Veritas Storage Foundation™ for Sybase ASE CE Installation and Configuration Guide

Solaris

6.0

February 2012

Veritas Storage Foundation for Sybase ASE CE 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: 6.0

Document version: 6.0.2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

doc_feedback@symantec.com

About Symantec Connect

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

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

Contents

Section 1

Installation overview and planning

Chapter 1

Introducing Veritas Storage Foundation for Sybase ASE CE

This chapter includes the following topics:

About Veritas Storage Foundation for Sybase ASE CE

Veritas Storage Foundation™ for Sybase® Adaptive Server Enterprise Cluster Edition (SF Sybase CE) by Symantec leverages proprietary storage management and high availability technologies to enable robust, manageable, and scalable deployment of Sybase ASE CE on UNIX platforms. The solution uses cluster file system technology that provides the dual advantage of easy file system management as well as the use of familiar operating system tools and utilities in managing databases.

SF Sybase CE integrates existing Symantec storage management and clustering technologies into a flexible solution which administrators can use to:

- Create a standard toward application and database management in data centers. SF Sybase CE provides flexible support for many types of applications and databases.
- Set up an infrastructure for Sybase ASE CE that simplifies database management while fully integrating with Sybase clustering solution.
- Apply existing expertise of Symantec technologies toward this product.

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 Sybase CE

SF Sybase CE provides the following benefits:

- Use of a generic clustered file system (CFS) technology or a local file system (VxFS) technology for storing and managing Sybase ASE CE installation binaries.
- Support for file system-based management. SF Sybase CE provides a generic clustered file system technology for storing and managing Sybase ASE CE data files as well as other application data.
- Use of Cluster File System (CFS) for the Sybase ASE CE quorum device.
- Support for a standardized approach toward application and database management. A single-vendor solution for the complete SF Sybase CE software stack lets you devise a standardized approach toward application and database management. Further, administrators can apply existing expertise of Veritas technologies toward SF Sybase CE.
- Easy administration and monitoring of SF Sybase CE clusters from a single web console.
- Enhanced scalability and availability with access to multiple Sybase ASE CE instances per database in a cluster.
- Prevention of data corruption in split-brain scenarios with robust SCSI-3 Persistent Reservation (PR) based I/O fencing.
- Support for sharing all types of files, in addition to Sybase ASE CE database files, across nodes.
- Increased availability and performance using Veritas Dynamic Multi-Pathing (DMP). DMP provides wide storage array support for protection from failures and performance bottlenecks in the Host Bus Adapters (HBAs) and Storage Area Network (SAN) switches.

- Fast disaster recovery with minimal downtime and interruption to users. Users can transition from a local high availability site to a wide-area disaster recovery environment with primary and secondary sites. If a node fails, clients that are attached to the failed node can reconnect to a surviving node and resume access to the shared database. Recovery after failure in the SF Sybase CE environment is far quicker than recovery for a failover database.
- Support for block-level replication using VVR.

For more information on the SF Sybase CE components, see the following documents:

Veritas Storage Foundation for Sybase ASE CE Installation and Configuration Guide

Veritas Storage Foundation for Sybase ASE CE Administrator's Guide

About SF Sybase CE components

SF Sybase CE manages database instances running in parallel on multiple nodes using the following architecture and communication mechanisms to provide the infrastructure for Sybase ASE CE.

Table 1-1 SF Sybase CE component products

Component product	Description
Cluster Volume Manager (CVM)	Enables simultaneous access to shared volumes based on technology from Veritas Volume Manager (VxVM).
Cluster File System (CFS)	Enables simultaneous access to shared file systems based on technology from Veritas File System (VxFS).
Cluster Server (VCS)	Uses technology from Veritas Cluster Server to manage Sybase ASE CE databases and infrastructure components.
VXFEN	The VCS module prevents cluster corruption through the use of SCSI3 I/O fencing.
VXFEND	The VXFEN daemon communicates directly with VCMP and relays membership modification messages.
VCMP	VCMP provides interface between Sybase cluster and the SF Sybase CE components.
QRMUTIL	QRMUTIL provides Sybase instance status.

Table 1-1 SF Sybase CE component products *(continued)*

Component product	Description
Sybase agent	The VCS agent is responsible for bringing Sybase ASE online, taking it offline, and monitoring it.. It obtains status by checking for processes, performing SQL queries on a running database, and interacting with QRMUTIL.

See "About Veritas Storage Foundation for Sybase ASE CE" on page 21.

About SF Sybase CE optional features

You can configure the following optional features in an SF Sybase CE cluster:

- VCS notifications
  See "About VCS notifications" on page 24.
- Global clusters
  See "About global clusters" on page 24.
- Veritas Volume Replicator
  See "About Veritas Volume Replicator" on page 25.

About VCS notifications

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

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

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

About global clusters

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

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) replicates data to remote locations over any standard IP network to provide continuous data availability. It is a fully integrated component of Veritas Volume Manager (VxVM). VVR is available as an optional, separately-licensed feature of SF Sybase CE.

VVR replicates the application writes on the volumes at the source location to one or more remote locations across any distance. It provides a consistent copy of application data at the remote locations. If a disaster occurs at the source location, you can use the copy of the application data at the remote location and restart the application at the remote location. The host at the source location on which the application is running is known as the Primary host. The host at the target location is known as the Secondary host. You can have up to 32 Secondary hosts in a VVR environment. VVR provides several methods to initialize the application data between the primary location and the remote location. Some of the methods include using the network, using the tape backup, and moving the disks physically.

About I/O fencing

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

The fencing operation determines the following:

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

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

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

See “About planning to configure I/O fencing” on page 42.

See the *Veritas Storage Foundation for Sybase ASE CE Administrator's Guide*.

About preferred fencing

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

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

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

See the *Veritas Storage Foundation for Sybase ASE CE Administrator's Guide* for more details.

About Cluster Manager (Java Console)

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

See *Veritas Cluster Server Administrator's Guide*.

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

About Veritas Operations Manager

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

Veritas Operations Manager provides a centralized management console for Veritas Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports.

You can download Veritas Operations Manager at no charge at http://go.symantec.com/vom.

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

Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

Among its broad set of features, SORT lets you do the following:

- Generate server-specific reports that describe how to prepare your servers for installation or upgrade of Symantec enterprise products.
- Access a single site with the latest production information, including patches, agents, and documentation.
- Create automatic email notifications for changes in patches, documentation, and array-specific modules.

To access SORT, go to:

https://sort.symantec.com

SF Sybase CE cluster setup models

SF Sybase CE supports a variety of cluster configurations.

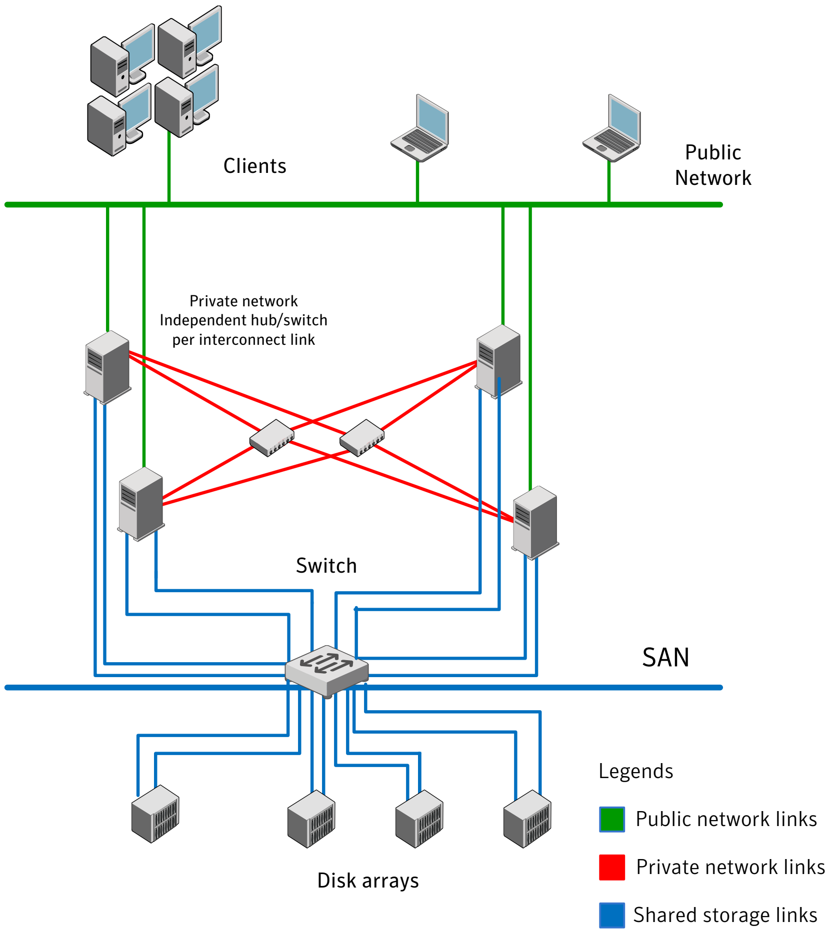
Depending on your business needs, you may choose from the following setup models:

- Basic setup
  See "Typical configuration of four-node SF Sybase CE cluster" on page 28.
- Secure setup
  See "Typical configuration of SF Sybase CE clusters in secure mode" on page 29.
- Central management setup
  See "Typical configuration of VOM-managed SF Sybase CE clusters" on page 30.
- Global cluster setup
  See "Typical configuration of SF Sybase CE global clusters for disaster recovery" on page 31.

Typical configuration of four-node SF Sybase CE cluster

Figure 1-1 depicts a high-level view of a basic SF Sybase CE configuration for a four-node cluster.

Figure 1-1 Sample four-node SF Sybase CE cluster



A basic topology has the following layout and characteristics:

- Multiple client applications that access nodes in the cluster over a public network.
- Nodes that are connected by at least two private network links (also called cluster interconnects) using 100BaseT or gigabit Ethernet controllers on each system.

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.
- Nodes that are connected with private network links using similar network devices and matching port numbers.
  For example, if you use bge1 on one end of a link, it is recommended that you use bge1 on the other end too.
- The quorum and Sybase datafile disks configured on the shared storage that is available to each node.
  Disks for Sybase ASE CE binary can be configured either on shared storage or on local storage.
  For shared storage:
  See "Preparing for shared mount point on CFS for Sybase ASE CE binary installation" on page 197.
  For local storage:
  See "Preparing for local mount point on VxFS for Sybase ASE CE binary installation " on page 196.
- VCS manages the resources that are required by Sybase ASE CE. The resources must run in parallel on each node.

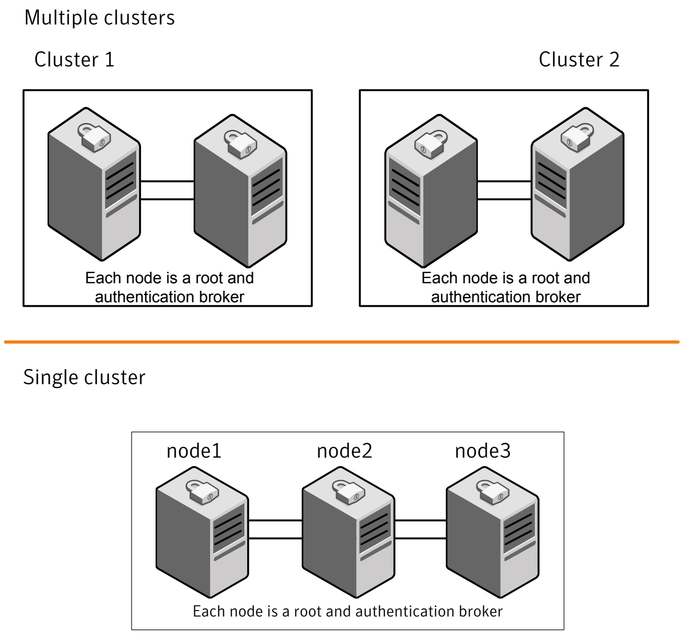
Typical configuration of SF Sybase CE clusters in secure mode

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

Figure 1-2 illustrates typical configuration of SF Sybase CE clusters in secure mode.

For information about how to configure secure clusters, see your product installation guide.

Figure 1-2 Typical configuration of SF Sybase CE clusters in secure mode



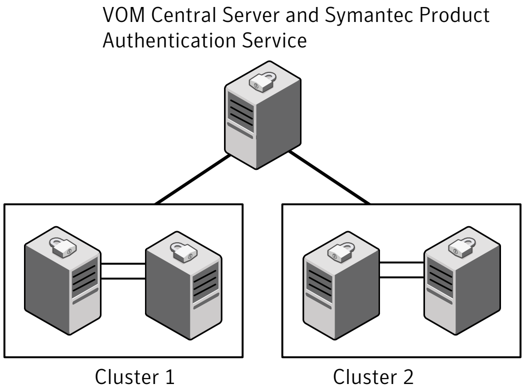
Typical configuration of VOM-managed SF Sybase CE clusters

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

See "About Veritas Operations Manager" on page 26.

Figure 1-3 illustrates a typical setup of SF Sybase CE clusters that are centrally managed using Veritas Operations Manager.

Figure 1-3 Typical configuration of VOM-managed clusters

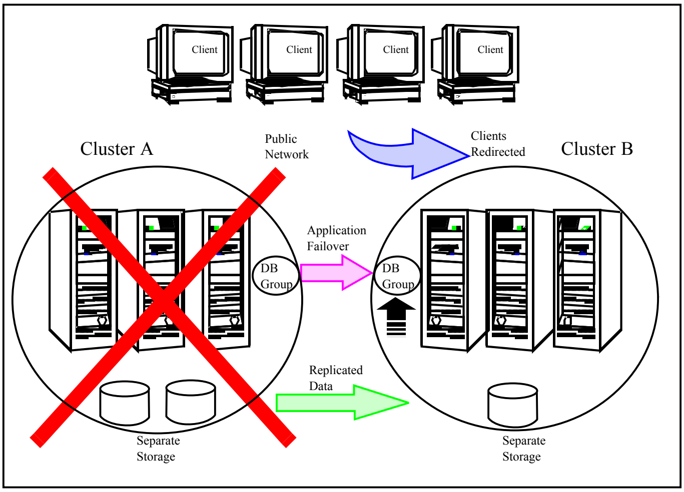


Typical configuration of SF Sybase CE global clusters for disaster recovery

SF Sybase CE leverages the global clustering feature of VCS to enable high availability and disaster recovery (HA/DR) for businesses that span wide geographical areas. Global clusters provide protection against outages caused by large-scale disasters such as major floods, hurricanes, and earthquakes. An entire cluster can be affected by such disasters. This type of clustering involves migrating applications between clusters over a considerable distance.

You can set up HA/DR using hardware-based or software-based replication technologies.

Figure 1-4 Global clusters



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

Note: You must have an SF Sybase CE HA/DR license to configure global clusters. If you use VVR for replication, you must also have a VVR license. You may configure a basic cluster initially and add the HA/DR and VVR licenses at a later time or you may add the licenses during the SF Sybase CE installation.

For information on supported replication technologies:

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

System requirements

This chapter includes the following topics:

Important preinstallation information

Before you install SF Sybase CE, make sure you have reviewed the following information:

- Hardware compatibility list for information about supported hardware:
  http://www.symantec.com/docs/TECH170013
- General information regarding the release, installation notes, known issues, and fixed issues:
  See *Veritas Storage Foundation for Sybase ASE CE Release Notes*.
- Sybase documentation for additional requirements pertaining to your version of Sybase.

Hardware requirements

Table 2-1 lists the hardware requirements for SF Sybase CE.

Table 2-1 Hardware requirements for basic clusters

Item	Description
SF Sybase CE systems	Two to four systems with two or more CPUs. For details on the additional requirements for Sybase, see the Sybase documentation.
DVD drive	A DVD drive on one of the nodes in the cluster.
Disk space	You can evaluate your systems for available disk space by running the product installation program. Navigate to the product directory on the product disc and run the following command: `# ./installsfsybasece -precheck node_name` You can also use the Veritas Web-based installation program to determine the available disk space. For details on the additional space that is required for Sybase, see the Sybase documentation.
RAM	Each SF Sybase CE system requires at least 2 GB.
Network	Two or more private links and one public link. Links must be 100BaseT or gigabit Ethernet directly linking each node to the other node to form a private network that handles direct inter-system communication. These links must be of the same type; you cannot mix 100BaseT and gigabit. Symantec recommends gigabit Ethernet using enterprise-class switches for the private links. You can also configure aggregated interfaces.
Fiber Channel or SCSI host bus adapters	At least one additional SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.

Supported operating systems

For information on supported operating systems, see the *Veritas Storage Foundation for Sybase ASE CE Release Notes*.

Coordinator disk requirements for I/O fencing

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

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

Supported database software

SF Sybase CE supports Sybase ASE CE 15.5 only at time of publication.

For the latest information on the supported Sybase ASE CE database versions, see the following Technical Support TechNote:

http://www.symantec.com/docs/DOC4848

See the Sybase ASE CE documentation for more information.

Supported SF Sybase CE configurations

The following Sybase configuration options are required in an SF Sybase CE environment:

- Set SF Sybase CE fencing to "sybase" mode.
- Configure Sybase private networks on LLT links
- Set Sybase cluster membership to "vcs" mode.
- Configure Sybase instances under VCS control.

Veritas File System requirements

Veritas File System requires that the values of the Solaris variables `lwp_default_stksize` and `svc_default_stksize` are at least 0x6000. When you install the Veritas File System package, `VRTSvxfs`, the VRTSvxfs packaging scripts check the values of these variables in the kernel. If the values are less than the required values, VRTSvxfs increases the values and modifies the `/etc/system` file with the required values. If the VRTSvxfs scripts increase the values, the installation proceeds as usual except that you must reboot and restart the installation program. A message displays if a reboot is required.

To avoid an unexpected need for a reboot, verify the values of the variables before installing Veritas File System. Use the following commands to check the values of the variables:

```
# echo "lwp_default_stksize/X" | mdb -k
lwp_default_stksize:
lwp_default_stksize:            6000

# echo "svc_default_stksize/X" | mdb -k
svc_default_stksize:
svc_default_stksize:            6000
```

If the values shown are less than 6000, you can expect a reboot after installation.

Note: The default value of the `svc_default_stksize` variable is 0 (zero), which indicates that the value is set to the value of the `lwp_default_stksize` variable. In this case, no reboot is required, unless the value of the `lwp_default_stksize` variable is too small.

To avoid a reboot after installation, you can modify the `/etc/system` file with the appropriate values. Reboot the system prior to installing the packages. Add the following lines to the `/etc/system` file:

```
set lwp_default_stksize=0x6000
set rpcmod:svc_default_stksize=0x6000
```

Supported replication technologies for global clusters

SF Sybase CE supports the software replication technology Veritas Volume Replicator (VVR) for global cluster configurations.

Discovering product versions and various requirement information

Symantec provides several methods to check the Veritas product you have installed, plus various requirement information.

You can check the existing product versions using the `installer` command with the `-version` option before or after you install. After you have installed the current version of the product, you can use the `showversion` script in the /opt/VRTS/install directory to find version information.

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

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

To run the version checker

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

```
# ./installer -version system1 system2
```

Chapter 3

Planning to install SF Sybase CE

This chapter includes the following topics:

Planning your network configuration

The following practices are recommended for a resilient network setup:

- Configure the private cluster interconnect over multiple dedicated gigabit Ethernet links. All single point of failures such as network interface cards (NIC), switches, and interconnects should be eliminated.
- The NICs used for the private cluster interconnect should have the same characteristics regarding speed, MTU, and full duplex on all nodes. Do not allow the NICs and switch ports to auto-negotiate speed.
- Configure non-routable IP addresses for private cluster interconnects.

Planning the public network configuration for Sybase ASE CE

Public interconnects are used by the clients to connect to Sybase ASE CE database. The public networks must be physically separated from the private networks.

See Sybase ASE CE documentation for more information on recommendations for public network configurations.

Planning the private network configuration for Sybase ASE CE

Private interconnect is an essential component of a shared disk cluster installation. It is a physical connection that allows inter-node communication. Symantec recommends that these interconnects and LLT links must be the same. You must have the IP addresses configured on these interconnects, persistent after reboot. You must use solutions specific to the operating System.

See Sybase ASE CE documentation for more information on recommendations for private network configurations.

Planning the storage

The following recommendations ensure better performance and availability of storage.

- Use multiple storage arrays, if possible, to ensure protection against array failures. The minimum recommended configuration is to have two HBAs for each host and two switches.
- Design the storage layout keeping in mind performance and high availability requirements. Use technologies such as striping and mirroring.
- Use appropriate stripe width and depth to optimize I/O performance.
- Use SCSI-3 persistent reservations (PR) compliant storage.
- Provide multiple access paths to disks with HBA/switch combinations to allow DMP to provide high availability against storage link failures and to provide load balancing.

Planning the storage for SF Sybase CE

Table 3-1 lists the type of storage required for SF Sybase CE.

Table 3-1 Type of storage required for SF Sybase CE

SF Sybase CE files	Type of storage
SF Sybase CE binaries	Local
SF Sybase CE fencing coordinator disks	Shared

Planning the storage for Sybase ASE CE

Review the storage options and guidelines for Sybase ASE CE:

- Storage options for Sybase ASE CE binaries
  See "Planning the storage for Sybase ASE CE binaries" on page 41.
- Storage options for Sybase ASE CE datafiles and quorum device
  See "Planning the storage for Sybase ASE CE datafiles and quorum device" on page 42.

Note: Symantec strongly recommends retaining the default setting (global) for the CVM diskgroup disk detach policy, for Sybase ASE CE binaries, datafiles, and quorum device. For other disk detach policy options, see the Veritas Storage Foundation Administrator's Guide.

Planning the storage for Sybase ASE CE binaries

The Sybase ASE CE binaries can be stored on a local or shared storage, depending on your high availability requirements.

Note: Symantec recommends that you install the Sybase ASE CE binaries on a shared storage on CFS.

Consider the following points while planning the installation:

- CFS installation provides a single Sybase ASE CE installation, regardless of the number of nodes. This scenario offers a reduction in the storage requirements and easy addition of nodes.
- Local installation provides improved protection against a single point of failure and also allows for applying the Sybase ASE CE patches in a rolling fashion.

Planning the storage for Sybase ASE CE datafiles and quorum device

Storage for Sybase ASE CE datafiles and quorum device has to be configured on shared storage on CFS.

Table 3-2 Type of storage required for Sybase ASE CE

Sybase ASE CE files	Type of storage
Sybase ASE CE binaries	Shared or local
Sybase ASE CE datafiles	Shared
Quorum device	Shared

Note: Refer to the Sybase ASE CE documentation for Sybase's recommendation on the required disk space for Sybase ASE CE binaries, Sybase ASE CE datafiles and quorum device.

