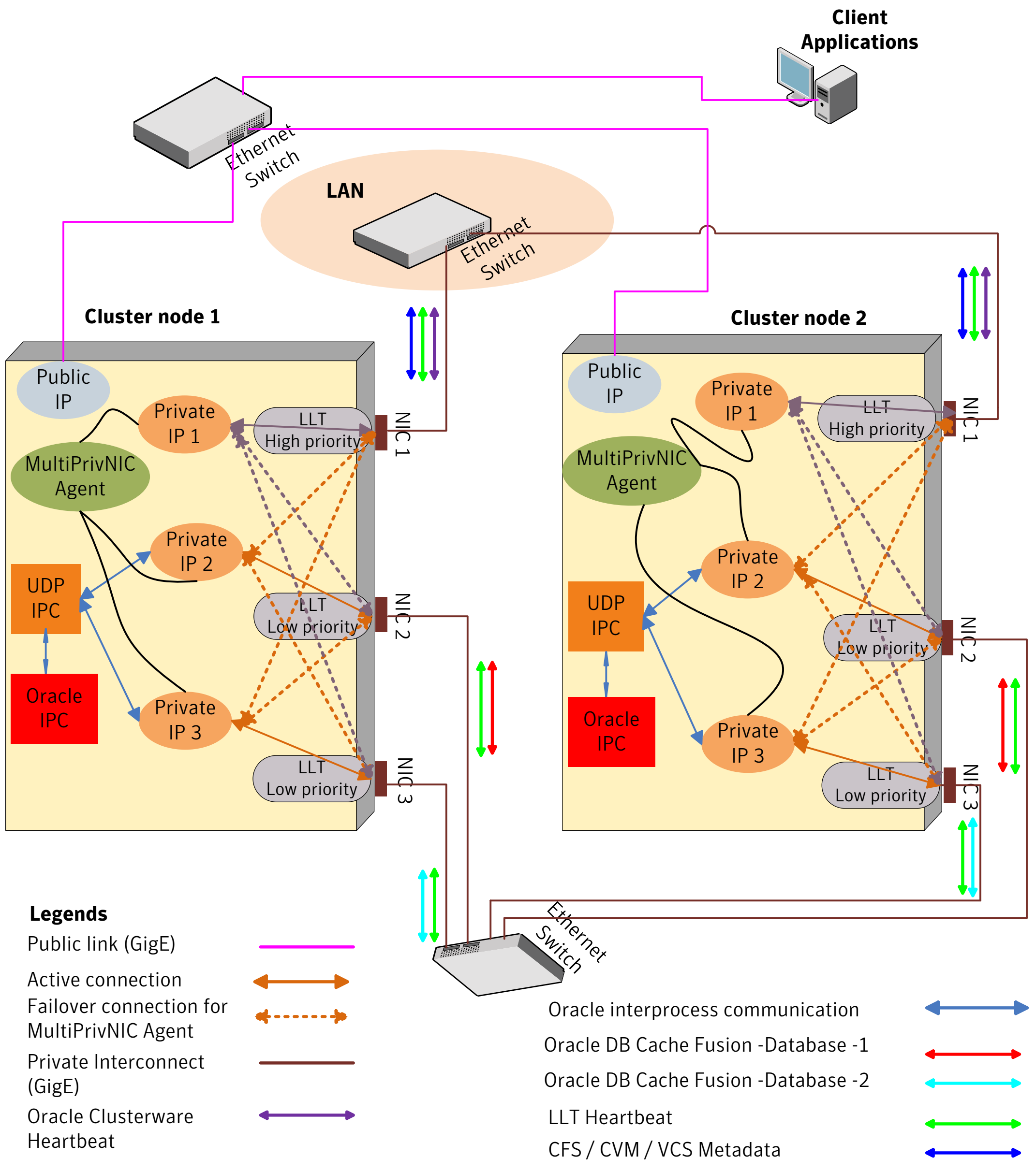
- The private network IP address used for database cache fusion is configured over a dedicated link for each database. These links are configured as low-priority LLT links.

Note: You need to specify the private network IP addresses used for Oracle database cache fusion in the `CLUSTER_INTERCONNECTS` initialization parameter. Remove the `cluster_interconnect` entry, if it exists in the OCR, using the following command: `$ oifcfg delif`

- 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 G-4 illustrates the logical view of a two-node SF Oracle RAC cluster with Oracle traffic isolated from VCS / CVM / CFS traffic (Oracle RAC 10g/Oracle RAC 11g).