Planning volume layout

The following recommendations ensure optimal layout of VxVM/CVM volumes:

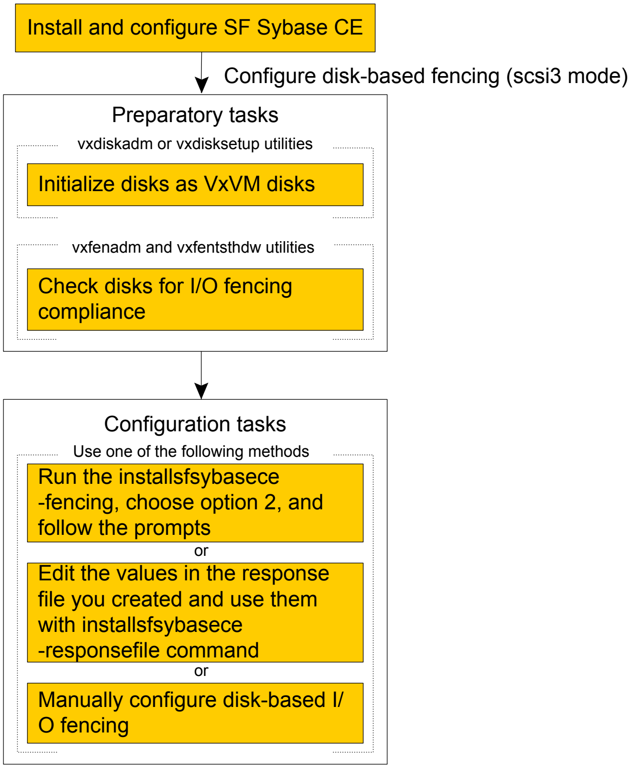
- Mirror the volumes across two or more storage arrays, if using VxVM mirrors. Keep the Fast Mirror Resync regionsize equal to the database block size to reduce the copy-on-write (COW) overhead. Reducing the regionsize increases the amount of Cache Object allocations leading to performance overheads.
- Distribute the I/O load uniformly on all Cache Objects when you create multiple Cache Objects.
- Implement zoning on SAN switch to control access to shared storage. Be aware that physical disks may be shared by multiple servers or applications and must therefore be protected from accidental access.
- Choose DMP I/O policy based on the storage network topology and the application I/O pattern.
- Exploit thin provisioning for better return on investment.

About planning to configure I/O fencing

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

Figure 3-1 illustrates a high-level flowchart to configure I/O fencing for the SF Sybase CE cluster.

Figure 3-1 Workflow to configure I/O fencing



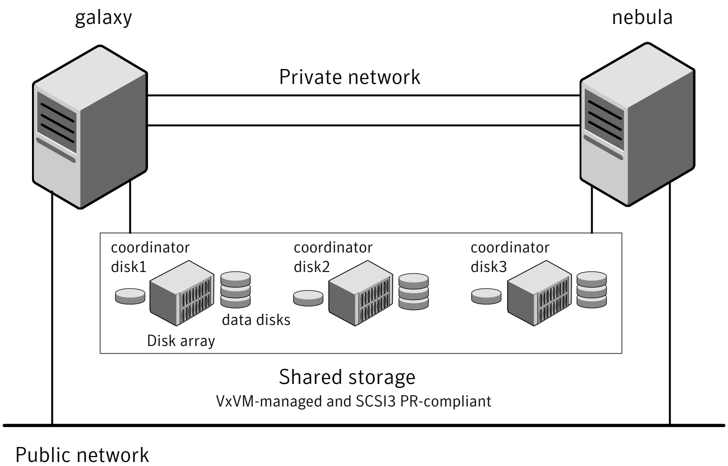
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installsfsybasece	See "Setting up disk-based I/O fencing using installsfsybasece" on page 109.
Using response files	See "Response file variables to configure disk-based I/O fencing" on page 243. See "Configuring I/O fencing using response files" on page 227.
Manually editing configuration files	See "Setting up disk-based I/O fencing manually" on page 117.

Typical SF Sybase CE cluster configuration with disk-based I/O fencing

Figure 3-2 displays a typical VCS configuration with two nodes and shared storage. The configuration uses three coordinator disks for I/O fencing.

Figure 3-2 Typical SF Sybase CE cluster configuration with disk-based I/O fencing



Planning for cluster management

Table 3-3 lists the various agents supported in SF Sybase CE installations for effective cluster management.

Table 3-3 List of agents

Agent	Description
VCS agent for Sybase	Sybase database management The VCS Sybase agent is recommended for managing Sybase databases. VCS controls the Sybase database in this configuration. In the basic monitoring mode, the agent detects an application failure if a configured Sybase server process is not running.
VCS agents for CVM	Volume management An SF Sybase CE installation automatically configures the CVMCluster resource and the CVMVxconfigd resource. You must configure the CVMVolDg agent for each shared disk group.

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

Agent	Description
VCS agents for CFS	File system management If the database uses cluster file systems, configure the CFSMount agent for each volume in the disk group.
VCS process agent for vxfend	vxfend process/daemon management

Planning for disaster recovery

SF Sybase CE supports global cluster configurations in multi-site clusters for disaster recovery. 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 Sybase CE supports the software replication technology Veritas Volume Replicator for data replication.

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

Planning a global cluster setup

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

Global clustering involves two steps:

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

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

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

Data replication considerations

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

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

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

Chapter 4

Licensing SF Sybase CE

This chapter includes the following topics:

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

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled or continue with keyless licensing by managing the server or cluster with a management server, such as Veritas Operations Manager (VOM). If you do not comply with the above terms, continuing to use the Symantec product is a violation of your end user license agreement, and results in warning messages.

For more information about keyless licensing, see the following URL: http://go.symantec.com/sfhakeyless

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 49.
  See the `vxkeyless(1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
  See "Installing Veritas product license keys" on page 51.
  See the `vxlicinst(1m)` manual page.

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

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

About SF Sybase CE licenses

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

Note: The SFSYBASECE_VFR and SFSYBASECE_VFR_GCO licenses are not supported.

Table 4-1 SF Sybase CE license levels (keyless licensing)

License	Description	Features enabled
SFSYBASECE	SF Sybase CE Enterprise Edition	The license enables the following features: ■ Veritas Volume Manager ■ Veritas File System ■ Veritas Cluster Server ■ Veritas Mapping Services
SFSYBASECE_VR	SF Sybase CE Enterprise Edition with VR (Veritas Replicator)	The license enables the following features: ■ Veritas Volume Manager Veritas Volume Replicator is enabled. ■ Veritas File System ■ Veritas Cluster Server ■ Veritas Mapping Services
SFSYBASECE_GCO	SF Sybase CE Enterprise Edition with GCO (Global Cluster Option)	The license enables the following features: ■ Veritas Volume Manager ■ Veritas File System ■ Veritas Cluster Server Global Cluster Option is enabled. ■ Veritas Mapping Services
SFSYBASECE_VR_GCO	SF Sybase CE Enterprise Edition with VR and GCO	The license enables the following features: ■ Veritas Volume Manager Veritas Volume Replicator is enabled. ■ Veritas File System ■ Veritas Cluster Server Global Cluster Option is enabled. ■ Veritas Mapping Services

Setting or changing the product level for keyless licensing

The keyless licensing method uses product levels to determine the Veritas products and functionality that are licensed. In order to use keyless licensing, you must set up a Management Server to manage your systems.

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

http://go.symantec.com/vom

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

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

To set or change the product level

1. Show your current working directory:

   ```
   # pwd
   ```

   Output resembles:

   ```
   /opt/VRTSvlic/bin
   ```

2. View the current setting for the product level.

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

3. View the possible settings for the product level.

   ```
   # ./vxkeyless displayall
   ```

4. Set the desired product level.

   ```
   # ./vxkeyless set prod_levels
   ```

   where *prod_levels* is a comma-separated list of keywords. The keywords are the product levels as shown by the output of step 3.

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

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

To clear the product license level

1 View the current setting for the product license level.

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

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

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

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

Installing Veritas product license keys

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin
```

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

Section 2

Installation and configuration of SF Sybase CE

Chapter 5

Preparing to install SF Sybase CE

This chapter includes the following topics:

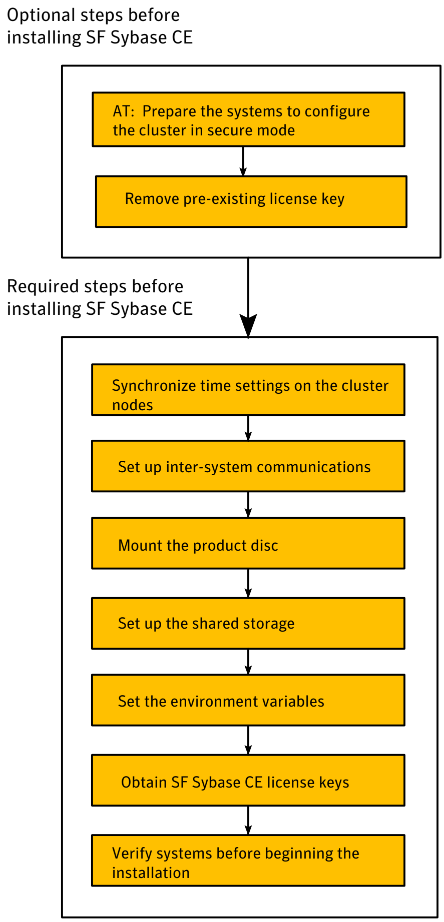
About preparing to install and configure SF Sybase CE

Before you install and configure SF Sybase CE, you need to perform some preinstallation tasks for the required and optional components of SF Sybase CE.

If you do not want to configure the optional components and features, proceed directly to the mandatory pre-installation tasks:

Figure 5-1 illustrates an overview of the mandatory and optional pre-installation steps for SF Sybase CE. The optional tasks are performed only for optional components or features that you plan to use.

Figure 5-1 SF Sybase CE pre-installation tasks



Synchronizing time settings on cluster nodes

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

The installer provides the option for automatic NTP synchronization.

Setting up inter-system communication

When you install SF Sybase CE using the installsfsybasece, make sure that communication between systems exists. By default the installer uses ssh. You must have root privileges for the system where you run installsfsybasece. This privilege facilitates to issue ssh or rsh commands on all systems in the cluster. If ssh is used to communicate between systems, it must be configured in a way such that it operates without requests for passwords or passphrases. Similarly, rsh must be configured in such a way to not prompt for passwords.

If system communication is not possible between systems using ssh or rsh, you have recourse.

Setting up ssh on cluster systems

Use the Secure Shell (ssh) to install SF Sybase CE on all systems in a cluster from a system outside of the cluster. Before you start the installation process, verify that ssh is configured correctly.

Use Secure Shell (ssh) to do the following:

- Log on to another system over a network
- Execute commands on a remote system
- Copy files from one system to another

The ssh shell provides strong authentication and secure communications over channels. It is intended to replace rlogin, rsh, and rcp.

Configuring ssh

The procedure to configure ssh uses OpenSSH example file names and commands.

Note: You can configure ssh in other ways. Regardless of how ssh is configured, complete the last step in the example to verify the configuration.

To configure ssh

1. Log in as root on the source system from which you want to install the Veritas product.
2. To generate a DSA key pair on the source system, type the following:

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

   System output similar to the following is displayed:

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

3 Press **Enter** to accept the default location of /.ssh/id_dsa. System output similar to the following is displayed:

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

4 Do not enter a passphrase. Press **Enter**.

Press **Enter** again.

5 Make sure the /.ssh directory is on all the target installation systems. If that directory is absent, create it on the target system and set the write permission to root only:

```
# mkdir /.ssh
# chmod go-w /
# chmod 700 /.ssh
# chmod go-rwx /.ssh
```

6 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems. To enable SFTP, the /etc/ssh/sshd_config file must contain the following two lines:

```
PermitRootLogin yes
Subsystem sftp /usr/lib/ssh/sftp-server
```

7 If the lines are not there, add them and restart SSH. To restart SSH on Solaris 10, type the following command:

```
# svcadm restart ssh
```

8 To copy the public DSA key, /.ssh/id_dsa.pub to each target system, type the following commands:

```
# sftp target_sys
```

If you run this step for the first time on a system, output similar to the following appears:

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

9 Enter **yes**. Output similar to the following is displayed:

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

10 Enter the root password.

11 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
```

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

```
sftp> quit
```

13 To begin the ssh session on the target system, type the following command:

```
# ssh target_sys
```

14 Enter the root password at the prompt:

```
password:
```

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

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

16 Delete the id_dsa.pub public key file. Before you delete this public key file, make sure to complete the following tasks:

- The file is copied to the target (host) system
- The file is added to the authorized keys file

To delete the id_dsa.pub public key file, type the following command:

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

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

```
# exit
```

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

19 Run the following commands on the source installation system. These commands bring the private key into the shell environment and makes the key globally available for the user root:

```
# exec /usr/bin/ssh-agent $SHELL
# ssh-add
Identity added: /.ssh/identity
```

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

20 To verify that you can connect to the target system, type the following command:

```
# ssh -l root target_sys uname -a
```

The command should execute on the remote system without any requests for a passphrase or password from the system.

Mounting the product disc

You must have superuser (root) privileges to load the SF Sybase CE software.

You can unmount the product disc after completing the SF Sybase CE 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 Sybase CE software into a drive that is connected to the system.

3 If Solaris volume management software is running on your system, the software disc automatically mounts as /cdrom/cdrom0.

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

```
# mount -F hsfs -o ro /dev/dsk/cXtXdXsX /dvd_mount
```

Where cXtXdXsX is the default address for the disc drive.

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:

  ```
  # format
  ```

- 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 `/tools/vxfentsthdw` on the product disc.

  ```
  # cd /cdrom/dvd/storage_foundation_for_sybase_ce/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:

For sh, ksh, or bash	`# MANPATH=/usr/share/man:/opt/VRTS/man` `# export MANPATH`

Set the PATH environment variable in the .profile file (or other appropriate shell setup file for your system) on each system to include installation and other commands.

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

For sh, ksh, or bash

Optimizing LLT media speed settings on private NICs

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

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

Guidelines for setting the media speed of the LLT interconnects

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

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

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

Verifying the systems before installation

Use the following to verify your systems before installation:

- Run the Veritas Installation Assessment Service (VIAS) utility.
  For information on downloading and running VIAS:
  https://vias.symantec.com/
- Run the installsfsybasece with the "-precheck" option by navigating to the directory that contains the installsfsybasece.

The program proceeds in a non-interactive mode, examining the systems for licenses, rpms, disk space, and system-to-system communications. The program displays the results of the check and saves 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 6

Installing SF Sybase CE

This chapter includes the following topics:

About installing SF Sybase CE

You can use one of the following tools to install and configure SF Sybase CE:

`installer` program	The `installer` program is the common product installation program that offers a high-level approach to installing or configuring multiple Veritas products.
`installsfsybasece` program	The `installsfsybasece` program is the product-specific installation program that offers a direct approach to specifically installing and configuring SF Sybase CE. You can choose one of the following ways: ■ Install the packages and proceed to configure SF Sybase CE. ■ Install the packages and leave the cluster configuration steps for later using the '-configure' option.

You can install SF Sybase CE on clusters of up to 4 nodes.

The following packages are installed on each cluster node:

- Veritas Cluster Server (VCS)
- Veritas Volume Manager (VxVM)
- Veritas File System (VxFS)

You can configure the following components for SF Sybase CE:

- Veritas Cluster Server (VCS)
- CVM (Veritas Volume Manager enabled for clusters)
- CFS (Veritas File System enabled for clusters)
- I/O Fencing
- Sybase instances under VCS control

About installation and configuration methods

You can use one of the following methods to install and configure SF Sybase CE.

SF Sybase CE does not support installation and configuration using the Web installer.

Table 6-1 Installation and configuration methods

Method	Description
Interactive installation and configuration using the script-based installer **Note:** If you obtained SF Sybase CE from an electronic download site, you must use the `installsfsybasece` script instead of the `installer` script.	You can use one of the following script-based installers: ■ Common product installer script: `installer` The common product installer script provides a menu that simplifies the selection of installation and configuration options. ■ The product-specific installation script provides command-line interface options. Installing and configuring with the `installsfsybasece` script is identical to specifying SF Sybase CE from the `installer` script. Use this method to install or configure only SF Sybase CE.

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

Method	Description
Silent installation using the response file	The response file automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. You can use the script-based installers with the response file to install silently on one or more systems.
JumpStart	You can use the Veritas product installer of the product-specific installation script to generate a JumpStart script file. Use the generated script to install Veritas packages from your JumpStart server.

Installing SF Sybase CE using the Veritas script-based installation program

During the installation, the installer performs the following tasks:

- Verifies system readiness for installation by checking system communication, network speed, installed packages, operating system patches, swap space, and available volume space.

  Note: If the installer reports that any of the patches are not available, install the patches on the system before proceeding with the SF Sybase CE installation.

- Installs the SF Sybase CE 6.0 packages.

The following sample procedure installs SF Sybase CE on two systems—galaxy and nebula.

To install SF Sybase CE

1. Log in as the superuser on one of the systems.
2. Start the installation program:

SF Sybase CE installer	Run the program: `# ./installsfsybasece galaxy nebula`

Common product installer	Navigate to the directory that contains the installation program. Run the program: `# ./installer galaxy nebula` From the opening Selection Menu, choose: "**I**" for "Install a Product."

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

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

```
Would you like the installer to setup ssh or rsh communication
automatically between the systems?
Superuser passwords for the systems will be asked. [y,n,q] (y)
Enter the superuser password for system vcslx613:

     1)  Setup ssh between the systems
     2)  Setup rsh between the systems
     b)  Back to previous menu
Select the communication method [1-2,b,q,?] (1)
```

4 If you had quit the installer in the process of an active installation, the installer discovers that installer process and provides the option of resuming the installation or starting a new installation. Provide a suitable response.

```
The installer has discovered an existing installer process.
The process exited while performing configure of SF Sybase CE
on galaxy.
Do you want to resume this process? [y,n,q,?] (y) n
```

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

6 Select the type of installation—Minimal, Recommended, All. Each option displays the disk space that is required for installation.

Symantec recommends you to choose the option **Install all packages**.

```
1)  Install minimal required packages
2)  Install recommended packages
3)  Install all packages
4)  Display packages to be installed for each option
Select the packages to be installed on all systems?
[1-4,q,?] (2) 3
```

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

The installer installs the SF Sybase CE packages and patches.

7 Select the appropriate license option.

```
1) Enter a valid license key
2) Enable keyless licensing and complete
system licensing later
How would you like to license the systems? [1-2,q]
```

- Enter **1** if you have a valid license key. When prompted, enter the license key.

  ```
  Enter a SF Sybase CE license key:
  xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-x
  ```

  If you plan to enable additional capabilities, enter the corresponding license keys when you are prompted for additional licenses.

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

- Enter **2** to enable keyless licensing.

  Note: The keyless license option enables you to install SF Sybase CE without entering a key. However, you must still acquire a valid license to install and use SF Sybase CE. Keyless licensing requires that you manage the systems with a Management Server.

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

  ```
  Would you like to enable the
  Veritas Volume Replicator? [y,n,q] (n)
  Would you like to enable the
  Global Cluster Option? [y,n,q] (n)
  ```

  The installer registers the license.

8 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.

9 Enter **y** to configure SF Sybase CE:

```
Would you like to configure SF Sybase CE on
galaxy nebula [y,n,q] (n) y
```

Note: If you had quit the installer before registering the sfsybasece license key, make sure the license key is registered on the system before starting the SF Sybase CE configuration. To register the license key, use the `installer -license` command.

---

10 Enter **y** if you want to send the installation information to Symantec.

```
Would you like to send the information about this installation
to Symantec to help improve installation
in the future? [y,n,q,?] (y) y
```

11 Enter **y** if you want to view the summary file.