Figure G-4 SF Oracle RAC cluster with isolated Oracle traffic and MultiPrivNIC agent (Oracle RAC 10g/Oracle RAC 11g)



SF Oracle RAC cluster with NIC bonding, VCS IPC and PrivNIC agent

This section illustrates the recommended configuration for the following scenario:

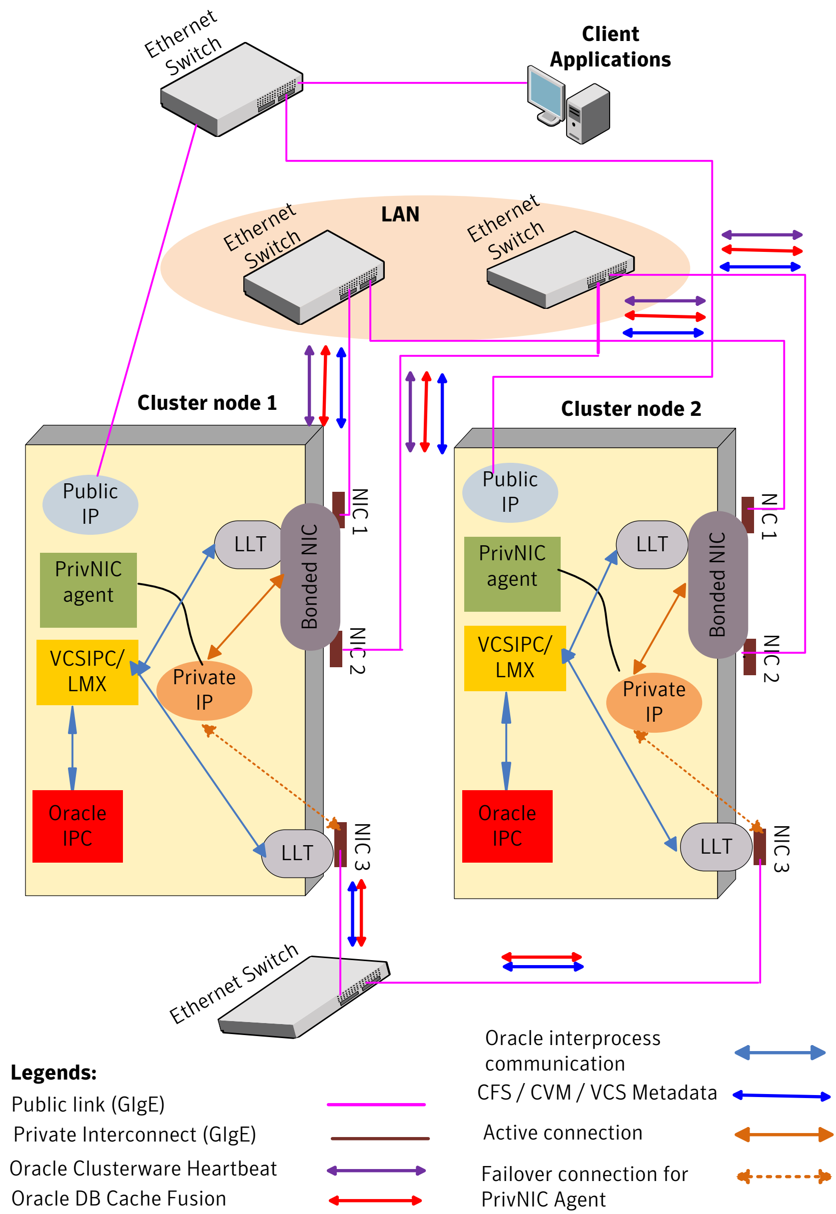
Deployment scenario	A bonded NIC interface is used along with another NIC interface to distribute Oracle RAC 10g database cache fusion traffic using VCS IPC over LMX/LLT.
Recommendation	Use the PrivNIC agent.
Sample main.cf configuration file	The following sample main.cf file describes the configuration: `/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 G-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 G-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 10g or Oracle RAC 11g 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:

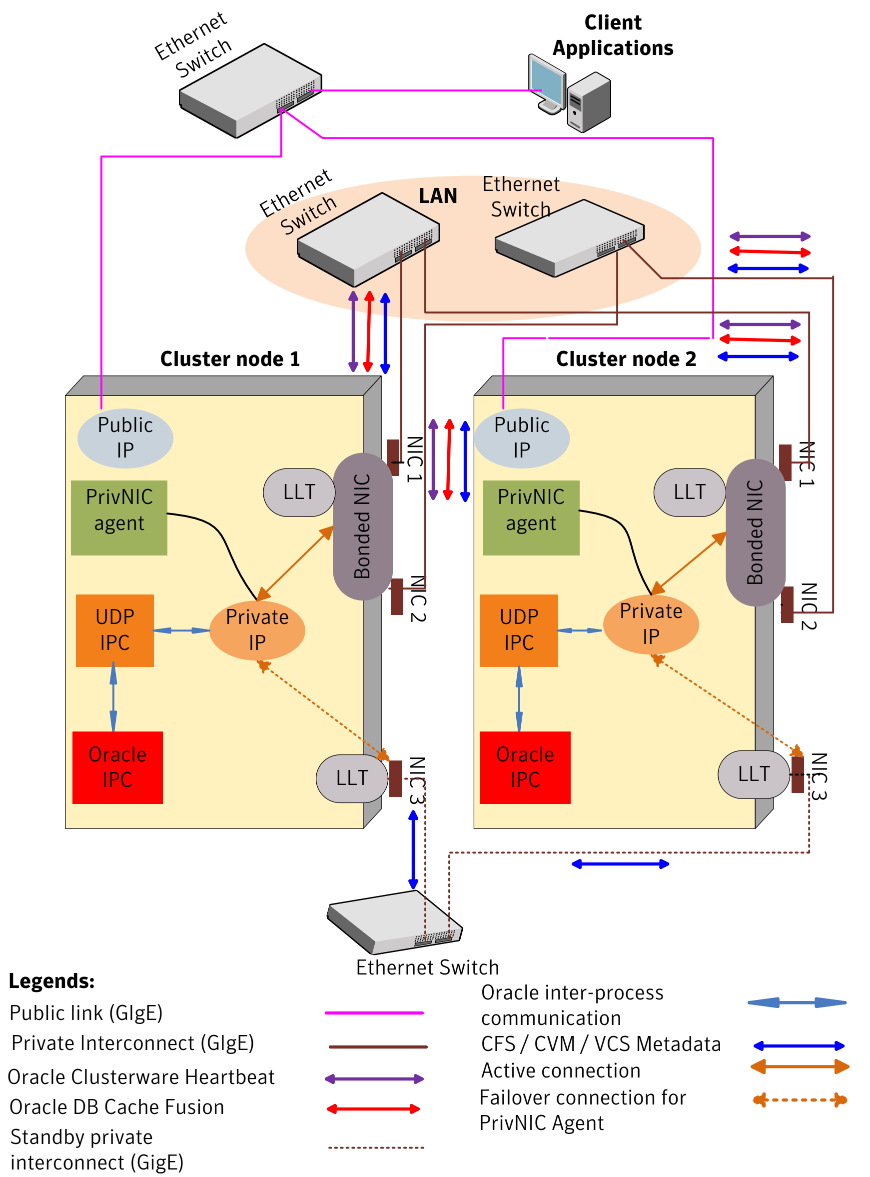
- A common IP address is used for Oracle Clusterware communication and Oracle database cache fusion that is distributed over two underlying physical links of the bonded NIC interface. The bonded NIC interface is configured as a single LLT link.

  Note: You need to specify the private network IP addresses used for Oracle database cache fusion in the `CLUSTER_INTERCONNECTS` initialization parameter. Remove the `cluster_interconnect` entry, if it exists in the OCR, using the following command:`$ oifcfg delif`

- 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 G-6 illustrates the logical view of a two-node SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent.

Figure G-6 SF Oracle RAC cluster with NIC bonding, UDP IPC, and PrivNIC agent



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 Multipathing)	A feature of Veritas Volume Manager 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.
DST (Dynamic Storage Tiering)	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. See also Veritas File System (VxFS)
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 SF Manager 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.

SFCFS (Storage Foundation Cluster File System)

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. VxVM 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

O

S

W