```
Would you like to view the summary file? [y,n,q] (n) y
```

Installing SF Sybase CE using Solaris JumpStart

This section provides instructions for installing SF Sybase CE using Solaris JumpStart. The instructions assume a working knowledge of Solaris JumpStart. See the operating system documentation for detailed information on using Solaris JumpStart.

Note: Only new installations of SF Sybase CE are supported using Solaris JumpStart.

Before you perform the instructions in this section, complete the preparatory tasks for installing SF Sybase CE.

Task overview for SF Sybase CE installation using JumpStart

This section provides a summary of the tasks for installing SF Sybase CE using Solaris JumpStart.

1. Set up a central Solaris JumpStart server on the network.

   For instructions, see the Solaris JumpStart documentation.

2. Add the systems, on which you want to install SF Sybase CE, as clients to the JumpStart server.

For instructions, see the Solaris JumpStart documentation.

3. Prepare the installation resources.

   See "Preparing the JumpStart installation resources" on page 69.

4. Install and configure SF Sybase CE.

   See "Installing and configuring SF Sybase CE using JumpStart" on page 76.

Preparing the JumpStart installation resources

This section contains instructions for creating the installation resources.

Table 6-2 lists the installation resources you must prepare before you install SF Sybase CE using Solaris JumpStart.

Table 6-2 Installation resources

Files	Description
Finish scripts	Generate the following finish scripts: ■ `jumpstart_sfsybasece.fin`(Required) ■ `encap_bootdisk_vm.fin` (Optional)
Response files	You need to create empty response files for the following packages: `VRTSaslapm, VRTSvxvm`
admin file	You need to create an admin file if you plan to perform a non-interactive installation.
rules file	You need to modify the rules file as appropriate for your systems.

Table 6-3 lists the sample directories used in the procedure.

Table 6-3 Sample directories used in the procedure

Files	Sample directories
SF Sybase CE product disc content	`/export/config`
Installation and finish scripts	`/export/config`
Response files for installation	`/export/config/dvd1/pkgs`

Table 6-3 Sample directories used in the procedure *(continued)*

Files	Sample directories
Admin file for non-interactive installations	/export/config/dvd1/pkgs

Note: The directories must be mounted as NFS-accessible directories to the JumpStart server.

To prepare the installation resources

1. Copy the packages from the product disc to the Solaris JumpStart server under a shared directory. The packages are in .pkg format.

   - First, create directories for installation.

     ```
     # mkdir /export/config
     ```

   - Insert the product disc into a drive that is connected to the system. The Solaris volume management software automatically mounts the disc as /dvdrom/dvd1. Type the command:

     ```
     # cd /dvd_mount/
     ```

   - Copy the contents of the product disc to the server.

     ```
     # cp -r * /export/config/dvd1
     ```

2. Create response files for the SF Sybase CE packages.

   See "Creating JumpStart response files" on page 71.

3 For non-interactive installations, create the file `admin` in the current directory on your JumpStart server (`/export/config/dvd1/pkgs`), and modify the file as follows:

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

Note: Specify the `-a adminfile` option with the `pkgadd` command in the finish script you generate in the next step.

---

4 Generate the installation and finish scripts.

See "Generating the JumpStart installation and finish scripts" on page 72.

5 Modify the rules file as required.

For example:

```
any - - profile_sfsybasece jumpstart_sfsybasece.fin
```

If you generated the root disk encapsulation finish file:

```
any - - profile_sfsybasece encap_bootdisk_vm.fin
```

For detailed instructions, see the Solaris JumpStart documentation.

Creating JumpStart response files

Response files contain the installation profile for packages. Some packages need empty response files, while some packages require specific settings.

Note: Make sure that you edit the `finish` script to use the `-r` option with the `pkgadd` command to install the packages using the corresponding response files:

```
# pkgadd -r responsefile_name package_name
```

For example, to install the `VRTSvxvm` package using its response file:

```
# pkgadd -r VRTSvxvm.response -d VRTSvxvm.pkg
```

The sample procedure places the response files in the directory `/export/config/dvd1/pkgs`.

To create response files

1. Change to the directory `/export/config/dvd1/pkgs`.

   ```
   # cd /export/config/dvd1/pkgs
   ```

2. For Solaris SPARC systems: Create a response file for each of the following packages: `VRTSaslapm, VRTSvxvm`

   ```
   # pkgask -r package_name.response -d package_name.pkg
   ```

   For example:

   ```
   # pkgask -r VRTSvxvm.response -d VRTSvxvm.pkg
   ```

Generating the JumpStart installation and finish scripts

Run the SF Sybase CE installer to generate the installation and finish scripts.

The installer generates the following scripts:

`jumpstart_sfsybasece.fin`	Finish script for installing SF Sybase CE
`encap_bootdisk_vm.fin`	Encapsulation finish script for root disk encapsulation

To generate the JumpStart installation and finish scripts

1. Run the SF Sybase CE installer to generate the installation and finish scripts:

   ```
   # cd /dvd_mount/storage_foundation_for_sybase_ce
   # ./installsfsybasece -jumpstart dir_path
   ```

   Where *dir_path* is the full path to the directory where the scripts are placed.

   For example:

   ```
   # ./installsfsybasece -jumpstart /export/config/
   ```

2. If you want to encapsulate the root disk automatically, generate a separate finish script for root disk encapsulation.

   Enter **y** to generate a sample finish script for root disk encapsulation.

   ```
   Would you like to generate the finish script to encapsulate
   the boot disk? [y,n,q,?] (y)
   ```

   Enter the disk group name, private region length, and the disk media name of the root disk to be encapsulated.

   ```
   Specify the disk group name of the root disk to be encapsulated: rootdg
   Specify the private region length of the root disk
   to be encapsulated: (65536)
   Specify the disk media name of the root disk to
   be encapsulated: (rootdg_01)
   ```

3. View the list of generated scripts.

   ```
   # ls /export/config
   ```

   The following scripts will be listed:

   ```
   encap_bootdisk_vm.fin
   jumpstart_sfsybasece.fin
   ```

   The root disk encapsulation script will be listed only if you chose to encapsulate the root disk automatically.

4. Modify the finish files, as required.

   You will need to update the following information in the finish file:

   - Installation order for packages
     The finish script must contain the correct order of the SF Sybase CE packages and the operating system packages.

See “Installation order of packages for JumpStart” on page 74.
Use the list of packages that is generated to replace the package list in the finish scripts.

- BUILDSRC value
  The path indicated in the BUILDSRC variable must contain the product disc content.
  The value must be in the following format:
  hostname_or_ip:/path_to_pkgs_patches_scripts
  For example:

  ```
  192.168.12.1:/export/config
  ```

- ENCAPSRC value
  The path indicated in the ENCAPSRC variable must contain the root encapsulation finish script.
  The value must be in the following format:
  hostname_or_ip:/path_to_encap_script
  For example:

  ```
  192.168.12.1:/export/config
  ```

- License information for root disk encapsulation
  If you want the root disk to be encapsulated, you must provide the Veritas Volume Manager license information in the root disk encapsulation finish file.

- Language pack information
  If you want to install SF Sybase CE in a language other than English, add the language pack information to the basic finish file.
  See “Adding language pack information to the JumpStart finish file” on page 75.

For a basic sample finish file:

See “Sample JumpStart finish file (basic installation) ” on page 76.

For a sample root disk encapsulation finish file:

See “Sample JumpStart finish file (for root encapsulation) ” on page 79.

Installation order of packages for JumpStart

The correct installation order of packages for JumpStart is as follows:

SF Sybase CE packages	The correct order of SF Sybase CE packages can be viewed by running the `installsfsybasece` program with one of the following options:
	■ -minpkgs
	Install SF Sybase CE with basic functionality.
	■ -recpkgs
	Installs the full feature set without optional packages.
	■ -allpkgs
	Installs all available packages.
	Symantec recommends installation of all the packages.
	For example, to view the installation order for installing SF Sybase CE 6.0:
	`# cd /dvd_mount/storage_foundation_for_sybase_ce`
	`# ./installsfsybasece -allpkgs`

Note: No additional packages are required for Solaris 10 Update 7 and later update versions.

Adding language pack information to the JumpStart finish file

Perform the steps in the following procedure to install SF Sybase CE in a language other than English. The packages need not be manually ordered as there are no package inter-dependencies.

To add language pack information to the finish file

1 Copy the packages from the language pack installation disc.

```
# cp -r pkgs/* /export/config/dvd1/pkgs
```

2 Add the following lines in the finish script.

```
for PKG in VRTSjacse VRTSjadbe VRTSmulic \
VRTSatJA VRTSjacs VRTSjafs \
VRTSatZH VRTSjacsu VRTSjaodm VRTSzhvm \
VRTSjacav VRTSjadba VRTSjavm
do
<...language pack instructions>
done
```

For sample finish file:

See “Sample JumpStart finish file (basic installation) ” on page 76.

Installing and configuring SF Sybase CE using JumpStart

Perform the steps in the following procedure to install SF Sybase CE using Solaris JumpStart.

To install and configure SF Sybase CE using JumpStart on Solaris SPARC systems

1. On each client node, run the following command to install the SF Sybase CE packages:

   ```
   ok> boot net - install
   ```

   The system is restarted after the packages are installed. If you choose to encapsulate the root disk on your systems, the systems start with an encapsulated root disk.

2. Configure SF Sybase CE.

   Note: Before you start the configuration, complete the preparatory tasks. Make sure the sfsybasece license key is registered on the system. To register the license key, use the `installer -license` command.

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

   For instructions on configuring SF Sybase CE, see the following chapters in this document:

   Configuring SF Sybase CE

   Configuring SF Sybase CE clusters for data integrity

3. Complete the post-installation tasks.

   For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Sample JumpStart finish file (basic installation)

The following extract is a sample finish file generated using the `installsfrac` program for SF Sybase CE installations on Solaris 10.

The text in bold indicates modifications required for installing SF Sybase CE.

```
#!/bin/sh

# $Copyright: Copyright (c) 2011 Symantec Corporation.
# All rights reserved.
#
# THIS SOFTWARE CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF
```

```
# SYMANTEC CORPORATION.  USE, DISCLOSURE OR REPRODUCTION IS PROHIBITED
# WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SYMANTEC CORPORATION.
#
# The Licensed Software and Documentation are deemed to be commercial
# computer software as defined in FAR 12.212 and subject to restricted
# rights as defined in FAR Section 52.227-19 "Commercial Computer
# Software - Restricted Rights" and DFARS 227.7202, "Rights in
# Commercial Computer Software or Commercial Computer Software
# Documentation", as applicable, and any successor regulations. Any use,
# modification, reproduction release, performance, display or disclosure
# of the Licensed Software and Documentation by the U.S. Government
# shall be solely in accordance with the terms of this Agreement.  $0

echo "==== Executing finish script: $me ===="

PATH=$PATH:/sbin:/usr/sbin
export PATH

#
# Notice:
# * Modify the BUILDSRC and ENCAPSRC below according to your
# * real environment
# * The location specified with BUILDSRC and ENCAPSRC should be NFS
#   accessible to the Jumpstart Server
# * It's requied to set ENCAPSRC only if you are using jumpstart for
#   automatic boot disk encapsulation
# * Copy the whole directories of pkgs from installation media
#   to the BUILDSRC
# * Create the admin and response file for pkgadd according
#   to 'jumpstart_readme.txt' in the DVD
#

BUILDSRC="<hostname_or_ip>:/path/to/pkgs_patches"
#ENCAPSRC="<hostname_or_ip>:/path/to/encap_script"

#
# Notice:
# * You do not have to change the following scripts
#

ROOT=/a
BUILDDIR="${ROOT}/build"
PKGDIR="${BUILDDIR}/pkgs"
```

```
PATCHDIR="${BUILDDIR}/patches"
ENCAPDIR="${ROOT}/encap_script"

mkdir -p ${BUILDDIR}
mount -F nfs -o vers=3 ${BUILDSRC} ${BUILDDIR}

for PKG in VRTSvlic VRTSperl VRTSsfcpi VRTSspt VRTSvxvm VRTSaslapm VRTSob
VRTSsfmh VRTSvxfs VRTSfsadv VRTSfssdk VRTSllt VRTSgab VRTSvxfen VRTSamf
VRTSvcs VRTSvcsag VRTSvcsea VRTSglm VRTScavf
do
    if [ -n "$PKG" ]
    then
        RESP="${PKGDIR}/${PKG}.response"
        echo "Installing package  -- $PKG"
        if [ -f ${RESP} ]
        then
            pkgadd -n -a ${PKGDIR}/admin  -d ${PKGDIR}/${PKG}.pkg -r
${RESP} -R ${ROOT} ${PKG}
        else
            pkgadd -v -a ${PKGDIR}/admin  -d ${PKGDIR}/${PKG}.pkg -R
${ROOT} ${PKG}
        fi
    fi
done

for PATCH in ""
do
    if [ -n "$PATCH" ]
    then
        patchadd -R ${ROOT} -M ${PATCHDIR} ${PATCH}
    fi
done

# Required for language package installation
for PKG in VRTSjacse VRTSjadbe VRTSmulic \
VRTSatJA VRTSjacs VRTSjafs \
VRTSatZH VRTSjacsu VRTSjaodm VRTSzhvm \
VRTSjacav VRTSjadba VRTSjavm
do
  echo "Installing package  -- $PKG"
  pkgadd -v -a ${PKGDIR}/admin -d ${PKGDIR}/${PKG}.pkg -R ${ROOT} ${PKG}
done
```

```
${ROOT}/opt/VRTS/install/bin/UXRT60/add_install_scripts

touch ${ROOT}/noautoshutdown

umount ${BUILDDIR}


echo "==== Completed finish script $me ===="

exit 0
```

Sample JumpStart finish file (for root encapsulation)

Root encapsulation requires the following finish files:

- encap_bootdisk_vm.fin
- jumpstart_sfsybasece.fin

The following sample finish files are generated using the `installsfsybasece` program for SF Sybase CE installations on Solaris 10 for encapsulating the root disk.

The text in bold indicates the license key required for installing SF Sybase CE.

Note: Do not modify the other statements in the script.

A sample `encap_bootdisk_vm.fin` file is as follows:

```
#!/bin/sh

# Copyright: Copyright (c) 2011 Symantec Corporation.
# All rights reserved.
#
# THIS SOFTWARE CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF
# SYMANTEC CORPORATION. USE, DISCLOSURE OR REPRODUCTION IS PROHIBITED
# WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SYMANTEC CORPORATION.
#
# The Licensed Software and Documentation are deemed to be commercial
# computer software as defined in FAR 12.212 and subject to restricted
# rights as defined in FAR Section 52.227-19 "Commercial Computer
# Software - Restricted Rights" and DFARS 227.7202, "Rights in
# Commercial Computer Software or Commercial Computer Software
# Documentation", as applicable, and any successor regulations. Any use,
# modification, reproduction release, performance, display or disclosure
```

```
# of the Licensed Software and Documentation by the U.S. Government
# shall be solely in accordance with the terms of this Agreement.

######################################################################
#
# The following init script encapsulates the root disk.
# The script was copied to the /etc/rc2.d directory remotely
# as part of the vxvm jumpstart installation procedure.
#
######################################################################

: ${VOLROOT_DIR:=$__VXVM_ROOT_DIR}
. ${VOL_SCRIPTS_LIB:-/usr/lib/vxvm/lib}/vxcommon

CMD=`basename $0`

quit()
{
    code=$1
    if [ -n "$DEBUG" ]; then
            set -x
    fi
    rm -f /etc/init.d/vxvm-jumpstart /etc/rc2.d/S01vxvm-jumpstart
    if [ "$code" -eq 100 ]; then
            shutdown -g0 -y -i6
            code=0
    fi
    exit $code
}

trap 'quit 2' INT HUP QUIT TERM

if [ -n "$DEBUG" ]; then
        set -x
fi

# if system is already encapsulated, then exit init script
df / | grep rootvol > /dev/null
if [ $? -eq 0 ]; then
        echo "INFO: $CMD: system is already encapsulated."
        quit 0
fi
```

```
# Do minimal vxvm installation
if [ -d /dev/vx/dmp ]
then
        /sbin/mount -F tmpfs dmpfs /dev/vx/dmp
fi
if [ -d /dev/vx/rdmp ]
then
        /sbin/mount -F tmpfs dmpfs /dev/vx/rdmp
fi

# set the license for vxconfigd to work
mount /opt 2> /dev/null
/opt/VRTS/bin/vxlicinst
-k XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX

vxconfigd -k -m disable > /dev/null 2>&1
vxdctl init > /dev/null 2>&1
vxdctl enable

voldmode=`vxdctl mode 2>/dev/null`
if [ "X$voldmode" != "Xmode: enabled" ]
then
        echo "ERROR: $CMD: vold could not be enabled."
        quit 1
fi

rm -f $mkdbfile

# Determine root disk of system
set_rootdisk
if [ -z "$rootdisk" ]; then
        echo "ERROR: $CMD: Could not locate root disk : $rootdisk."
        quit 2
fi

# Encapsulate root disk
/usr/lib/vxvm/bin/vxencap -c -g rootdg -f sliced -s 65536
rootdg_01=$rootdisk

# Exit if encapsulation of root disk failed
if [ ! -s /etc/vx/reconfig.d/disk.d/$rootdisk/newpart ]
then
        echo "ERROR: $CMD: Encapsulation of root disk failed."
```

```
        quit 3
fi

# encapsulation was successful.  Shutdown the system to complete
encapsulation.
quit 100
```

A sample `jumpstart_sfsybasece.fin` file is as follows:

```
#!/bin/sh

# $Copyright: Copyright (c) 2011 Symantec Corporation.
# All rights reserved.
#
# THIS SOFTWARE CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF
# SYMANTEC CORPORATION.  USE, DISCLOSURE OR REPRODUCTION IS PROHIBITED
# WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SYMANTEC CORPORATION.
#
# The Licensed Software and Documentation are deemed to be commercial
# computer software as defined in FAR 12.212 and subject to restricted
# rights as defined in FAR Section 52.227-19 "Commercial Computer
# Software - Restricted Rights" and DFARS 227.7202, "Rights in
# Commercial Computer Software or Commercial Computer Software
# Documentation", as applicable, and any successor regulations. Any use,
# modification, reproduction release, performance, display or disclosure
# of the Licensed Software and Documentation by the U.S. Government
# shall be solely in accordance with the terms of this Agreement.  $0

echo "==== Executing finish script: $me ===="

PATH=$PATH:/sbin:/usr/sbin
export PATH

#
# Notice:
# * Modify the BUILDSRC and ENCAPSRC below according to your
# * real environment
# * The location specified with BUILDSRC and ENCAPSRC should be NFS
#   accessible to the Jumpstart Server
# * It's requied to set ENCAPSRC only if you are using jumpstart for
#   automatic boot disk encapsulation
# * Copy the whole directories of pkgs from installation media
#   to the BUILDSRC
# * Create the admin and response file for pkgadd according
```

```
#   to 'jumpstart_readme.txt' in the DVD
#

BUILDSRC="<hostname_or_ip>:/path/to/pkgs_patches"
ENCAPSRC="<hostname_or_ip>:/path/to/encap_script"
#
# Notice:
# * You do not have to change the following scripts
#

ROOT=/a
BUILDDIR="${ROOT}/build"
PKGDIR="${BUILDDIR}/pkgs"
PATCHDIR="${BUILDDIR}/patches"
ENCAPDIR="${ROOT}/encap_script"

mkdir -p ${BUILDDIR}
mount -F nfs -o vers=3 ${BUILDSRC} ${BUILDDIR}

for PKG in VRTSvlic VRTSperl VRTSsfcpi VRTSspt VRTSvxvm VRTSaslapm
VRTSob VRTSsfmh VRTSvxfs VRTSfsadv VRTSfssdk VRTSllt VRTSgab
VRTSvxfen VRTSamf VRTSvcs VRTSvcsag VRTSvcsea VRTSglm VRTScavf
do
    if [ -n "$PKG" ]
    then
        RESP="${PKGDIR}/${PKG}.response"
        echo "Installing package  -- $PKG"
        if [ -f ${RESP} ]
        then
            pkgadd -n -a ${PKGDIR}/admin  -d ${PKGDIR}/${PKG}.pkg -r
${RESP} -R ${ROOT} ${PKG}
        else
            pkgadd -v -a ${PKGDIR}/admin  -d ${PKGDIR}/${PKG}.pkg -R
${ROOT} ${PKG}
        fi
    fi
done

for PATCH in ""
do
    if [ -n "$PATCH" ]
    then
        patchadd -R ${ROOT} -M ${PATCHDIR} ${PATCH}
```

```
    fi
done

${ROOT}/opt/VRTS/install/bin/UXRT60/add_install_scripts

touch ${ROOT}/noautoshutdown

umount ${BUILDDIR}


mkdir -p ${ENCAPDIR}
mount -F nfs -o vers=3 ${ENCAPSRC} ${ENCAPDIR}

cp ${ENCAPDIR}/encap_bootdisk_vm.fin ${ROOT}/etc/init.d/vxvm-jumpstart
ln ${ROOT}/etc/init.d/vxvm-jumpstart ${ROOT}/etc/rc2.d/S01vxvm-jumpstart
chmod 755 ${ROOT}/etc/init.d/vxvm-jumpstart


echo "==== Completed finish script $me ===="

exit 0
```

Using a Flash archive to install SF Sybase CE and the operating system

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

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

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

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

Flash archive creation overview

1. Ensure that you have installed Solaris 10 on the master system.
2. Use JumpStart to create a clone of a system.
3. Reboot the cloned system.
4. Install the Veritas products on the master system.

   Perform one of the installation procedures from this guide.
5. If you have configured the product on the master system, create the vrts_deployment.sh file and the vrts_deployment.cf file and copy them to the master system.

   See “Creating the Veritas post-deployment scripts” on page 85.
6. Use the `flarcreate` command to create the Flash archive on the master system.
7. Copy the archive back to the JumpStart server.
8. Use JumpStart to install the Flash archive to the selected systems.
9. Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:

   ```
   # /opt/VRTS/install/installsfsybasece -configure
   ```
10. Perform post-installation and configuration tasks.

    See the chapter "Performing post-installation and configuration tasks" in this document.

Creating the Veritas post-deployment scripts

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

To create the post-deployment scripts

1 Mount the product disc.

2 From the prompt, run the `-flash_archive` option for the installer. Specify a directory where you want to create the files.

```
# ./installer -flash_archive /tmp
```

3 Copy the vrts_postedeployment.sh file and the vrts_postedeployment.cf file to the golden system.

4 On the golden system perform the following:

- Put the vrts_postdeployment.sh file in the /etc/flash/postdeployment directory.
- Put the vrts_postdeployment.cf file in the /etc/vx directory.

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

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

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

Installing SF Sybase CE on an alternate root

Installing SF Sybase CE on an alternate root enables you to boot from the second disk instead of the default disk. Installing on an alternate root also enables you to upgrade the OS on a Solaris system without affecting the existing configuration or requiring much downtime. Using an alternate root is required when using Live Upgrade to upgrade to SF Sybase CE 6.0.

Perform the steps in the following procedure on the active root disk of each node.

To install SF Sybase CE 6.0 on the alternate root disk of your system

1 Verify that the Solaris operating system is installed on the alternate root disk of the system.

For example, `/dev/dsk/cXtXdXs2`, where cXtXdXs2 is the alternate root disk.

2 Mount your alternate root disk.

```
# mkdir /altroot
# mount /dev/dsk/cXtXdXs0 /altroot
```

The mount point must have the same name on all systems.

3 Start the installer with the `-rootpath` option.

```
# cd /dvd_mount/storage_foundation_for_sybase_ase_ce
# ./installsfsybasece -rootpath /altroot galaxy nebula
```

4 Stop the applications that are running on the current root disk using native application commands.

5 Restart the systems with the alternate root `/altroot`.

- Display the current boot disk device and device aliases.

```
# eeprom
boot-device=vx-rootdg vx-int_disk
use-nvramrc?=true
nvramrc=devalias vx-int_disk /pci@1c,600000/scsi@2/disk@0,0:a
devalias vx-rootdg01 /pci@1c,600000/scsi@2/disk@1,0:a
```

- Set the device from which to boot using the eeprom command. This example shows booting from the alternate root disk.

```
# eeprom boot-device=/pci@780/pci@0/pci@9/scsi@0/disk@1
```

- Reboot the system.

```
# shutdown -g0 -i6 -y
```

6 Configure SF Sybase CE.

```
# ./installsfsybasece -configure galaxy nebula
```

7 Install the language packages if you would like to run SF Sybase CE in a language other than English. Follow the procedure for the appropriate language packages.

See “Installing language packages” on page 127.

8 Complete the post-installation tasks.

For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Chapter 7

Configuring SF Sybase CE

This chapter includes the following topics:

About configuring SF Sybase CE

You need to configure SF Sybase CE when:

- You have completed installation of SF Sybase CE on your systems.
- You want to reconfigure an existing SF Sybase CE cluster.

Note: Before you reconfigure a cluster, make sure that you stop any running applications that use VxFS/CFS. Then, unmount the VxFS/CFS mounts.

SF Sybase CE configuration involves the following high-level tasks:

- Starting the product installer (if you quit the installer after installation or want to reconfigure the cluster)
- Configuring the SF Sybase CE components—VCS, CVM, and CFS
- Configuring the SF Sybase CE clusters for data integrity

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

- Verifies the cluster information.
- Stops SF Sybase CE processes.
- Creates SF Sybase CE configuration files.
- Starts SF Sybase CE processes.

- Creates a new directory with a log file that contains any system commands executed, and their output, a response file that can be used with the -responsefile option of the installer, and a summary file that contains the output of the install scripts. The location of the files is indicated by the installer.

Configuring the SF Sybase CE components using the script-based installer

After installation, log in to the product installer to configure SF Sybase CE components. No configuration changes are made to the systems until all configuration questions are completed and confirmed.

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

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

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

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

Note: If you want to reconfigure SF Sybase CE, before you start the installer you must stop all the resources that are under VCS control using the `hastop` command or the `hagrp -offline` command. You must also unmount the all VxFS/CFS mounts that are not configured under VCS.

To configure the SF Sybase CE components

1 Log in as the superuser on any of the nodes in the cluster.

2 Start the configuration program.

SF Sybase CE installer	Run the program:
	`# cd /opt/VRTS/install`
	`# ./installsfsybasece -configure galaxy nebula`

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

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

3 Enter **1** to select the option **Configure SF Sybase CE sub-components**.

```
1)  Configure Cluster File System
2)  Configure I/O Fencing in Sybase Mode
3)  Configure Sybase ASE CE Instance in VCS
4)  Exit SFSYBASECE Configuration
Choose option: [1-4,q] (1)
```

4 If you had quit the installer in the process of an active configuration, the installer discovers that installer process and provides the option of resuming the configuration or starting a new configuration. Provide a suitable response.

```
The installer has discovered an existing installer process.
The process exited while performing configure of
SF Sybase CE on galaxy.
Do you want to resume this process? [y,n,q,?] (y) n
```

5 Configure the Veritas Cluster Server component to set up the SF Sybase CE cluster.

See "Configuring the SF Sybase CE cluster" on page 92.

6 Add VCS users.

See "Adding VCS users" on page 101.

7 Configure SMTP email notification.

See "Configuring SMTP email notification" on page 102.

8 Configure SNMP trap notification.

See "Configuring SNMP trap notification" on page 104.

Configuring the SF Sybase CE cluster

Configure the sytems on which you installed SF Sybase CE to be part of your cluster.

To configure a cluster for SF Sybase CE

1 Log in to the installer.

See "Configuring the SF Sybase CE components using the script-based installer" on page 90.

2 Select the **Configure Cluster File System** option from the main menu.

Press Return to continue.

If there are any SF Sybase CE processes running, these processes are stopped. Press Return to continue.

3 VCS configuration includes configuring the cluster, users, secure mode if required, and notification.

To configure a cluster:

- Configure the cluster name.
  See "Configuring the cluster name" on page 92.
- Configure private heartbeat links.
  See "Configuring private heartbeat links" on page 93.

Configuring the cluster name

Enter the cluster information when the installer prompts you.

To configure the cluster

1 Review the configuration instructions that the installer presents.

2 Enter a unique cluster name.

```
Enter the unique cluster name: [q,?] syb_cluster101
```

Configuring private heartbeat links

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

The following procedure helps you configure LLT over Ethernet.

To configure private heartbeat links

1. Choose one of the following options at the installer prompt based on whether you want to configure LLT over Ethernet or UDP.

   - Option 1: LLT over Ethernet (answer installer questions)
     Enter the heartbeat link details at the installer prompt to configure LLT over Ethernet.
     Skip to step 2.

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

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

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

   The installer discovers and lists the network interface cards.

   Answer the installer prompts. The following example shows different NICs based on architecture:

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

     ```
     Enter the NIC for the first private heartbeat link on system1:
     [b,q,?] bge1
     Would you like to configure a second private heartbeat link?
     ```

```
[y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on system1:
[b,q,?] bge2
Would you like to configure a third private heartbeat link?
[y,n,q,b,?](n)
```

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

```
Enter the NIC for the first private heartbeat
link on system1: [b,q,?] private_NIC1
Do you want to use address 192.168.0.1 for the
first private heartbeat link on system1: [y,n,q,b,?] (y)
Enter the UDP port for the first private heartbeat
link on system1: [b,q,?] (50000) ?
Would you like to configure a second private
heartbeat link? [y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat
link on system1: [b,q,?] private_NIC2
Do you want to use address 192.168.1.1 for the
second private heartbeat link on system1: [y,n,q,b,?] (y)
Enter the UDP port for the second private heartbeat
link on system1: [b,q,?] (50001) ?
Do you want to configure an additional low priority
heartbeat link? [y,n,q,b,?] (n) y
Enter the NIC for the low priority heartbeat
link on system1: [b,q,?] (private_NIC0)
Do you want to use address 192.168.3.1 for
the low priority heartbeat link on system1: [y,n,q,b,?] (y)
Enter the UDP port for the low priority heartbeat
link on system1: [b,q,?] (50004)
```

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

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

If you want to use the NIC details that you entered for system1, make sure the same NICs are available on each system. Then, enter **y** at the prompt.

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

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

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

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

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

6 Enter a unique cluster ID:

```
Enter a unique cluster ID number between 0-65535: [b,q,?] (60842)
```

The cluster cannot be configured if the cluster ID 60842 is in use by another cluster. Installer performs a check to determine if the cluster ID is duplicate. The check takes less than a minute to complete.

```
Would you like to check if the cluster ID is in use by another
cluster? [y,n,q] (y)
```

7 Verify and confirm the information that the installer summarizes.

Configuring the virtual IP of the cluster

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

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

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

To configure the virtual IP of the cluster

1. Review the required information to configure the virtual IP of the cluster.
2. When the system prompts whether you want to configure the virtual IP, enter `y`.
3. Confirm whether you want to use the discovered public NIC on the first system.

   Do one of the following:

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

   ```
   Active NIC devices discovered on system1: bge0
   Enter the NIC for Virtual IP of the Cluster to use on system1:
   [b,q,?](bge0)
   ```

4. Confirm whether you want to use the same public NIC on all nodes.

   Do one of the following:

   - If all nodes use the same public NIC, enter `y`.
   - If unique NICs are used, enter `n` and enter a NIC for each node.

   ```
   Is bge0 to be the public NIC used by all systems
   [y,n,q,b,?] (y)
   ```

Configuring the cluster in secure mode

The installer prompts whether you want to configure a secure cluster.

```
Would you like to configure the SF Sybase CE cluster in secure mode?
[y,n,q,?] (n)
```

To configure a secure cluster, enter **`y`**.

If you want to confirm that the configured cluster is in secure mode, verify that the output of the following command is 1.

```
# haclus -value SecureClus
```

```
1
```

Setting up trust relationships for your SF Sybase CE cluster

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

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

To set up a trust relationship

1. Ensure that you are logged in as superuser on one of the nodes in the cluster.
2. Enter the following command:

   ```
   # /opt/VRTS/install/installsfsybasece -securitytrust
   ```

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

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

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

   Specify a port number or press Enter to accept the default port.

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

   Specify a valid data directory or press Enter to accept the default directory.
4. The installer performs one of the following actions:
   - If you specified a valid directory, the installer prompts for a confirmation.

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

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

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

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

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

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

Configuring a secure cluster node by node

For environments that do not support passwordless ssh or passwordless rsh, you cannot use the `-security` option to enable secure mode for your cluster. Instead, you can use the `-securityonenode` option to configure a secure cluster node by node.

Table 7-1 lists the tasks that you must perform to configure a secure cluster.

Table 7-1 Configuring a secure cluster node by node

Task	Reference
Configure security on one node	See "Configuring the first node" on page 98.
Configure security on the remaining nodes	See "Configuring the remaining nodes" on page 99.
Complete the manual configuration steps	See "Completing the secure cluster configuration" on page 100.

Configuring the first node

Perform the following steps on one node in your cluster.

To configure security on the first node

1. Ensure that you are logged in as superuser.
2. Enter the following command:

   ```
   # /opt/VRTS/install/installsfsybasece -securityonenode
   ```

   The installer lists information about the cluster, nodes, and service groups. If VCS is not configured or if VCS is not running on all nodes of the cluster, the installer prompts whether you want to continue configuring security. It then prompts you for the node that you want to configure.

   ```
   VCS is not running on all systems in this cluster. All VCS systems
   must be in RUNNING state. Do you want to continue? [y,n,q] (n) y

   1) Perform security configuration on first node and export
   security configuration files.

   2) Perform security configuration on remaining nodes with
   security configuration files.

   Select the option you would like to perform [1-2,q.?] 1
   ```

   Warning: All configurations about cluster users are deleted when you configure the first node. You can use the `/opt/VRTSvcs/bin/hauser` command to create cluster users manually.

   ---

3. The installer completes the secure configuration on the node. It specifies the location of the security configuration files and prompts you to copy these files to the other nodes in the cluster. The installer also specifies the location of log files, summary file, and response file.
4. Copy the security configuration files from the `/var/VRTSvcs/vcsauth/bkup` directory to temporary directories on the other nodes in the cluster.

Configuring the remaining nodes

On each of the remaining nodes in the cluster, perform the following steps.

To configure security on each remaining node

1 Ensure that you are logged in as superuser.

2 Enter the following command:

```
# /opt/VRTS/install/installsfsybasece -securityonenode
```

The installer lists information about the cluster, nodes, and service groups. If VCS is not configured or if VCS is not running on all nodes of the cluster, the installer prompts whether you want to continue configuring security. It then prompts you for the node that you want to configure. Enter **2**.

```
VCS is not running on all systems in this cluster. All VCS systems
must be in RUNNING state. Do you want to continue? [y,n,q] (n) y

1) Perform security configuration on first node and export
security configuration files.

2) Perform security configuration on remaining nodes with
security configuration files.

Select the option you would like to perform [1-2,q.?]  2
```

The installer completes the secure configuration on the node. It specifies the location of log files, summary file, and response file.

Completing the secure cluster configuration

Perform the following manual steps to complete the configuration.

To complete the secure cluster configuration

1 On the first node, freeze all service groups except the ClusterService service group.

```
# /opt/VRTSvcs/bin/haconf -makerw

# /opt/VRTSvcs/bin/hagrp -list Frozen=0

# /opt/VRTSvcs/bin/hagrp -freeze groupname -persistent

# /opt/VRTSvcs/bin/haconf -dump -makero
```

2 On the first node, stop the VCS engine.

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

3 On all nodes, stop the CmdServer.

```
# /opt/VRTSvcs/bin/CmdServer -stop
```

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

```
cluster clus1 (
SecureClus = 1
)
```

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

```
# touch /etc/VRTSvcs/conf/config/.secure
```

6 On the first node, start VCS. Then start VCS on the remaining nodes.

```
# /opt/VRTSvcs/bin/hastart
```

7 On all nodes, start CmdServer.

```
# /opt/VRTSvcs/bin/CmdServer
```

8 On the first node, unfreeze the service groups.

```
# /opt/VRTSvcs/bin/haconf -makerw
```

```
# /opt/VRTSvcs/bin/hagrp -list Frozen=1
```

```
# /opt/VRTSvcs/bin/hagrp -unfreeze groupname -persistent
```

```
# /opt/VRTSvcs/bin/haconf -dump -makero
```

Adding VCS users

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

To add VCS users

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

```
Do you wish to accept the default cluster credentials of
'admin/password'? [y,n,q] (y) n
Enter the user name: [b,q,?] (admin)
Enter the password:
Enter again:
```

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

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

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

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

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

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

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

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

Configuring SMTP email notification

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

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

To configure SMTP email notification

1. Review the required information to configure the SMTP email notification.
2. Specify whether you want to configure the SMTP notification.

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

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

   See "Configuring SNMP trap notification" on page 104.
3. Provide information to configure SMTP notification.

   Provide the following information:

   - Enter the NIC information.

     ```
     Active NIC devices discovered on system1: bge0
     Enter the NIC for the VCS Notifier to use on system1:
     [b,q,?] (bge0)
     Is bge0 to be the public NIC used by all systems?
     [y,n,q,b,?] (y)
     ```

   - Enter the SMTP server's host name.

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

   - Enter the email address of each recipient.

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

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

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

4. Add more SMTP recipients, if necessary.

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

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

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

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

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

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

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

5 Verify and confirm the SMTP notification information.

```
NIC: bge0

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

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

Configuring SNMP trap notification

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

Note that you can also configure the notification after installation.

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

To configure the SNMP trap notification

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

2 Specify whether you want to configure the SNMP notification.

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

See "Configuring global clusters" on page 106.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

```
Active NIC devices discovered on system1: bge0
Enter the NIC for the VCS Notifier to use on system1:
[b,q,?] (bge0)
Is bge0 to be the public NIC used by all systems?
[y,n,q,b,?] (y)
```

- Enter the SNMP trap daemon port.

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

- Enter the SNMP console system name.

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

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

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

4 Add more SNMP consoles, if necessary.

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

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

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

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

5 Verify and confirm the SNMP notification information.

```
NIC: bge0

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

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

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

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

To configure the global cluster option

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

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

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

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

3 Provide information to configure this cluster as global cluster.

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

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

4 Verify and confirm the configuration of the global cluster.

```
Global Cluster Option configuration verification:

NIC: bge0
IP: 192.168.1.16
Netmask: 255.255.240.0

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

Configuring SF Sybase CE clusters for data integrity

This chapter includes the following topics:

Setting up disk-based I/O fencing using installsfsybasece

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

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

1. List the new external disks or the LUNs as recognized by the operating system. On each node, enter:

   ```
   # devfsadm
   ```

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

   - Use the interactive vxdiskadm utility to initialize the disks as VxVM disks. For more information see the *Veritas Storage Foundation Administrator's Guide*.
   - Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

```
# vxdisksetup -i device_name
```

The example specifies the CDS format:

```
# vxdisksetup -i c2t13d0
```

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

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See "Initializing disks as VxVM disks" on page 109.

Review the following procedure to identify disks to use as coordinator disks.

To identify the coordinator disks

1. List the disks on each node.

   For example, execute the following commands to list the disks:

   ```
   # vxdisk -o alldgs list
   ```

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

   See "Checking shared disks for I/O fencing" on page 110.

Checking shared disks for I/O fencing

Make sure that the shared storage you set up while preparing to configure SF Sybase CE meets the I/O fencing requirements. You can test the shared disks using the vxfentsthdw utility. The two nodes must have `ssh` (default) or `rsh` communication. To confirm whether a disk (or LUN) supports SCSI-3 persistent reservations, two nodes must simultaneously have access to the same disks. Because a shared disk is likely to have a different name on each node, check the serial number to verify the identity of the disk. Use the `vxfenadm` command with the `-i` option. This command option verifies that the same serial number for the LUN is returned on all paths to the LUN.

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

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

See the *Veritas Storage Foundation for Sybase ASE CE Administrator's Guide*.

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

- Verifying the Array Support Library (ASL)
  See "Verifying Array Support Library (ASL)" on page 111.
- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 112.
- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 113.

Verifying Array Support Library (ASL)

Make sure that the Array Support Library (ASL) for the array that you add is installed.

To verify Array Support Library (ASL)

1. If the Array Support Library (ASL) for the array that you add is not installed, obtain and install it on each node before proceeding.

   The ASL for the supported storage device that you add is available from the disk array vendor or Symantec technical support.

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

   The following output is a sample:

   ```
   # vxddladm listsupport all


   LIBNAME              VID                  PID
   ============================================================
   libvx3par.so         3PARdata             VV
   libvxCLARiiON.so     DGC                  All
   libvxFJTSYe6k.so     FUJITSU              E6000
   libvxFJTSYe8k.so     FUJITSU              All
   libvxap.so           SUN                  All
   libvxatf.so          VERITAS              ATFNODES
   libvxcompellent.so   COMPELNT             Compellent Vol
   libvxcopan.so        COPANSYS             8814, 8818
   ```

3. Scan all disk drives and their attributes, update the VxVM device list, and reconfigure DMP with the new devices. Type:

   ```
   # vxdisk scandisks
   ```

   See the Veritas Volume Manager documentation for details on how to add and configure disks.

Verifying that the nodes have access to the same disk

Before you test the disks that you plan to use as shared data storage or as coordinator disks using the vxfentsthdw utility, you must verify that the systems see the same disk.

To verify that the nodes have access to the same disk

1. Verify the connection of the shared storage for data to two of the nodes on which you installed SF Sybase CE.

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

```
# vxfenadm -i diskpath
```

Refer to the `vxfenadm` (1M) manual page.

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

From node A, enter:

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

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

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

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

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

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

Testing the disks using vxfentsthdw utility

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

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

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

```
The disk /dev/rdsk/c1t1d0s2 is ready to be configured for I/O Fencing on
node system1
```

For more information on how to replace coordinator disks, refer to the *Veritas Storage Foundation for Sybase ASE CE Administrator's Guide*.

To test the disks using vxfentsthdw utility

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

2. From one node, start the utility.

   Run the utility with the -n option if you use `rsh` for communication.

   ```
   # vxfentsthdw [-n]
   ```

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

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

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

   Do you still want to continue : [y/n] (default: n) y
   Enter the first node of the cluster: system1
   Enter the second node of the cluster: system2
   ```

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

   ```
   Enter the disk name to be checked for SCSI-3 PGR on node
   IP_adrs_of_system1 in the format:
   for dmp: /dev/vx/rdmp/cxtxdxsx
   for raw: /dev/rdsk/cxtxdxsx
   Make sure it's the same disk as seen by nodes
   IP_adrs_ofsystem1 and IP_adrs_of_system2
     /dev/rdsk/c2t13d0s2

   Enter the disk name to be checked for SCSI-3 PGR on node
   IP_adrs_of_system2 in the format:
   for dmp: /dev/vx/rdmp/cxtxdxsx
   for raw: /dev/rdsk/cxtxdxsx
   Make sure it's the same disk as seen by nodes
   IP_adrs_ofsystem1 and IP_adrs_of_system2
     /dev/rdsk/c2t13d0s2
   ```

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

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

6 If a disk is ready for I/O fencing on each node, the utility reports success for each node. For example, the utility displays the following message for the node system1.

```
The disk is now ready to be configured for I/O Fencing on node
system1

ALL tests on the disk /dev/rdsk/c1t1d0s2 have PASSED
The disk is now ready to be configured for I/O Fencing on node
system1
```

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

Configuring disk-based I/O fencing using installsfsybasece

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

To set up disk-based I/O fencing using the installsfsybasece

1 Start the installsfsybasece with `-fencing` option.

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

The installsfsybasece starts with a copyright message and verifies the cluster information.

Note the location of log files which you can access in the event of any problem with the configuration process.

2 Confirm that you want to proceed with the I/O fencing configuration at the prompt.

The program checks that the local node running the script can communicate with remote nodes and checks whether SF Sybase CE 6.0 is configured properly.

3 Review the I/O fencing configuration options that the program presents. Type **1** to configure fencing in Sybase mode.

```
Select the fencing mechanism to be configured in this
Application Cluster [1-3,b,q] 1
```

4 Review the output as the configuration program checks whether VxVM is already started and is running.

- If the check fails, configure and enable VxVM before you repeat this procedure.
- If the check passes, then the program prompts you for the coordinator disk group information.

5 Choose whether to use an existing disk group or create a new disk group to configure as the coordinator disk group.

   The program lists the available disk group names and provides an option to create a new disk group. Perform one of the following:

   - To use an existing disk group, enter the number corresponding to the disk group at the prompt.
     The program verifies whether the disk group you chose has an odd number of disks and that the disk group has a minimum of three disks.
   - To create a new disk group, perform the following steps:
     - Enter the number corresponding to the **Create a new disk group** option.
       The program lists the available disks that are in the CDS disk format in the cluster and asks you to choose an odd number of disks with at least three disks to be used as coordinator disks.
       Symantec recommends that you use three disks as coordination points for disk-based I/O fencing.
       If the available VxVM CDS disks are less than the required, installer asks whether you want to initialize more disks as VxVM disks. Choose the disks you want to initialize as VxVM disks and then use them to create new disk group.
     - Enter the numbers corresponding to the disks that you want to use as coordinator disks.
     - Enter the disk group name.

6 Verify that the coordinator disks you chose meet the I/O fencing requirements.

   You must verify that the disks are SCSI-3 PR compatible using the vxfentsthdw utility and then return to this configuration program.

   See "Checking shared disks for I/O fencing" on page 110.

7 After you confirm the requirements, the program creates the coordinator disk group with the information you provided.

8 Enter the I/O fencing disk policy that you chose to use. For example:

```
Enter disk policy for the disk(s) (raw/dmp): [b,q,?] raw
```

   The program also does the following:

- Populates the /etc/vxfendg file with this disk group information
- Populates the /etc/vxfenmode file on each cluster node with the I/O fencing mode information and with the SCSI-3 disk policy information

9 Verify and confirm the I/O fencing configuration information that the installer summarizes.

10 Review the output as the configuration program does the following:

- Stops VCS and I/O fencing on each node.
- Configures disk-based I/O fencing and starts the I/O fencing process.
- Updates the VCS configuration file main.cf if necessary.
- Copies the /etc/vxfenmode file to a date and time suffixed file /etc/vxfenmode-*date-time*. This backup file is useful if any future fencing configuration fails.
- Starts VCS on each node to make sure that the SF Sybase CE is cleanly configured to use the I/O fencing feature.

11 Review the output as the configuration program displays the location of the log files, the summary files, and the response files.

12 Configure the Coordination Point agent to monitor the coordinator disks.

See "Configuring CoordPoint agent to monitor coordination points" on page 121.

Setting up disk-based I/O fencing manually

Table 8-1 lists the tasks that are involved in setting up I/O fencing.

Table 8-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See "Initializing disks as VxVM disks" on page 109.
Identifying disks to use as coordinator disks	See "Identifying disks to use as coordinator disks" on page 110.
Checking shared disks for I/O fencing	See "Checking shared disks for I/O fencing" on page 110.
Setting up coordinator disk groups	See "Setting up coordinator disk groups" on page 118.

Table 8-1 Tasks to set up I/O fencing manually *(continued)*

Task	Reference
Creating I/O fencing configuration files	See "Creating I/O fencing configuration files" on page 119.
Modifying SF Sybase CE configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 120.
Configuring CoordPoint agent to monitor coordination points	See "Configuring CoordPoint agent to monitor coordination points" on page 121.
Starting SF Sybase CE on all nodes	See "Starting SF Sybase CE on all nodes" on page 123.
Verifying I/O fencing configuration	See "Verifying I/O fencing configuration" on page 125.

Setting up coordinator disk groups

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

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

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

The following example procedure assumes that the disks have the device names c1t1d0s2, c2t1d0s2, and c3t1d0s2.

To create the vxfencoorddg disk group

1 On any node, create the disk group by specifying the device names:

```
# vxdg init vxfencoorddg c1t1d0s2 c2t1d0s2 c3t1d0s2
```

2 Set the coordinator attribute value as "on" for the coordinator disk group.

```
# vxdg -g vxfencoorddg set coordinator=on
```

3 Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

4 Import the disk group with the `-t` option to avoid automatically importing it when the nodes restart:

```
# vxdg -t import vxfencoorddg
```

5 Deport the disk group. Deporting the disk group prevents the coordinator disks from serving other purposes:

```
# vxdg deport vxfencoorddg
```

Creating I/O fencing configuration files

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

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

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

1 On each nodes, type:

```
# echo "vxfencoorddg" > /etc/vxfendg
```

Do not use spaces between the quotes in the "vxfencoorddg" text.

This command creates the /etc/vxfendg file, which includes the name of the coordinator disk group.

2 On all cluster nodes depending on the SCSI-3 mechanism, type one of the following selections:

- For DMP configuration:

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

- For raw device configuration:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_raw /etc/vxfenmode
```

3 To check the updated /etc/vxfenmode configuration, enter the following command on one of the nodes. For example:

```
# more /etc/vxfenmode
```

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

/etc/default/vxfen

Modifying VCS configuration to use I/O fencing

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

To modify VCS configuration to enable I/O fencing

1 Save the existing configuration:

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

2 Stop VCS on all nodes:

```
# hastop -all
```

3 If the I/O fencing driver vxfen is already running, stop the I/O fencing driver.

```
# svcadm disable -t vxfen
```

4 Make a backup copy of the main.cf file:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.orig
```

5 On one node, use vi or another text editor to edit the main.cf file. To modify the list of cluster attributes, add the UseFence attribute and assign its value as SCSI3.

```
cluster syb_cluster101(
UserNames = { admin = "cDRpdxPmHpzS." }
Administrators = { admin }
HacliUserLevel = COMMANDROOT
CounterInterval = 5
UseFence = SCSI3
)
```

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

6 Save and close the file.

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

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

8 Using rcp or another utility, copy the VCS configuration file from a node (for example, system1) to the remaining cluster nodes.

For example, on each remaining node, enter:

```
# rcp system1:/etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config
```

Configuring CoordPoint agent to monitor coordination points

The following procedure describes how to manually configure the CoordPoint agent to monitor coordination points.

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

To configure CoordPoint agent to monitor coordination points

1. Ensure that your SF Sybase CE cluster has been properly installed and configured with fencing enabled.
2. Create a parallel service group vxfen and add a coordpoint resource to the vxfen service group using the following commands:

```
# haconf -makerw
# hagrp -add vxfen
# hagrp -modify vxfen SystemList system1 0 system2 1
# hagrp -modify vxfen AutoFailOver 0
# hagrp -modify vxfen Parallel 1
# hagrp -modify vxfen SourceFile "./main.cf"
# hares -add coordpoint CoordPoint vxfen
# hares -modify coordpoint FaultTolerance 1
# hares -modify coordpoint Enabled 1
# haconf -dump -makero
```

3 Verify the status of the agent on the SF Sybase CE cluster using the `hares` commands. For example:

```
# hares -state coordpoint
```

The following is an example of the command and output::

```
# hares -state coordpoint

# Resource     Attribute    System    Value
coordpoint   State        system1   ONLINE
coordpoint   State        system2   ONLINE
```

4 Access the engine log to view the agent log. The agent log is written to the engine log.

The agent log contains detailed CoordPoint agent monitoring information; including information about whether the CoordPoint agent is able to access all the coordination points, information to check on which coordination points the CoordPoint agent is reporting missing keys, etc.

To view all such information in the engine log, change the dbg level for that node using the following commands:

```
# haconf -makerw

# hatype -modify Coordpoint LogDbg 10

# haconf -dump -makero
```

The agent log can now be viewed at the following location:

/var/VRTSvcs/log/engine_A.log

Starting SF Sybase CE on all nodes

You must start SF Sybase CE 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:

```
# svcadm enable vxfen
```

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 131.

To verify GAB port membership

◆ Run the `gabconfig -a` command.

For example:

```
system1# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen  ada401 membership 01
Port b gen  ada40d membership 01
Port f gen  ada41c membership 01
Port h gen  ada40f membership 01
Port u gen  ada41a membership 01
Port v gen  ada416 membership 01
Port w gen  ada418 membership 01
Port y gen  ada424 membership 01
```

Verifying the CVM group is online

Make sure the cvm group is in the online state.

To verify CVM group

1 On any node, run the following command to verify that the cvm group is online:

```
# hagrp -state cvm
```

2 On any node, run the following command to make sure CVM has started properly:

```
# vxclustadm nidmap
```

Verifying I/O fencing configuration

Verify from the vxfenadm output that the SCSI-3 disk policy reflects the configuration in the /etc/vxfenmode file.

To verify I/O fencing configuration

1 On one of the nodes, type:

```
# vxfenadm -d
```

Output similar to the following appears if the fencing mode is SYBASE and the SCSI3 disk policy is dmp:

```
I/O Fencing Cluster Information:
================================

Fencing Protocol Version: 201
Fencing Mode: SYBASE
Fencing SCSI3 Disk Policy: dmp
Cluster Members:

   * 0 (system1)
   1 (system2)

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

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

```
# vxfenconfig -l
```

Chapter 9

Performing post-installation and configuration tasks

This chapter includes the following topics:

Installing language packages

To install SF Sybase CE in a language other than English, install the required language packages after installing the English packages.

To install the language packages on the server

1. Insert the "Language" disc into the DVD-ROM or CD-ROM drive. With Solaris volume management software, the disc is automatically mounted as `/cdrom/cdrom0`.
2. Install the language packages using the `install_lp` command.

```
# cd /cdrom/cdrom0
# ./install_lp
```

Performing a postcheck on a node

The installer's `postcheck` command can help you to determine installation-related problems and provide troubleshooting information.

See "About using the postcheck option" on page 355.

To run the postcheck command on a node

1. Run the installer with the `-postcheck` option.

```
# ./installer -postcheck system_name
```

2. Review the output for installation-related information.

Verifying SF Sybase CE installation using VCS configuration file

The configuration file, main.cf, is created on each node at /etc/VRTSvcs/conf/config/. Review the main.cf configuration file after the SF Sybase CE installation and before the Sybase installation.

Verify the following information in the main.cf file:

- The cluster definition within the main.cf includes the cluster information that was provided during the configuration. The cluster information includes the cluster name, cluster address, and the names of cluster users and administrators.
- The UseFence = SCSI3 attribute is not automatically present; you must manually add it after the installation.
- If you configured the cluster in secure mode, the "SecureClus = 1" cluster attribute is set.

For more information on the configuration file:

Verifying LLT, GAB, and cluster operation

Verify the operation of LLT, GAB, and the cluster using the VCS commands.

To verify LLT, GAB, and cluster operation

1. Log in to any node in the cluster as superuser.
2. Make sure that the PATH environment variable is set to run the VCS commands.
3. Verify LLT operation.

   See "Verifying LLT" on page 129.
4. Verify GAB operation.

   See "Verifying GAB" on page 131.
5. Verify the cluster operation.

   See "Verifying the cluster" on page 132.

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 system1.
2. Run the `lltstat` command on the node system1 to view the status of LLT.

   ```
   lltstat -n
   ```

   The output on system1 resembles:

   ```
   LLT node information:
       Node                 State            Links
       *0 system1              OPEN             2
        1 system2              OPEN             2
   ```

   Each node has two links and each node is in the OPEN state. The asterisk (*) denotes the node on which you typed the command.

If LLT does not operate, the command does not return any LLT links information: If only one network is connected, the command returns the following LLT statistics information:

```
LLT node information:
    Node                 State    Links
   * 0 system1            OPEN        2
     1 system2            OPEN        2
     2 system3            OPEN        1
```

3 Log in as superuser on the node system2.

4 Run the `lltstat` command on the node system2 to view the status of LLT.

```
lltstat -n
```

The output on system2 resembles:

```
    LLT node information:
        Node             State          Links
         0 system1          OPEN           2
        *1 system2          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 system1 in a two-node cluster:

```
lltstat -nvv active
```

The output on system1 resembles the following:

- For Solaris SPARC:

```
Node          State      Link    Status      Address
*0 system1      OPEN
                         bge1 UP     08:00:20:93:0E:34
                         bge2 UP     08:00:20:93:0E:38
1 system2       OPEN
                         bge1 UP     08:00:20:8F:D1:F2
                         bge2 DOWN
```

The command reports the status on the two active nodes in the cluster, system1 and system2.

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 system2. 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 system1 in a two-node cluster:

```
lltstat -p
```

The output resembles:

```
LLT port information:
  Port  Usage       Cookie
  0     gab          0x0
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  7     gab          0x7
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
  31    gab          0x1F
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
        connects:    0 1
```

Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information. The output displays the nodes that have membership with the modules you installed and configured. You can use GAB port membership as a method of determining if a specific component of the SF Sybase CE stack communicates with its peers.

Table 9-1 lists the different ports that the software configures for different functions.

Table 9-1 GAB port description

Port	Function
a	GAB

Table 9-1 GAB port description *(continued)*

Port	Function
b	I/O fencing
f	Cluster File System (CFS)
h	Veritas Cluster Server (VCS: High Availability Daemon)
u	Cluster Volume Manager (CVM) (to ship commands from slave node to master node) Port u in the `gabconfig` output is visible with CVM protocol version >= 100.
v	Cluster Volume Manager (CVM)
w	vxconfigd (module for CVM)
y	Cluster Volume Manager (CVM) I/O shipping

For more information on GAB, refer to the *Veritas Cluster Server Administrator's Guide*.

To verify GAB

- To verify the GAB operation, type the following command on each node:

  ```
  # /sbin/gabconfig -a
  ```

  For example, the command returns the following output:

  ```
  GAB Port Memberships
  ===============================================================
  Port a gen  ada401 membership 01
  Port b gen  ada40d membership 01
  Port f gen  ada41c membership 01
  Port h gen  ada40f membership 01
  Port u gen  ada41a membership 01
  Port v gen  ada416 membership 01
  Port w gen  ada418 membership 01
  Port y gen  ada42a membership 01
  ```

Verifying the cluster

Verify the status of the cluster using the `hastatus` command. This command returns the system state and the group state.

Refer to the `hastatus(1M)` manual page.

Refer to the *Veritas Cluster Server Administrator's Guide* for a description of system states and the transitions between them.

To verify the cluster

1 To verify the status of the cluster, type the following command:

```
# hastatus -summary
```

The output resembles:

```
-- SYSTEM STATE
-- System              State                   Frozen

A  system1               RUNNING                 0
A  system2               RUNNING                 0

-- GROUP STATE
-- Group           System        Probed  AutoDisabled   State
```

2 Review the command output for the following information:

- The system state
  If the value of the system state is RUNNING, the cluster is successfully started.

Verifying the cluster nodes

Verify the information of the cluster systems using the `hasys -display` command. The information for each node in the output should be similar.

Refer to the `hasys(1M)` manual page.

Refer to the *Veritas Cluster Server Administrator's Guide* for information about the system attributes for VCS.

To verify the cluster nodes

◆ On one of the nodes, type the `hasys -display` command:

```
# hasys -display
```

The example shows the output when the command is run on the node system1. The list continues with similar information for system2 (not shown) and any other nodes in the cluster.

```
#System    Attribute              Value
system1    AgentsStopped          0
system1    AvailableCapacity      100
system1    CPUBinding             BindTo None CPUNumber 0
system1    CPUThresholdLevel      Critical 90 Warning 80 Note 70
                                  Info 60
system1    CPUUsage               0
system1    CPUUsageMonitoring     Enabled 0 ActionThreshold 0
                                  ActionTimeLimit 0 Action NONE
                                  NotifyThreshold 0 NotifyTimeLimit 0

system1    Capacity               100
system1    ConfigBlockCount       130
system1    ConfigCheckSum         46688
system1    ConfigDiskState        CURRENT
system1    ConfigFile             /etc/VRTSvcs/conf/config
system1    ConfigInfoCnt          0
system1    ConfigModDate          Thu Sep 22 07:14:23 CDT 2011
system1    ConnectorState         Down
system1    CurrentLimits
system1    DiskHbStatus
system1    DynamicLoad            0
system1    EngineRestarted        0
system1    EngineVersion          6.0.00.0
system1    FencingWeight          0
system1    Frozen                 0
system1    GUIIPAddr
system1    HostUtilization        CPU 7 Swap 0
```

```
system1    LLTNodeId             0
system1    LicenseType           PERMANENT_SITE
system1    Limits
system1    LinkHbStatus          bge1 UP bge2 UP
system1    LoadTimeCounter       0
system1    LoadTimeThreshold     600
system1    LoadWarningLevel      80
system1    NoAutoDisable         0
system1    NodeId                0
system1    OnGrpCnt              1
system1    PhysicalServer
system1    ShutdownTimeout       600
system1    SourceFile            ./main.cf
system1    SwapThresholdLevel    Critical 90 Warning 80 Note 70
                                 Info 60
system1    SysInfo               Solaris:system1,Generic_
                                 118558-11,5.9,sun4u
system1    SysName               system1
system1    SysState              RUNNING
system1    SystemLocation
system1    SystemOwner
system1    SystemRecipients
system1    TFrozen               0
system1    TRSE                  0
system1    UpDownState           Up
system1    UserInt               0
system1    UserStr
```

```
system1    VCSFeatures          NONE

system1    VCSMode
```

About enabling LDAP authentication for clusters that run in secure mode

Symantec Product Authentication Service (AT) supports LDAP (Lightweight Directory Access Protocol) user authentication through a plug-in for the authentication broker. AT supports all common LDAP distributions such as Oracle Directory Server, Netscape, OpenLDAP, and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

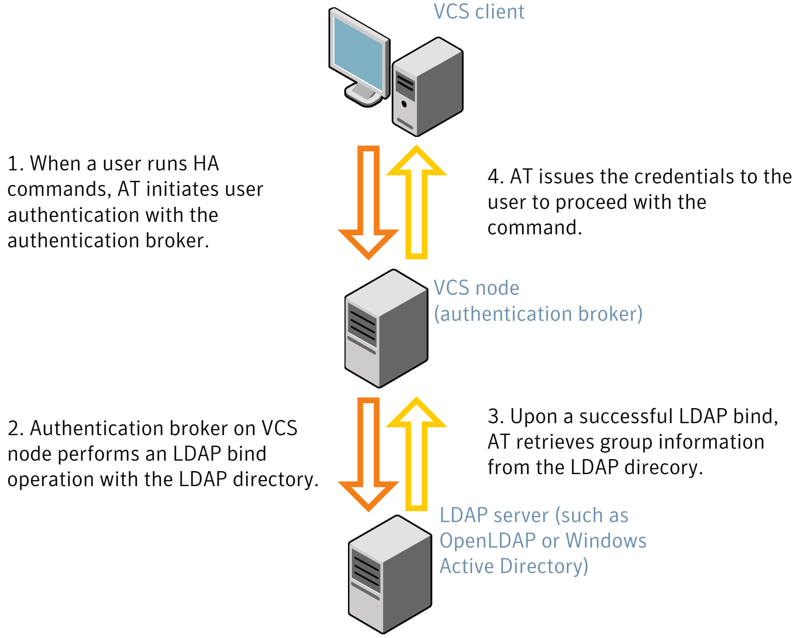
See "Enabling LDAP authentication for clusters that run in secure mode" on page 138.

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

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

Figure 9-1 depicts the SF Sybase CE cluster communication with the LDAP servers when clusters run in secure mode.

Figure 9-1 Client communication with LDAP servers



The LDAP schema and syntax for LDAP commands (such as, ldapadd, ldapmodify, and ldapsearch) vary based on your LDAP implementation.

Before adding the LDAP domain in Symantec Product Authentication Service, note the following information about your LDAP environment:

- The type of LDAP schema used (the default is RFC 2307)
  - UserObjectClass (the default is posixAccount)
  - UserObject Attribute (the default is uid)
  - User Group Attribute (the default is gidNumber)
  - Group Object Class (the default is posixGroup)
  - GroupObject Attribute (the default is cn)
  - Group GID Attribute (the default is gidNumber)
  - Group Membership Attribute (the default is memberUid)
- URL to the LDAP Directory
- Distinguished name for the user container (for example, UserBaseDN=ou=people,dc=comp,dc=com)

- Distinguished name for the group container (for example, GroupBaseDN=ou=group,dc=comp,dc=com)

Enabling LDAP authentication for clusters that run in secure mode

The following procedure shows how to enable the plug-in module for LDAP authentication. This section provides examples for OpenLDAP and Windows Active Directory LDAP distributions.

Before you enable the LDAP authentication, complete the following steps:

- Make sure that the cluster runs in secure mode.

  ```
  # haclus -value SecureClus
  ```

  The output must return the value as 1.

- Make sure that the AT version is 6.1.6.0 or later.

  ```
  # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion
  vssat version: 6.1.6.0
  ```

See the `vssat.1m` and the `atldapconf.1m` manual pages.

To enable OpenLDAP authentication for clusters that run in secure mode

1 Add the LDAP domain to the AT configuration using the `vssat` command.

The following example adds the LDAP domain, MYENTERPRISE:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat addldapdomain \
--domainname "MYENTERPRISE.symantecdomain.com"\
--server_url "ldap://my_openldap_host.symantecexample.com"\
--user_base_dn "ou=people,dc=symantecdomain,dc=myenterprise,dc=com"\
--user_attribute "cn" --user_object_class "account"\
--user_gid_attribute "gidNumber"\
--group_base_dn "ou=group,dc=symantecdomain,dc=myenterprise,dc=com"\
--group_attribute "cn" --group_object_class "posixGroup"\
--group_gid_attribute "member"\
--admin_user "cn=manager,dc=symantecdomain,dc=myenterprise,dc=com"\
--admin_user_password "password" --auth_type "FLAT"
```

2 Verify that you can successfully authenticate an LDAP user on the SF Sybase CE 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.

```
system1# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat authenticate
--domain ldap:MYENTERPRISE.symantecdomain.com
--prplname vcsadmin1 --broker system1:14149

Enter password for vcsadmin1: ##########

authenticate
----------------------
----------------------

Authenticated User vcsadmin1
----------------------
```

3 Add the LDAP user to the main.cf file.

```
# haconf makerw
# hauser -add "CN=vcsadmin1/CN=people/\
DC=symantecdomain/DC=myenterprise/\
DC=com@myenterprise.symantecdomain.com" -priv Administrator
# haconf -dump -makero
```

If you want to enable group-level authentication, you must run the following command:

```
# hauser -addpriv \
ldap_group@ldap_domain AdministratorGroup
```

4 Verify that the main.cf file has the following lines:

```
# cat /etc/VRTSvcs/conf/config/main.cf
...
...
cluster syb_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 the Korn shell (ksh), run the following commands:

```
# export VCS_DOMAIN=myenterprise.symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
system1     Attribute  RUNNING
system2     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SF Sybase CE node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

To enable Windows Active Directory authentication for clusters that run in secure mode

1. Run the LDAP configuration tool atldapconf using the -d option. The -d option discovers and retrieves an LDAP properties file which is a prioritized attribute list.

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -d \
   -s domain_controller_name_or_ipaddress \
   -u domain_user -g domain_group
   ```

   For example:

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
   -d -s 192.168.20.32 -u Administrator -g "Domain Admins"
   Search User provided is invalid or Authentication is required to
   proceed further.
   Please provide authentication information for LDAP server.

   Username/Common Name: symantecdomain\administrator
   Password:

   Attribute file created.
   ```

2. Run the LDAP configuration tool atldapconf using the -c option. The -c option creates a CLI file to add the LDAP domain.

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
   -c -d windows_domain_name
   ```

   For example:

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
   -c -d symantecdomain.com
   Attribute list file not provided, using default AttributeList.txt.
   CLI file name not provided, using default CLI.txt.

   CLI for addldapdomain generated.
   ```

3. Run the LDAP configuration tool atldapconf using the -x option. The -x option reads the CLI file and executes the commands to add a domain to the AT.

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -x
   ```

4 List the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat listldapdomains

Domain Name :          symantecdomain.com
Server URL :           ldap://192.168.20.32:389
SSL Enabled :          No
User Base DN :         CN=people,DC=symantecdomain,DC=com
User Object Class :    account
User Attribute :       cn
User GID Attribute :   gidNumber
Group Base DN :        CN=group,DC=symantecdomain,DC=com
Group Object Class :   group
Group Attribute :      cn
Group GID Attribute : cn
Auth Type :            FLAT
Admin User :
Admin User Password :
Search Scope :         SUB
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh) or the Korn shell (ksh), run the following commands:

```
# export VCS_DOMAIN=symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
system1     Attribute  RUNNING
system2     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the SF Sybase CE node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

Configuring Veritas Volume Replicator

Perform this step only if you have not already configured VVR during the installation.

By default, the installer installs the required VVR configuration files irrespective of whether or not you choose to enable VVR. To configure VVR manually in SF Sybase CE, simply start VVR using the `vxstart_vvr` command . The command starts the VVR daemons and configures the ports. You may change the default settings at any time.

For instructions on changing the default settings, see the *Veritas Volume Replicator Administrator's Guide*.

To configure VVR

1 Log into each node in the cluster as the root user.

2 Start VVR:

```
# vxstart_vvr start
VxVM VVR INFO V-5-2-3935 Using following ports:
heartbeat: 4145
vradmind: 8199
vxrsyncd: 8989
data: Anonymous-Ports
To change, see vrport(1M) command
VxVM VVR  V-5-2-5942 Starting Communication daemon: [OK]
```

Running SORT Data Collector to collect configuration information

SORT Data Collector now supersedes the VRTSexplorer utility. Run the Data Collector with the `VxExplorer` option to gather information about the system.

Visit the SORT Website and download the UNIX Data Collector appropriate for your operating system.

https://sort.symantec.com

For more information:

https://sort.symantec.com/public/help/wwhelp/wwhimpl/js/html/wwhelp.htm

Section 3

Upgrade of SF Sybase CE

Chapter 10

About upgrading to SF Sybase CE 6.0

This chapter includes the following topics:

About types of upgrade

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

SF Sybase CE does not support upgrades using the Web installer.

Table 10-1 lists the supported types of upgrade.

Table 10-1 Types of upgrade

Type of upgrade	Method of upgrade	Procedures
Full upgrade	Veritas script-based installation programs ■ Interactive mode ■ Non-interactive mode using response files	Complete the following steps: ■ Preparing to upgrade ■ Upgrading to SF Sybase CE 6.0 See the chapter *Performing a full upgrade to SF Sybase CE 6.0.* ■ Completing post-upgrade tasks See the chapter *Performing post-upgrade tasks.*

Table 10-1 Types of upgrade *(continued)*

Type of upgrade	Method of upgrade	Procedures
Phased upgrade	Combination of manual steps and the Veritas script-based installation programs	Complete the steps in the chapter *Performing a phased upgrade to SF Sybase CE 6.0.*
Solaris Live Upgrade	Combination of native operating system upgrade mechanism and the Veritas script-based installation programs	Complete the following steps: ■ Upgrading to SF Sybase CE 6.0 See the chapter *Upgrading to SF Sybase CE 6.0 using Live Upgrade.* ■ Completing post-upgrade tasks See the chapter *Performing post-upgrade tasks.*

Supported upgrade paths

Table 10-2 lists the supported upgrade paths.

Table 10-2 Supported upgrade paths

From SF Sybase CE version	To SF Sybase CE version	Supported upgrade type
5.0.1 and later (including maintenance packs and rolling patches on 5.0.1)	6.0	Full or phased upgrade

Chapter 11

Performing a full upgrade to SF Sybase CE 6.0

This chapter includes the following topics:

About full upgrades

A full upgrade involves upgrading all the nodes in the cluster at the same time. The cluster remains unavailable for the duration of the upgrade.

Note: You can not roll back the upgrade to a previous version after you upgrade to version 6.0.

You can perform the upgrade using one of the following Veritas script-based installation programs:

- Common product installer (`installer` or `webinstaller`)
  The common product installer provides menu options for installing and configuring multiple Veritas products.
- SF Sybase CE installation programs (`installsfsybasece`)
  The SF Sybase CE installation program provide menu options for installing and configuring SF Sybase CE.

Note: If you obtained SF Sybase CE from an electronic download site, you must use the product installer (`installsfsybasece`) instead of the common product installer (`installer`).

You can also perform a full upgrade using a response file. You can create a response file by using the response file template or by customizing a response file that is generated by the script-based installer.

For more information about response files:

See "About response files" on page 217.

Preparing to perform a full upgrade to SF Sybase CE 6.0

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

To prepare to upgrade SF Sybase CE

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

   For example:

   ```
   # cp /etc/VRTSvcs/conf/config/main.cf \
   /etc/VRTSvcs/conf/config/main.cf.save
   # cp /etc/VRTSvcs/conf/config/types.cf \
   /etc/VRTSvcs/conf/config/types.cf.save
   # cp /etc/VRTSvcs/conf/config/SybaseTypes.cf \
   /var/tmp/SybaseTypes.cf.save
   ```

3 Stop all applications that use VxFS or VxVM disk groups, whether local or CFS.

If the applications are under VCS control:

```
# hagrp -offline grp_name -any
```

If the applications are not under VCS control:

Use native application commands to stop the application.

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

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

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

```
# haconf -makerw
# hagrp -modify sybase_group AutoStart 0
# haconf -dump -makero
```

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

```
# mount -v |grep vxfs

# fuser -c /mount_point

# umount /mount_point
```

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

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

7 Stop VCS on all nodes:

```
# hastop -all
```

Note: The installer displays the following warning:

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

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

One way to check whether or not the configuration is valid is to check the main.cf file as follows:

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

However, this method can not verify whether all configurations are vaild. If SF Sybase CE was running properly before the upgrade, the configurations are valid.

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

```
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# modunload -i module_no
# /etc/init.d/llt stop
```

Upgrading to SF Sybase CE 6.0

Perform the steps in the following procedure to upgrade to SF Sybase CE 6.0.

To upgrade to SF Sybase CE 6.0

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

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

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

- Upgrade the operating system on all nodes in the cluster.
  For instructions, see the operating system documentation.
- After the system restarts, restore the `/etc/llttab` file to its original name:

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

2 Upgrade to SF Sybase CE 6.0 using the script-based installer.

See "Upgrading SF Sybase CE using the Veritas script-based installation program" on page 156.

You can also perform a silent upgrade:

See "Upgrading SF Sybase CE using a response file" on page 158.

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

4 Bring the Sybase Binaries service group (binmnt group) online.

```
# hagrp -online binmnt -sys node_name
```

5 Bring the sybasece resource group online.

```
# hagrp -online sybasece -sys node_name
```

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

7
- If Sybase is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the Sybase Binaries service group (binmnt) and sybasece service group online automatically when VCS starts:

  ```
  # haconf -makerw
  # hagrp -modify sybasece AutoStart 1
  # haconf -dump -makero
  ```

8 Complete other post-upgrade steps.

For instructions, see the chapter *Performing post-upgrade tasks* in this document.

9 Upgrade Sybase ASE CE.

For instructions, see the section *Upgrading Sybase ASE CE* in this document.

10 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

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

```
# vxdctl upgrade
```

Upgrading SF Sybase CE using the Veritas script-based installation program

Use one of the following Veritas script-based installation programs to upgrade SF Sybase CE: `installer` or `installsfsybasece`

The installer performs the following tasks to upgrade SF Sybase CE:

- Verifies the compatibility of the systems before the upgrade.
- Stops the SF Sybase CE processes before the upgrade.
- Uninstalls SF Sybase CE.
- Installs the SF Sybase CE 6.0 packages on the nodes.
- Starts SF Sybase CE 6.0 on all the nodes.
- Displays the location of the log files, summary file, and response file.

Note: The SF Sybase CE processes are started automatically after the upgrade completes successfully.

To upgrade to SF Sybase CE 6.0 using the installsfsybasece program

1 Start the installation program using one of the following ways:

SF Sybase CE installer	Navigate to the product directory on the installation media that contains the installation program. The program is located in the `storage_foundation_for_sybase_ce` directory. Run the program: `# ./installsfsybasece galaxy nebula`
Common product installer	Navigate to the product directory on the installation media that contains the installation program. Run the program: `# ./installer galaxy nebula` From the opening Selection Menu, choose **G** for "**Upgrade a Product**." Select the option **Full Upgrade**." Select the option **Veritas Storage Foundation for Sybase ASE CE**.

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

2 Enter **3** to install all the SF Sybase CE packages.

The installer verifies the systems for compatibility.

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

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

3 Press **Enter** to continue with the upgrade.

Depending on the installation option selected, the installer displays the list of packages that will be installed.

The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's book disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer y.

4 Enter the name of the backup boot disk group when prompted. Press **Enter** to accept the default.

You are prompted to start the split operation.

5 Enter **y** to continue with the split operation.

The split operation can take some time to complete.

Note: Verify the boot device from which the system is set to boot. Make sure that the system is set to start from the boot device with the required version of SF Sybase CE.

---

6 Enter **y** to stop the SF Sybase CE processes.

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

The installer stops the processes and uninstalls SF Sybase CE. After the uninstallation, the installer installs SF Sybase CE 6.0 and starts SF Sybase CE 6.0 on all the nodes.

7 Install the language packages and patches if you would like to run SF Sybase CE in a language other than English.

See "Installing language packages" on page 127.

8 Complete the remaining tasks to finish the upgrade:

See "Upgrading to SF Sybase CE 6.0" on page 154.

Upgrading SF Sybase CE using a response file

You can upgrade from SF Sybase CE version 5.0 and later using a response file.

Perform the steps in the following procedure to upgrade to SF Sybase CE 6.0 using a response file.

To upgrade SF Sybase CE using a response file

1. Upgrade the operating system, if required.

   For instructions, see the operating system documentation.

2. Create a response file using one of the available options.

   Note: Make sure that you replace the host names in the response file with the names of the systems that you plan to upgrade.

   For information on various options available for creating a response file:

   See "About response files" on page 217.

   For response file variable definitions:

   See "Response file variables to upgrade SF Sybase CE" on page 159.

   For a sample response file:

   See "Sample response file for upgrading SF Sybase CE" on page 161.

3. Navigate to the product directory on the installation media that contains the SF Sybase CE installation program.

4. Start the installation:

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

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

5. Complete the post-upgrade steps.

Response file variables to upgrade SF Sybase CE

Table 11-1 lists the response file variables that you can define to upgrade SF Sybase CE.

Table 11-1 Response file variables specific to upgrading SF Sybase CE

Variable	List or Scalar	Description
CFG{opt}{upgrade}	Scalar	Upgrades SF Sybase CE packages. (Required)
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)

Table 11-1 Response file variables specific to upgrading SF Sybase CE *(continued)*

Variable	List or Scalar	Description
CFG{systems}	List	List of systems on which the product is to be upgraded. (Required)
CFG{prod}	Scalar	Defines the product to be upgraded. (Optional)
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{pkgpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. (Optional)

Table 11-1 Response file variables specific to upgrading SF Sybase CE *(continued)*

Variable	List or Scalar	Description
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)

Sample response file for upgrading SF Sybase CE

The following sample response file performs a full upgrade on the system galaxy.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{upgrade}=1;
$CFG{opt}{vr}=1;
$CFG{systems}=[ qw(galaxy) ];
$CFG{vcs_allowcomms}=1;
```

Chapter 12

Performing a phased upgrade to SF Sybase CE 6.0

This chapter includes the following topics:

About phased upgrade

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

For supported upgrade paths:

See "Supported upgrade paths" on page 150.

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 examples in the procedures assume a four-node SF Sybase CE 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 Sybase CE from version 5.0 and later releases

Table 12-1 illustrates the phased upgrade process. Each column describes the steps to be performed on the corresponding subcluster and the status of the subcluster when operations are performed on the other subcluster.

Table 12-1 Summary of phased upgrade

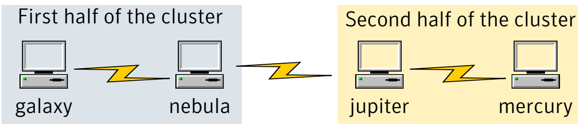
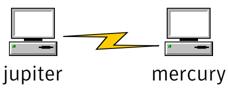
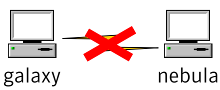
<table>
<tr><th>First half of the cluster</th><th>Second half of the cluster</th></tr>
<tr><td colspan="2">SF Sybase CE cluster before the upgrade:
</td></tr>
<tr><td>STEP 1: Perform the following pre-upgrade steps:
Switch failover applications.
Stop all parallel applications.
See “Step 1: Performing pre-upgrade tasks on the first half of the cluster” on page 165.
STEP 2: Upgrade SF Sybase CE.
See “Step 2: Upgrading the first half of the cluster” on page 167.</td><td>The second half of the cluster is up and running.
</td></tr>
<tr><td>The first half of the cluster is not running.
</td><td>STEP 3: Perform the following pre-upgrade steps:
Stop all parallel and failover applications.
Stop SF Sybase CE.
See “Step 3: Performing pre-upgrade tasks on the second half of the cluster” on page 168.
The downtime starts now.</td></tr>
</table>

Table 12-1 Summary of phased upgrade *(continued)*

<table>
<tr><th>First half of the cluster</th><th>Second half of the cluster</th></tr>
<tr><td>

STEP 4: Perform the following post-upgrade steps:

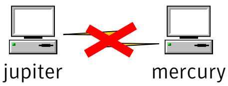
- Start SF Sybase CE.
- Start all applications.

See “Step 4: Performing post-upgrade tasks on the first half of the cluster” on page 169.

The downtime ends here.

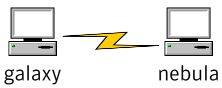
</td><td>

The second half of the cluster is not running.



</td></tr>
<tr><td>

The first half of the cluster is up and running.



</td><td>

STEP 5: Upgrade SF Sybase CE.

See “Step 5: Upgrading the second half of the cluster” on page 170.

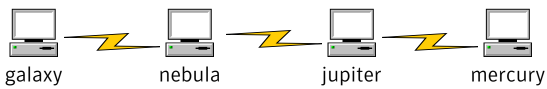
STEP 6: Perform the following post-upgrade steps:

- Start SF Sybase CE.
- Start all applications.

See “Step 6: Performing post-upgrade tasks on the second half of the cluster” on page 171.

</td></tr>
<tr><td colspan="2">

The phased upgrade is complete and both the first and the second half of the cluster are running.



</td></tr>
</table>

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

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

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

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

   For example:

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

2. Stop all applications that are not configured under VCS but dependent on Sybase ASE CE or resources controlled by VCS. Use native application commands to stop the application.

3. Stop the applications configured under VCS. Take the Sybase database group offline.

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

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

   ```
   # haconf -makerw
   # hagrp -modify sybasece AutoStart 0
   # haconf -dump -makero
   ```

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

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

     ```
     # mount | grep vxfs
     ```

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

   - Unmount the non-system VxFS or CFS file system:

     ```
     # umount /mount_point
     ```

6 Stop any open volumes that are not managed by VCS.

7 Stop the parallel service groups and switch over failover service groups:

```
# hastop -local
```

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

```
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

Use the `modinfo` command to check for loaded Veritas kernel modules and unload the modules, if any.

Step 2: Upgrading the first half of the cluster

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

To upgrade the first half of the cluster

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

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

2 Upgrade the operating system, if required.

For instructions, see the operating system documentation.

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

```
# shutdown -g0 -y -i6
```

You may see some errors in the system log file when the nodes restart. This is because LLT is disabled. Ignore these messages.

```
svc.startd[7]: [ID 652011 daemon.warning] svc:/system/llt:default:
Method "/lib/svc/method/llt start" failed with exit status 2.
gab: [ID 438192 kern.notice] GAB WARNING V-15-1-20115
Port d registration failed, GAB not configured
```

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

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

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

6 Upgrade SF Sybase CE. Navigate to the product directory on the installation media. When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```
# cd /dvd_mount/storage_foundation_for_sybase_ce
```

```
# ./installsfsybasece -upgrade galaxy nebula
```

Note: After you complete the upgrade of the first half of the cluster, no GAB ports will be shown in the output when you run the `gabconfig -a` command.

---

7 Change the `/etc/default/llt` file to prevent LLT from starting automatically after reboot by setting the LLT_START attribute to 0:

```
LLT_START=0
```

8 Restart the nodes:

```
# shutdown -g0 -y -i6
```

You may see some errors in the system log file when the nodes restart. This is because LLT is disabled. Ignore these messages.

```
svc.startd[7]: [ID 652011 daemon.warning] svc:/system/llt:default:
Method "/lib/svc/method/llt start" failed with exit status 2.
gab: [ID 438192 kern.notice] GAB WARNING V-15-1-20115
Port d registration failed, GAB not configured
```

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

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

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

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

Note: The downtime starts now.

2 Unmount the VxFS or CFS file systems that are not managed by VCS.

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

```
# mount | grep vxfs
```

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

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

3 Stop any open volumes that are not managed by VCS.

4 Stop VCS:

```
# hastop -local
```

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

```
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

Use the `modinfo` command to check for loaded Veritas kernel modules and unload the modules, if any.

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

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

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

1. Change `/etc/default/llt` to start LLT on the nodes by setting the LLT_START attribute to 1:

   Run the following command to bring LLT online, if it is in maintenance mode:

   ```
   # svcadm clear llt
   ```

   ```
   LLT_START=1
   ```

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

   ```
   # gabconfig -x
   ```

3. On the first half of the cluster, start SF Sybase CE:

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

   ```
   # ./installsfsybasece -start galaxy nebula
   ```

   Verify that the GAB ports a, b, and h appear in the `gabconfig -a` command output.

4. On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.

5. Bring the sybasece group online.

   ```
   # hagrp -online sybasece -sys node_name
   ```

   Note: The downtime ends here.

   ---

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

Step 5: Upgrading the second half of the cluster

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

To upgrade the second half of the cluster

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

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

2. Upgrade the operating system, if required.

   For instructions, see the operating system documentation.

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

   ```
   # shutdown -g0 -y -i6
   ```

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

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

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

6. On the second half of the cluster, upgrade SF Sybase CE. Navigate to the product directory on the installation media.

   Invoke the SF Sybase CE installer with the `- upgrade` option. The installer upgrades the second half of the cluster.

   ```
   # cd /dvd_mount/storage_foundation_for_sybase_ce
   ```

   ```
   # ./installsfsybasece -upgrade jupiter mercury
   ```

7. Restart the nodes:

   ```
   # shutdown -g0 -y -i6
   ```

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

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

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

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

2. Upgrade VxVM disk group version.

   See "Upgrading CVM protocol version and VxVM disk group version " on page 189.

3 Upgrade disk layout version.

See "Upgrading disk layout versions" on page 189.

4 Bring the sybasece group online.

```
# hagrp -online sybasece_group -sys node_name
```

5 If the Sybase database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrp -modify sybasece AutoStart 1
# haconf -dump -makero
```

6 Set or change the product license level, if required.

See "Setting or changing the product license level" on page 188.

Note: In case of Sybase ASE CE version prior to 15.5 ASE CE, upgrade the database to 15.5 ASE CE or 15.5 ASE CE latest ESD, after upgrading the cluster.

See "Upgrading Sybase ASE CE" on page 213.

Chapter 13

Upgrading to SF Sybase CE 6.0 using Live Upgrade

This chapter includes the following topics:

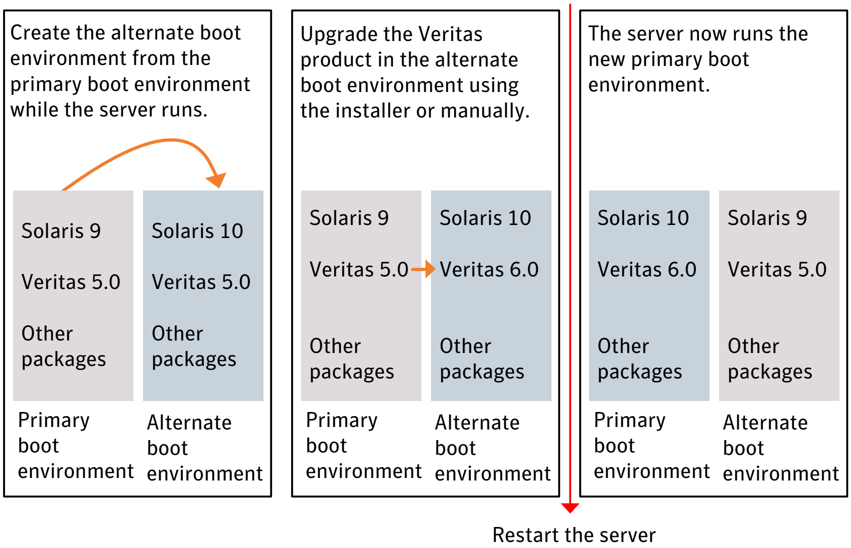
About Live Upgrade

You can use Live Upgrade to perform the following types of upgrade:

- Upgrade the operating system and SF Sybase CE.
- Upgrade the operating system.
- Upgrade SF Sybase CE.

Figure 13-1 illustrates an example of an upgrade of Veritas products from 5.0 to 6.0, and the operating system from Solaris 9 to Solaris 10.

Figure 13-1 Live Upgrade process



Some service groups (failover and parallel) may be online in this cluster and they are not affected by the Live Upgrade process. The only downtime experienced is when the server is rebooted to boot into the alternate boot disk.

Supported upgrade paths for Live Upgrade

The systems where you plan to use Live Upgrade must run Solaris 9 or Solaris 10. You can upgrade from systems that run Solaris 9, but SF Sybase CE 6.0 is not supported on Solaris 9.

SF Sybase CE version must be at least 5.0.

Before you upgrade SF Sybase CE using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1. Make sure that the SF Sybase CE installation media and the operating system installation images are available and on hand.
2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.

   If the primary boot disk is mirrored, you need to break off the mirror for the alternate boot disk.
3. On the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
4. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.

   Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at /*cdrom*/*solaris_release*/Tools/Installers/liveupgrade20. If scripting, you can use:

   ```
   # /cdrom/solaris_release/Tools/Installers/liveupgrade20 \
   -nodisplay -noconsole
   ```

5 Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot disk for the upgrade.

To preview the commands, specify the `vxlustart` script with the `-V` option.

Symantec recommends that you preview the commands to ensure there are no problems before beginning the Live Upgrade process.

The `vxlustart` script is located on the distribution media, in the scripts directory.

```
# cd /cdrom/scripts
```

```
# ./vxlustart -V -u targetos_version -s osimage_path -d diskname
```

-V	Lists the commands to be executed during the upgrade process without executing them and pre-checks the validity of the command. If the operating system is being upgraded, the user will be prompted to compare the patches that are installed on the image with the patches installed on the primary boot disk to determine if any critical patches are missing from the new operating system image.
-u	Specifies the operating system version for the upgrade on the alternate boot disk. For example, use `5.10` for Solaris 10.
-U	Specifies that only the Storage Foundation products are upgraded. The operating system is cloned from the primary boot disk.
-s	Indicates the path of the operating system image to be installed on the alternate boot disk. If this option is omitted, you are prompted to insert the discs that contain the operating system image. If the `-U` option is specified, you can omit the **-s** option. The operating system is cloned from the primary boot disk.
-d	Indicates the name of the alternate boot disk on which you intend to upgrade. If you do not specify this option with the script, you are prompted for the disk information.
-v	Indicates verbose, the executing commands display before they run.
-Y	Indicates a default yes with no questions asked.
-D	Prints with debug option on, and is for debugging.
-F	Specifies the rootdisk's file system, where the default is `ufs`.
-t	Specifies the number of CDs involved in upgrade.

-r	Specifies that if the machine crashes or reboots before the `vxlufinish` command is run, the alternate disk is remounted using this option.

For example, to preview the commands to upgrade only the Veritas product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0
```

Note: This command prompts you to compare the patches that are installed on the image with the patches installed on the primary boot disk. If any patches are missing from the new operating system's image, note the patch numbers. To ensure the alternate boot disk is the same as the primary boot disk, you will need to install these patches on the alternate boot disk.

---

6 If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

In the procedure examples, the primary or current boot environment resides on Disk0 (c0t0d0) and the alternate or inactive boot environment resides on Disk1 (c0t1d0).

Upgrading the operating system and SF Sybase CE using Live Upgrade

Perform the following steps to upgrade both the operating system and SF Sybase CE using Live Upgrade.

To upgrade the operating system and SF Sybase CE using Live Upgrade

1 Prepare to upgrade using Solaris Live Upgrade.

See "Before you upgrade SF Sybase CE using Solaris Live Upgrade" on page 174.

2 Create a new boot environment on the alternate boot disk.

See "Creating a new boot environment on the alternate boot disk" on page 179.

3 Upgrade SF Sybase CE using the installer or manually.

See "Upgrading SF Sybase CE using the installer for a Live Upgrade" on page 181.

4 Complete the Live Upgrade.

See "Completing the Live Upgrade" on page 182.

5 Verify Live Upgrade of SF Sybase CE.

See "Verifying Live Upgrade of SF Sybase CE" on page 185.

Upgrading SF Sybase CE only using Live Upgrade

Perform the following steps to upgrade only SF Sybase CE using Live Upgrade.

To upgrade only SF Sybase CE using Live Upgrade

1 Prepare to upgrade using Solaris Live Upgrade.

See "Before you upgrade SF Sybase CE using Solaris Live Upgrade" on page 174.

2 Create a new boot environment on the alternate boot disk.

See "Creating a new boot environment on the alternate boot disk" on page 179.

3 Upgrade SF Sybase CE using the installer or manually.

See "Upgrading SF Sybase CE using the installer for a Live Upgrade" on page 181.

4 Complete the Live Upgrade.

See "Completing the Live Upgrade" on page 182.

5 Verify Live Upgrade of SF Sybase CE.

See "Verifying Live Upgrade of SF Sybase CE" on page 185.

Upgrading Solaris only using Live Upgrade

Perform the following steps to upgrade only Solaris using Live Upgrade.

To upgrade only Solaris using Live Upgrade

1 Prepare to upgrade using Solaris Live Upgrade.

See "Before you upgrade SF Sybase CE using Solaris Live Upgrade" on page 174.

2 Create a new boot environment on the alternate boot disk.

See "Creating a new boot environment on the alternate boot disk" on page 179.

3 Complete the Live Upgrade.

See "Completing the Live Upgrade" on page 182.

4 Verify Live Upgrade of SF Sybase CE.

See "Verifying Live Upgrade of SF Sybase CE" on page 185.

Creating a new boot environment on the alternate boot disk

Run the `vxlustart` command on each node in the cluster to create a new boot environment on the alternate boot disk.

Note: This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

To create a new boot environment on the alternate boot disk

Perform the steps in this procedure on each node in the cluster.

1 Navigate to the install media for the Symantec products:

```
# cd /dvd_mount/scripts
```

2 View the list of VxVM disks on which you want to create the new boot environment.

```
# vxdisk list
```

3 Before you upgrade, make sure that you exclude the CFS mount points that are used by the database or applications from being copied to the new boot environment. During Live Upgrade, the `vxlustart` utility fails to recognize the CFS mount points that are configured under VCS. As a result, the data in Sybase and the mount points for Sybase ASE CE binaries, data files, and quorum that are configured as CFS mount points under VCS get copied into the local file system of the alternate boot environment. To prevent these shared mount points from being copied to the new boot environment, you need to identify and exclude these mount points as follows:

```
# for i in `hatype -resources CFSMount`; \
do hares -display $i -attribute MountPoint | awk ' \
NR != 1 { print "-", $4}'; done > /var/tmp/file_list
# cat /var/tmp/file_list
- /sybase_binary
- /masterdb
- /sysprocdb
- /db
```

Where */var/tmp/file_list* is a temporary file that contains the list of CFS mount points to be excluded from the new boot environment and */sybase_binary, /masterdb, /sysprocdb, and /db* are CFS mount points that are used by the database or applications. The items in the file list are preceded either by a + or - symbol. The + symbol indicates that the mount point is included in the new boot environment and the - symbol indicates that the mount point is excluded from the new boot environment. Apart from CFS mount points, you may choose to include or exclude other files.

4 Run one of the following commands to perform the upgrade:

For example:

```
# /vxlustart -v -u 5.10 -s /mnt/sol10u9 -d c0t1d0s2 \
-z /var/tmp/file_list
```

where */mnt/sol10u9* is the path to the operating system image that contains the `.cdtoc` file.

5 Create the mount points manually on the alternate boot environment as follows:

```
# for i in `cat /tmp/sfsybcemnt` ; \
do mkdir -p /altroot.5.10/$i; done
```

6. Update the permissions, user name, and group name of the mount points (created on the ABE) to match that of the existing directories on the primary boot environment.
7. Review the output and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

   If you need to remount, run the command:

   ```
   # vxlustart -r -u targetos_version -d disk_name
   ```

8. After the alternate boot disk is created and mounted on */altroot.5.10*, install any operating system patches or packages on the alternate boot disk that are required for the Veritas product installation:

   ```
   # pkgadd -R /altroot.5.10 -d pkg_dir
   ```

Upgrading SF Sybase CE using the installer for a Live Upgrade

You can use the Veritas product installer to upgrade SF Sybase CE as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade SF Sybase CE on all the nodes in the cluster. The program uninstalls the existing version of SF Sybase CE on the alternate boot disk during the process.

At the end of the process the following occurs:

- SF Sybase CE 6.0 is installed on the alternate boot disk.

To perform Live Upgrade of SF Sybase CE using the installer

1. Insert the product disc with SF Sybase CE 6.0 or access your copy of the software on the network.
2. Run the installer script specifying the root path as the alternate boot disk:

   ```
   # ./installer -upgrade -rootpath /altroot.5.10
   ```

3. Enter the names of the nodes that you want to upgrade to SF Sybase CE 6.0.

   The installer displays the list of packages to be installed or upgraded on the nodes.

4. Press **Return** to continue with the installation.
5. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.

   ```
   # pkginfo -R /altroot.5.10 -l VRTSpkgname
   ```

   For example:

   Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

Completing the Live Upgrade

At the end of the process:

- If the original primary boot disk was encapsulated, the alternate boot disk is encapsulated.
- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.

When completing the Live Upgrade process, take the following limitations into consideration for Solaris 10 Update 10:

- In a shared disk group environment, extra CFS mount entries are ignored when the `vxlustart` command is run, as they are included in `/etc/vfstab`. The entries must be manually removed before booting from the alternate boot environment.
- On Sparc, Live Upgrade from Solaris 9 to Solaris 10 Update 10 may fail using the `lucreate` command.

See the *Veritas Storage Foundation for Sybase ASE CE Release notes* for more details.

To complete the Live Upgrade

1. Complete the Live Upgrade process using one of the following commands:

   If the primary root disk is not encapsulated, run the following command:

   ```
   # ./vxlufinish -u target_os_version
   Live Upgrade finish on the Solaris release <5.10>
   ```

   If the primary root disk is encapsulated by VxVM, run the following command:

   ```
   # ./vxlufinish -u target_os_version -g diskgroup
   Live Upgrade finish on the Solaris release <5.10>
   ```

   The Live Upgrade process encapsulates the alternate root disk if the primary root disk was encapsulated.

2. If the system crashes or reboots before Live Upgrade completes successfully, you may remount the alternate disk using the following command:

   ```
   # ./vxlustart -r -u target_os_version
   ```

   Then, rerun the `vxlufinish` command:

   ```
   # ./vxlufinish -u target_os_version
   ```

3. If the Sybase database is managed by VCS, modify the VCS configuration file on the alternate root disk (`/altroot.5.10/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 0. This prevents the database service group from starting automatically when VCS starts:

   ```
   group sybasece (
           SystemList = { galaxy = 0, nebula = 1 }
           AutoStart = 0
           AutoFailOver = 0
           Parallel = 1
           AutoStartList = { galaxy, nebula }
           )
   .
   .
   ```

4. Perform the following steps on the primary boot environment:

   - Stop the applications using native application commands.
   - Make sure that no processes are running which make use of mounted shared file system or shared volumes.

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

- Take offline all sybase binary groups (binmnt) and sybase database groups (sybasece) that contain CFSMount and CVMVolDg:

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

- Unmount the VxFS file systems:

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

- Deport CVM disk groups:

  ```
  # vxdg deport diskgroup_name
  ```

- Make sure that no disk groups are imported:

  ```
  # vxdg list
  NAME STATE ID
  ```

5 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

Note: DO NOT use the reboot, halt, or uadmin commands to reboot the system. Use either the init or the shutdown commands to enable the system to boot using the alternate boot environment.

```
# shutdown -g0 -y -i6
```

6 Start the database group on all nodes:

```
# hagrp -online sybasece -any
```

7 If the Sybase database is managed by VCS, modify the VCS configuration file (`/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 1.

```
group sybasece (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoStart = 1
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )
.
.
```

8 Complete the post-upgrade tasks.

See the chapter "Performing post-upgrade tasks" in this document.

9 If you are on an unsupported version of Sybase ASE CE, upgrade to ASE CE 15.5.

See "Upgrading Sybase ASE CE" on page 213.

Verifying Live Upgrade of SF Sybase CE

To ensure that Live Upgrade has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

To verify that Live Upgrade completed successfully

1. Verify that the alternate boot environment is active.

   ```
   # lustatus
   ```

   If the alternate boot environment is not active, you can revert to the primary boot environment.

   See "Reverting to the primary boot environment" on page 186.

2. In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

   ```
   # gabconfig -a
   Port a gen   d77c08 membership 0123
   Port b gen   d77c0a membership 0123
   Port f gen   d77c2d membership 0123
   Port h gen   d77c3d membership 0123
   Port u gen   d77c2f membership 0123
   Port v gen   d77c28 membership 0123
   Port w gen   d77c2a membership 0123
   Port y gen   d77c26 membership 0123
   ```

3. Perform other verification as required to ensure that the new boot environment is configured correctly.

Reverting to the primary boot environment

If the alternate boot environment fails to start, you can revert to the primary boot environment.

On each node, start the system from the primary boot environment in the PROM monitor mode.

```
ok> boot disk0
```

where *disk0* is the primary boot disk.

Chapter 14

Performing post-upgrade tasks

This chapter includes the following topics:

Re-joining the backup boot disk group into the current disk group

Perform this procedure to rejoin the backup boot disk if you split the mirrored boot disk during upgrade. After a successful upgrade and reboot, you no longer need to keep the boot disk group backup.

To re-join the backup boot disk group

◆ Re-join the *backup_bootdg* disk group to the boot disk group.

```
# /etc/vx/bin/vxrootadm -Y join backup_bootdg
```

where the `-Y` option indicates a silent operation, and *backup_bootdg* is the name of the backup boot disk group that you created during the upgrade.

Reverting to the backup boot disk group after an unsuccessful upgrade

Perform this procedure if your upgrade was unsuccessful and you split the mirrored boot disk to back it up during upgrade. You can revert to the backup that you created when you upgraded.

To revert the backup boot disk group after an unsuccessful upgrade

1 To determine the boot disk groups, look for the *rootvol* volume in the output of the `vxprint` command.

```
# vxprint
```

2 Use the `vxdg` command to find the boot disk group where you are currently booted.

```
# vxdg bootdg
```

3 Boot the operating system from the backup boot disk group.

4 Join the original boot disk group to the backup disk group.

```
# /etc/vx/bin/vxrootadm -Y join original_bootdg
```

where the `-Y` option indicates a silent operation, and *original_bootdg* is the boot disk group that you no longer need.

Setting or changing the product license level

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

After you upgrade, perform one of the following steps:

- Obtain a valid license key and run the `vxlicinst` command to add it to your system.
- Use the `vxkeyless` command to update the license keys to the keyless license model.

For more information and instructions, see the chapter *Licensing SF Sybase CE*.

Upgrading disk layout versions

In this release, you can create and mount only file systems with disk layout Version 7, 8, and 9. You can only local mount disk layout Version 6 only to upgrade to a later disk layout version.

Disk layout Version 6 has been deprecated and you cannot cluster mount an existing file system that has disk layout Version 6. To upgrade a cluster file system with disk layout Version 6, you must local mount the file system and then upgrade the file system using the `vxupgrade` utility to a later version.

See the `vxupgrade`(1M) manual page.

Support for disk layout Version 4 and 5 has been removed. You must upgrade any existing file systems with disk layout Version 4 or 5 to disk layout Version 7 or later using the `vxfsconvert` command.

See the `vxfsconvert`(1M) manual page.

Note: Symantec recommends that you upgrade existing file systems to the highest supported disk layout version prior to upgrading to this release.

You can check which disk layout version your file system has by using the following command:

```
# fstyp -v /dev/vx/dsk/dg1/vol1 | grep -i version
```

For more information about disk layout versions, see the *Veritas Storage Foundation Administrator's Guide*.

Upgrading CVM protocol version and VxVM disk group version

The default Cluster Volume Manager protocol version is 110.

Run the following command to verify the CVM protocol version:

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

If the protocol version is not 110, run the following command to upgrade the version:

```
# /opt/VRTS/bin/vxdctl upgrade
```

All Veritas Volume Manager disk groups have an associated version number. Each VxVM release supports a specific set of disk group versions and can import and perform tasks on disk groups with those versions. Some new features and tasks work only on disk groups with the current disk group version. Before you can perform the tasks, you need to upgrade existing disk group version to 170.

Check the existing disk group version:

```
# vxdg list dg_name|grep -i version
```

If the disk group version is not 170, run the following command on the master node to upgrade the version:

```
# vxdg -T 170 upgrade dg_name
```

Verifying the cluster

After completing the upgrade procedure, you must perform the following checks on each node of the cluster.

To verify the cluster

1 Verify that all ports are up on the cluster.

```
# gabconfig -a
GAB Port Memberships
========================================================
Port a gen   8ea203 membership 0123
Port b gen   8ea206 membership 0123
Port f gen   8ea21f membership 0123
Port h gen   8ea216 membership 0123
Port u gen   8ea21d membership 0123
Port v gen   8ea219 membership 0123
Port w gen   8ea21b membership 0123
Port y gen   8ea218 membership 0123
```

2 Verify all service groups and resources are online.

```
# hagrp -state

hagrp -state
#Group        Attribute             System     Value
binmnt        State                 vcssx005   |ONLINE|
binmnt        State                 vcssx012   |ONLINE|
binmnt        State                 vcssx013   |ONLINE|
binmnt        State                 vcssx014   |ONLINE|
cvm           State                 vcssx005   |ONLINE|
cvm           State                 vcssx012   |ONLINE|
cvm           State                 vcssx013   |ONLINE|
cvm           State                 vcssx014   |ONLINE|
sybasece      State                 vcssx005   |ONLINE|
sybasece      State                 vcssx012   |ONLINE|
sybasece      State                 vcssx013   |ONLINE|
sybasece      State                 vcssx014   |ONLINE|
```

Section 4

Installation and upgrade of Sybase ASE CE

Chapter 15

Installing, configuring, and upgrading Sybase ASE CE

This chapter includes the following topics:

Before installing Sybase ASE CE

Before you install Sybase ASE CE, make sure that you perform the following tasks:

- Install SF Sybase CE
- Configure SF Sybase CE
- Set I/O fencing to Sybase mode

The high level flow for installing Sybase ASE CE in an SF Sybase CE environment:

- Create the Sybase user and groups. See Sybase ASE CE documentation.

- Create local or shared disk group, volume, and mount point for Sybase binary installation
- Install Sybase ASE CE
- Create a disk group, volume, and mount point for the Sybase quorum device
- Create a disk group, volume, and mount point for the Sybase datafiles
- Create the Sybase ASE CE cluster
- Configure Sybase ASE CE instances under VCS control

Preparing for local mount point on VxFS for Sybase ASE CE binary installation

The following procedure provides instructions for setting up the disk groups, volume, and mount point for installing Sybase ASE CE binaries for local mount point on VxFS.

To create the disk group, volume and mount point for Sybase binaries

1 Initialize the disk.

For example:

```
# vxdisksetup -i Disk_1 format=cdsdisk
```

2 Create a diskgroup.

For example:

```
# vxdg init sybbindg_101 Disk_1 Disk_2
```

3 Create a mirrored volume in the group:

```
# vxassist -g sybbindg_101 make sybbinvol
12G layout=mirrored nmirrors=2
```

4 Create a VxFS file system on which to install the Sybase binaries:

```
# mkfs -F vxfs /dev/vx/rdsk/sybbindg_101/sybbinvol
```

For a binary installation on a local file system, run the command on each node.

5 Create the sybase home ($SYBASE) directory on the node:

```
# mkdir /sybase
```

6 Mount the directory:

```
# mount -F vxfs /dev/vx/dsk/sybbindg_101/sybbinvol /sybase
```

7 Repeat the above steps on all other cluster nodes.

8 On each system, change permission of the directory to sybase.

```
# chown -R sybase:sybase /sybase
```

Preparing for shared mount point on CFS for Sybase ASE CE binary installation

The following procedure provides instructions for setting up the disk groups, volume, and mount point for installing Sybase ASE CE binaries for shared mount point on CFS.

To create the disk group, volume and mount point for Sybase binaries

1 Initialize the disk.

For example:

```
# vxdisksetup -i Disk_1 format=cdsdisk
```

2 Create a CVM diskgroup.

For example:

```
# vxdg -s init sybbindg_101 Disk_1 Disk_2
```

3 Create a mirrored volume in the group:

```
# vxassist -g sybbindg_101 make sybbinvol
12G layout=mirrored nmirrors=2
```

4 Create a VxFS file system on which to install the Sybase binaries:

```
# mkfs -F vxfs -o largefiles /dev/vx/rdsk/sybbindg_101/sybbinvol
```

For a binary installation on a shared file system, you may run the command on any one node.

5 Create a Sybase ASE CEhome directory ($SYBASE) on all nodes:

```
# mkdir /sybase
```

6 Mount the directory:

```
# mount -F vxfs -o cluster /dev/vx/dsk/sybbindg_101/sybbinvol /sybase
```

7 On each system, change permission of the directory to sybase.

```
# chown -R sybase:sybase /sybase
```

Installing Sybase ASE CE software

For information on installing Sybase ASE CE software, see the Sybase ASE CE product documentation.

Requirements for the Sybase ASE CE configuration:

- Use the CFS mount points you created in the previous section for installing the binaries
  See "To create the disk group, volume and mount point for Sybase binaries" on page 197.

Preparing to create a Sybase ASE CE cluster

The following procedure provides instructions for creating a file system for the quorum device.

To create the disk group, volume and mount point for a quorum device

1 Initalize the disk.

For exampe:

```
# vxdisksetup -i Disk_3 format=cdsdisk
# vxdisksetup -i Disk_4 format=cdsdisk
```

2 As root user, from the CVM master, create a shared VxVM diskgroup for the quorum device.

```
# vxdg -s init quorum_101 Disk_3 Disk_4
```

3 As root user, from the CVM master, create a mirrored volume, *quorumvol*:

```
# vxassist -g quorum_101 make quorumvol
1G layout=mirrored \
nmirrors=2
```

4 As root user, from the CVM master, create a filesystem with the volume,*quorumvol*.

```
# mkfs -F vxfs /dev/vx/rdsk/quorum_101/quorumvol
```

5 On each system, create a directory, /*quorum*:

```
# mkdir /quorum
```

6 On each system, mount /*quorum*

```
# mount -F vxfs -o cluster /dev/vx/dsk/quorum_101/quorumvol
/quorum
```

7 As root user, from any system, change permissions on /*quorum*

```
# chown -R sybase:sybase /quorum
```

To create the disk group, volume and mount point for the datafiles

1 Initalize the disk.

For exampe:

```
# vxdisksetup -i Disk_5 format=cdsdisk
# vxdisksetup -i Disk_6 format=cdsdisk
```

2 As root user, create a shared VxVM diskgroup for the datafiles.

```
# vxdg -s init sybdata_101 Disk_5 Disk_6
```

3 As root user, create a mirrored volume, *sybvol*:

```
# vxassist -g sybdata_101 make sybvol 1G layout=mirrored \
nmirrors=2
```

4 As root user, create a filesystem with the volume,*sybvol*.

```
# mkfs -F vxfs /dev/vx/rdsk/sybdata_101/sybvol
```

5 On each system, create a directory, /*sybdata*:

```
# mkdir /sybdata
```

6 On each system, mount /*sybdata*

```
# mount -F vxfs -o cluster /dev/vx/dsk/sybdata_101/sybvol
/sybdata
```

7 As root user, from any system, change permissions on /*sybdata*

```
# chown -R sybase:sybase /sybdata
```

Creating the Sybase ASE CE cluster

For information on creating a Sybase ASE CE cluster, see the Sybase ASE CE product documentation. Follow the normal process.

Requirements for the Sybase ASE CE configuration:

- When you choose the private interconnect, set them on LLT links
- SF Sybase CE supports only one instance per node
- You can create a VCS cluster in local mode. Ignore the message "If you want to create a VCS cluster, specify "Shared" mode.", if it appears.
- Put the quorum device on the mount point created for the quorum device.
  See "To create the disk group, volume and mount point for a quorum device" on page 198.
- Put the datafiles on the mount point created in for the datafiles.
  See "To create the disk group, volume and mount point for the datafiles" on page 199.

Preparing to configure the Sybase instances under VCS control

Before putting the Sybase instances under VCS control, you may need to perform the following tasks:

- Language settings for the Sybase agent
- Configuring Sybase for detail monitoring
- Encrypting passwords for Sybase
- About setting up detail monitoring for the agentfor Sybase

Language settings for the Sybase agent

For the Veritas agent for Sybase to function with the desired locale, make sure that the Sybase installation has the correct localization files. For example, if the Sybase server requires 'LANG=en_US.UTF-8' environment variable, verify that the localization files corresponding to language 'en_US.UTF-8' are installed with Sybase.

Also, edit the file $VCS_HOME/bin/vcsenv to contain the following:

```
LANG=en_US.UTF-8;export LANG
```

This change affects all the agents that are configured on the nodes.

Configuring Sybase for detail monitoring

This section describes the tasks to be performed to configure a Sybase server for detail monitoring.

See "About setting up detail monitoring for the agentfor Sybase" on page 203.

Note: The steps that are described here are specific to the sample script, SqlTest.pl, provided with the agent. If you use a custom script for detail monitoring, you must configure the Sybase database accordingly.

Perform these steps only once in a Sybase cluster.

To configure Sybase for detail monitoring

1. Source the SYBASE.sh file or SYBASE.csh file (depending on the user shell) to set the $SYBASE and $SYBASE_ASE environment variables.
2. Start the Sybase server.

   ```
   # startserver -f ./$SYBASE/$SYBASE_ASE/install/RUN_server_name
   ```

3. Start the Sybase client on any cluster node.

   ```
   # isql -Usa -SSYBASE_SERVER_NAME
   ```

   Enter the administrator password when prompted to do so.
4. Connect to the master database.

   ```
   # use master
   # go
   ```

5 Create a Sybase user account.

```
# sp_addlogin user_name, password
# go
```

The detail monitor script should use this account to make transactions on the database.

6 Create a database.

```
# create database database_name
# go
```

The detail monitor script should make transactions on this database.

7 If required, restrict the size of the log file for the database.

```
# sp_dboption database_name, "trunc log on chkpt", true
# go
```

8 Connect to the database that is created in step 6.

```
# use database_name
# go
```

9 Associate the user created in step 5 with the database created in step 6.

```
# sp_adduser user_name
# go
```

10 Change the user to the one created in step 5.

```
# setuser user_name
# go
```

11 Create a table in the database.

```
# create table table_name (lastupd datetime)
# go
```

The detail monitor script should make transactions on this table.

If you use the SqlTest.pl for detail monitoring, make sure you create a table with a lastupd field of type datetime.

12 Verify the configuration by adding an initial value to the table.

```
# insert into table_name (lastupd) values (getdate())
# go
```

13 Exit the database.

```
# exit
```

Encrypting passwords for Sybase

VCS provides a vcsencrypt utility to encrypt user passwords. Encrypt passwords before specifying them for Sybase and SybaseBk resource type definition.

The vcsencrypt utility also allows you to encrypt the agent passwords using a security key. The security key supports AES (Advanced Encryption Standard) encryption which creates a more secure password for the agent. See the *Veritas Cluster Server Administrator's Guide* for more information.

To encrypt passwords

1 From the path $VCS_HOME/bin/, run the vcsencrypt utility.

2 Type the following command.

```
# vcsencrypt -agent
```

The utility prompts you to enter the password twice. Enter the password and press Return.

```
Enter Password:
Enter Again:
```

3 The utility encrypts the password and displays the encrypted password.

4 Enter this encrypted password as the value for the attribute.

Copy the encrypted password for future reference.

About setting up detail monitoring for the agentfor Sybase

The Veritas agent for Sybase provides two levels of application monitoring: basic and detail. In basic monitoring, Sybase resource monitors the Sybase daemon processes to verify that they are continuously active.

In detail monitoring, the Sybase resource performs transactions on a table (provided by the user) in the database to ensure that the Sybase server functions properly. The agent uses this table for internal purposes. Symantec recommends that you do not perform any other transaction on this table. The agent uses the script that is defined in the attribute Monscript of the Sybase resource. During detail monitoring, the agent executes the specified script. If the script successfully executes, the agent considers the database available. You can customize the default script according to your configurations.

To activate detail monitoring, the LevelTwoMonitorFreq attribute must be set to a positive integer and User, UPword, Db, and Table attributes must not be empty (""). The attribute Monscript, which contains the path of the detail monitor script, must also exist and must have execute permissions for the root.

Enabling detail monitoring for the agent for Sybase

Perform the following steps to enable detail monitoring on a database.

To enable detail monitoring

1 Make sure the Sybase server is configured for detail monitoring.

See "Configuring Sybase for detail monitoring" on page 201.

2 Make the VCS configuration writable.

```
# haconf -makerw
```

3 Enable detail monitoring for Sybase.

```
# hatype -modify Sybase LevelTwoMonitorFreq <value>
# hares -modify Sybase_resource User user_name
# hares -modify Sybase_resource UPword encrypted-password
# hares -modify Sybase_resource Db database_name
# hares -modify Sybase_resource Table table_name
# hares -modify Sybase_resource Monscript
"/opt/VRTSagents/ha/bin/Sybase/SqlTest.pl"
```

Note: To enable detail monitoring, the LevelTwoMonitorFreq attribute must be set to a positive value. You can also override the value of this attribute at the resource level.

4 Save the configuration.

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

Note: If detail monitoring is configured and the database is full, the SQL queries take considerable time to commit the results. In such a case, the monitor routine for the agent fails and attempts to fail over the service group. This issue is not encountered if detail monitoring is not configured.

Disabling detail monitoring for the agent for Sybase

1 Make the VCS configuration writable with:

```
# haconf -makerw
```

2 To disable detail monitoring for Sybase run the following command:

```
# hatype -modify Sybase LevelTwoMonitorFreq 0
```

3 Save the configuration with:

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

Configuring a Sybase ASE CE cluster under VCS control using the SF Sybase CE installer

A VCS service group is a collection of resources working together to provide application services to clients. A VCS service group typically includes multiple resources that are both hardware and software based. For example, a resource maybe a physical component such as a disk or network interface card, or a software component such as Sybase or a Web server, or a configuration component such as an IP address or mounted file system.

For an example configuration file:

See "Sample main.cf for a basic Sybase ASE CE cluster configuration under VCS control with shared mount point on CFS for Sybase binary installation" on page 378.

The SF Sybase CE installer enables you to configure VCS service groups for putting a basic Sybase ASE CE cluster under VCS control. For examples of the VCS service group dependencies for SF Sybase CE see the following diagrams.

Figure 15-1 displays the service group dependencies for an SF Sybase CE configuration on local disk group with VxFS.

Figure 15-1 Service group dependencies for an SF Sybase CE configuration on local disk group with VxFS

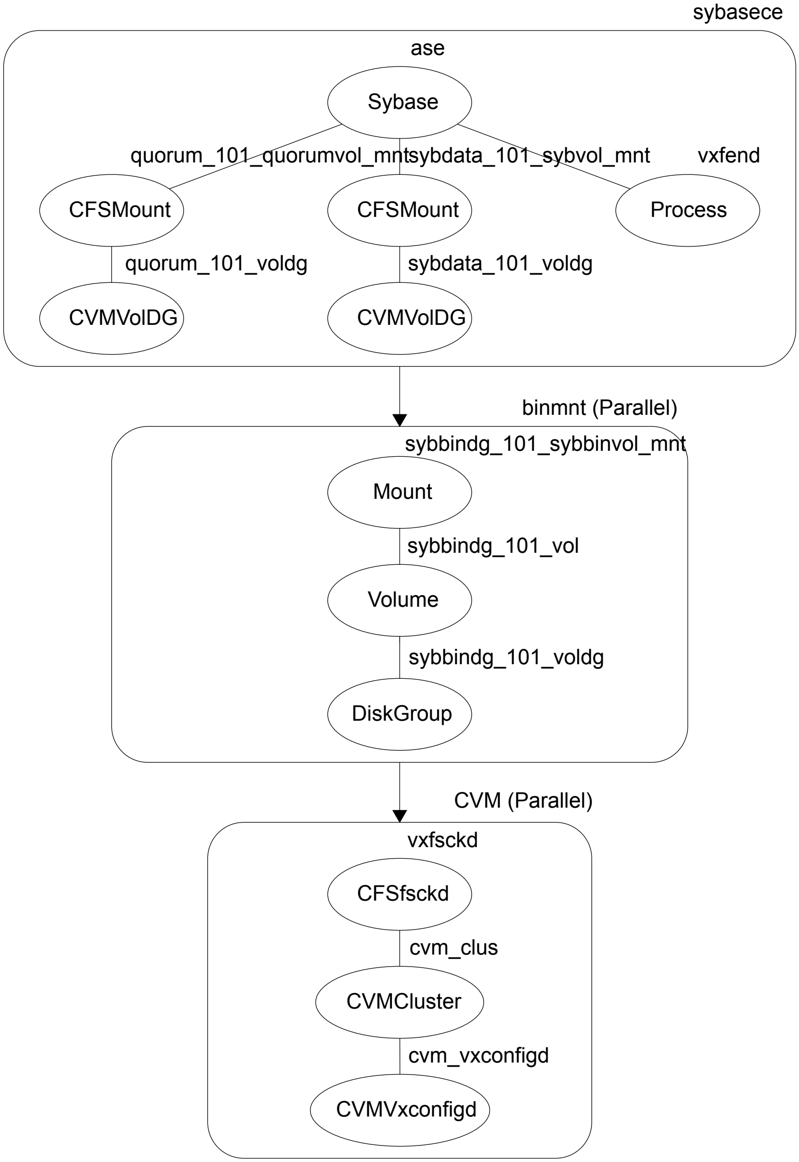
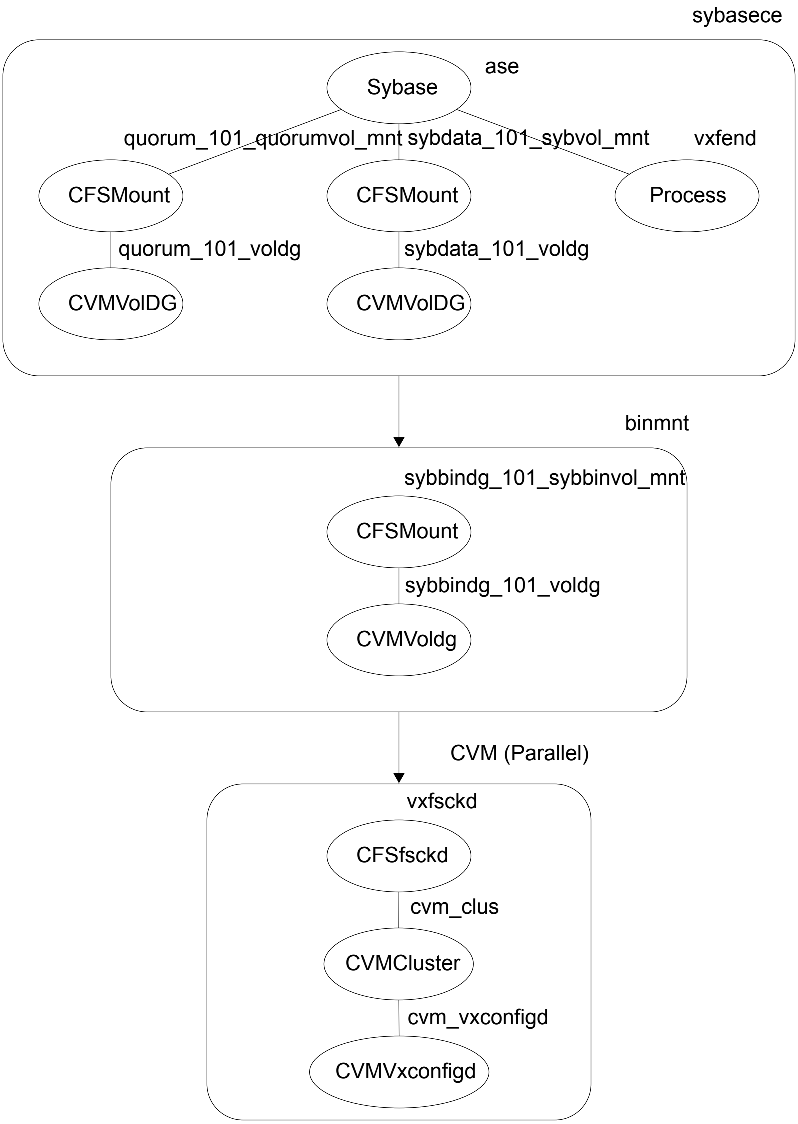


Figure 15-2 displays the service group dependencies for an SF Sybase CE configuration on shared disk group with CFS.

Figure 15-2 Service group dependencies for an SF Sybase CE configuration on shared disk group with CFS



Requirements for configuring the SF Sybase CE cluster under VCS control:

- Install SF Sybase CE.
- Configure SF Sybase CE.

- Configure I/O fencing in Sybase mode.
- Create Sybase user and group.
  See Sybase documentation.
- Create a local or shared disk group, volume, and mount point for Sybase binary installation.
- Install the Sybase ASE CE software
- Create a shared disk group, volume and mount point for the Sybase ASE CE quorum device
- Create a shared disk group, volume and mount point for the Sybase ASE CE datafiles
- Create the Sybase ASE CE cluster

To put the Sybase ASE CE cluster and its resources under VCS control, the installer's configuration process will add the required resources to appropriate VCS service groups.

Table 15-1 lists the required resources for configuring Sybase ASE CE under VCS control.

Table 15-1 Required resources for configuring Sybase ASE CE under VCS control

Required resources	Example values	
Resources for the Sybase ASE CE binary installation:	Example values for shared mount point:	Example values for local mount point:
■ Disk group ■ Mount point ■ Volume	■ *sybbindg_101* ■ */sybase* ■ *sybbinvol*	■ *sybbindg_101_voldg* ■ */sybase* ■ *sybbindg_101_vol*
Resources for the Sybase ASE CE quorum device:	Example values for shared mount point:	
■ Disk group ■ Mount point ■ Volume	■ *quorum_101* ■ */quorum* ■ *quorumvol*	
Resources for the Sybase ASE CE datafiles:	Example values for shared mount point:	
■ Disk group ■ Mount point ■ Volume	■ *sybdata_101* ■ */sybdata* ■ *sybvol*	

Table 15-1 Required resources for configuring Sybase ASE CE under VCS control *(continued)*

Required resources	Example values
Any other CFS disk group, mount point, and volume used for Sybase ASE CE resources that are required by the Sybase ASE CE cluster	As needed
The quorum device name	/quorum/quorum.dat

Warning: You will not be able to proceed using the installer to configure the Sybase ASE CE cluster under VCS control without the items listed in Table 15-1

To configure VCS service groups for Sybase ASE CE

1 Log in to the installer if you are not currently logged in.

See "Configuring the SF Sybase CE components using the script-based installer" on page 90.

2 When prompted to select an option from the main menu, choose the option: **Configure Sybase ASE CE Instance in VCS**.

The installer will not be able to proceed any further unless you have the required resources available.

See Table 15-1 on page 209.

3 To select the type of file system where Sybase ASE CE binaries reside, choose one of the options.

Symantec recommends CFS.

4 Configure the Sybase ASE CE binary installation resources under VCS control. These are the resources which were created while preparing to install Sybase ASE CE.

See "Preparing for shared mount point on CFS for Sybase ASE CE binary installation" on page 197. for shared mount point.

See "Preparing for local mount point on VxFS for Sybase ASE CE binary installation " on page 196. for local mount point.

To configure the Sybase resources under VCS control:

- To select a disk group used for Sybase ASE CE installation, choose one of the options.

Note: If you use Sybase ASE CE installation binaries on the local VxFS mount, you must specify the disk group for each node.

- To select the volume used for Sybase ASE CE installation, choose one of the options.
- Enter the mount point for the selected volume.

5 The quorum device resources must be added into the resource group if it is under a different CFS than the Sybase database installation. These resources were created while preparing for a Sybase ASE CE cluster.

See "Preparing to create a Sybase ASE CE cluster" on page 198.

To configure the quorum device under VCS control:

- Enter **y** if the quorum device is under a different CFS than the Sybase database resources you have configured in the previous step, otherwise enter **n**.
- If you entered **y**, select a disk group for the quorum device.
- Select a volume for the qourum device.
- Enter **y** if there is a CFS on the volume you selected, otherwise enter **n**. The quorum device can use either a volume which you have selected directly or a file under CFS created on the selected volume.
- Enter the mount point for the volume.

6 If there are any other disk groups, volumes, or mount points used for the Sybase ASE CE cluster, such as other database files, for instance master, system, etc., which are using a different CFS, they must also be put under VCS control.

To add other disk groups, volumes, and mount points to the resource group, enter **y** when prompted, otherwise enter **n**.

7 Verify the disk groups, volumes and mount points information when prompted.

8 To configure the Sybase ASE CE resources:

- Enter the Sybase instance on ASE1 and ASE2 when prompted.
- Enter the Sybase UNIX user name.
- Enter Sybase home directory, where the Sybase binaries reside.
- Enter Sybase version.

- If required, enter the username and password for the Admin user. The default username is 'sa', password is''.
- Enter the Sybase quorum device information.
  During configuration of Sybase instance under VCS control, if the quorum device is on CFS and is not mounted, the following warning message appears on the installer screen:

  ```
  Error: CPI WARNING V-9-0-0 The quorum file /quorum/quorum.dat
  cannot be accessed now, may be due to file system is not mounted.
  ```

  This message may be safely ignored. The resource will be onlined and available when the service is completed.
- Verify the Sybase configuration information by entering **y**, otherwise enter **n**. For example:

  ```
  Sybase configuration information verification:

          sybase Server on system1: ASE1
          sybase Server on system2: ASE2
          Sybase UNIX user name: sybase
          Sybase home directory where sybase binaries reside: /sybase
          Sybase version: 15
          sybase sa: sa
          Passwords are not displayed
          sybase quorum: /quorum/quorum.dat
  ```

  Once you confirm the information is correct, the installer configures and onlines the VCS service groups for Sybase ASE CE. This completes the configuration of Sybase ASE CE under VCS control.
- Note the location of the configuration log files for future reference.

9 To verify the service groups have been created and are available online, enter:

```
# hagrp -state
```

```
hagrp -state
#Group        Attribute              System     Value
binmnt        State                  system1     |ONLINE|
binmnt        State                  system2     |ONLINE|
cvm           State                  system1     |ONLINE|
cvm           State                  system2     |ONLINE|
sybasece      State                  system1     |ONLINE|
sybasece      State                  system2     |ONLINE|
```

Upgrading Sybase ASE CE

SF Sybase CE supports Sybase ASE CE 15.5 only at the time of publication.

For information on upgrading Sybase ASE CE software, see the Sybase ASE CE product documentation:

See infocenter.sybase.com.

Section 5

Installation of SF Sybase CE and Sybase ASE CE using a response file

Chapter 16

About reponse files

This chapter includes the following topics:

- About response files
- Response file syntax
- Guidelines for creating the SF Sybase CE response file
- Installation scenarios for response files

About response files

Use response files to standardize and automate installations on multiple clusters.

You can perform the following installation activities using a response file:

- Installing and configuring SF Sybase CE
- Uninstalling SF Sybase CE

Table 16-1 lists the various options available for creating or obtaining a response file.

Table 16-1 Options for obtaining a response file

Option	Description
Create a response file	Create a response file based on the sample response file. See "Sample response files for installing and configuring SF Sybase CE" on page 225.

Table 16-1 Options for obtaining a response file *(continued)*

Option	Description

Reuse or customize the response files generated by an installation	The response file generated by the installer is located in the following directory:
	`/opt/VRTS/install/logs/installsfsybasece-`*`installernumber`*`\`
	`/installsfsybasece-`*`installernumber`*`.response file`
	Note: Response files are not created if the tasks terminated abruptly or if you entered **q** to quit the installation. To generate the response file when you plan to discontinue a task, use the **Exit SF Sybase CE configuration** option.

Use the `-makeresponsefile` option with the SF Sybase CE installer	Create a response file by specifying the `-makeresponsefile` option with the SF Sybase CE installer. Mount the product disc and navigate to the folder that contains the installation program. Start the installation program. Use the `-makeresponsefile` option only to generate response files. No actual software installation occurs when you use this option. The response file is created in the directory `/opt/VRTS/install/logs/`. **Note:** You can use the `-makeresponsefile` option to create response files only for installing, configuring, or uninstalling SF Sybase CE. For more information: See "About the `-makeresponsefile` option" on page 219.

At the end of the SF Sybase CE installation, the following files are created:

- A log file that contains executed system commands and output.
- A summary file that contains the output of the installation scripts.
- Response files to be used with the -responsefile option of the installer.

Note: The SF Sybase CE response files also contain VCS variables used for the installation and configuration of VCS.

For the VCS variable definitions, see the *Veritas Cluster Server Installation Guide*.

About the `-makeresponsefile` option

The SF Sybase CE installer includes the option (`-makeresponsefile`) to generate sample response files that can be customized to perform installation, configuration, or uninstallation of the product.

Note: No actual installation, configuration, or uninstallation occurs when you use this option.

Use the option in the following situations:

- To understand the information that is required when you install, configure, or uninstall SF Sybase CE
- To create a response file
  The option creates a response file that can be used as a template for installing, configuring, or uninstalling SF Sybase CE. You can customize the response file, as required.

To generate the response file for installing and configuring the product, specify the `-makeresponsefile` option with the installer or product installation script at the command line.

To generate the response file for uninstalling the product, specify the `-makeresponsefile` option with the installer or the product uninstall script at the command line.

Response file syntax

The Perl statement syntax that is included in the response file varies, depending on whether “Scalar” or “List” values are required by the variables.

For example,

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

or, in the case of an integer value:

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

or, in the case of a list:

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

Guidelines for creating the SF Sybase CE response file

This section provides guidelines for creating the SF Sybase CE response file.

1. Create a response file using one of the available options.

   For various options on creating or obtaining an SF Sybase CE response file:

   See "About response files" on page 217.

2. Set the following master values to 1 to enable SF Sybase CE installation and configuration.

   Note: The master settings must be set to 1 to enable the installer to read dependent variable definitions. For example, if the value `$CFG{opt}{install}` is not set to 1, the other dependent installation values in the response file will be disregarded. This is true for any master setting.

   The following is the list of master values that must be set for installing and configuring SF Sybase CE.

Installing SF Sybase CE	`$CFG{opt}{install}=1;` `$CFG{opt}{installallpkgs}=1;`
Configuring SF Sybase CE	`$CFG{opt}{configure}=1;`

3. Now, set the appropriate value in the dependent variable definitions for installing and configuring SF Sybase CE.

   The set of minimum definitions for a successful installation and configuration is as follows:

```
$CFG{config_cfs}=1;
$CFG{fencingenabled}=0;
$CFG{lltoverudp}=0;
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{prod}="SFSYBASECE60";
$CFG{sfsybasece}{menu}=1;
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_allowcomms}=1;
```

```
$CFG{vcs_clusterid}=1720;
$CFG{vcs_clustername}="clus1720";
$CFG{vcs_lltlink1}{vcslx017}="bge2";
$CFG{vcs_lltlink1}{vcslx018}="bge2";
$CFG{vcs_lltlink1}{vcslx019}="bge2";
$CFG{vcs_lltlink1}{vcslx020}="bge2";
$CFG{vcs_lltlink2}{vcslx017}="bge3";
$CFG{vcs_lltlink2}{vcslx018}="bge3";
$CFG{vcs_lltlink2}{vcslx019}="bge3";
$CFG{vcs_lltlink2}{vcslx020}="bge3";
$CFG{vcs_userenpw}=[ qw(HIJbIDiFJeJJhRJdIG) ];
$CFG{vcs_username}=[ qw(admin) ];
$CFG{vcs_userpriv}=[ qw(Administrators) ];

1;
```

You can add more variable definitions, as required.

Installation scenarios for response files

The chapters in this section cover the following installation scenarios using response files:

- Installing and configuring SF Sybase CE
  See "Installing and configuring SF Sybase CE" on page 223.
- Configuring a SF Sybase CE instance in VCS
  See "Configuring a Sybase cluster under VCS control with a response file " on page 229.
- Configuring I/O fencing forSF Sybase CE with a response file

Chapter 17

Installing and configuring SF Sybase CE using a response file

This chapter includes the following topics:

Installing and configuring SF Sybase CE

You can create a single response file or separate response files for installing and configuring SF Sybase CE.

The installer performs the following tasks:

- Installs SF Sybase CE.
- Configures SF Sybase CE.

The following sample procedure uses a single response file for installing and configuring SF Sybase CE.

To install and configure SF Sybase CE using response files

1. Make sure that the systems meet the installation requirements.

   See "Hardware requirements" on page 34.

2. Complete the preparatory steps before starting the installation.

   For instructions, see the chapter "Preparing to install and configure SF Sybase CE" in this document.

3. Create a response file using one of the available options.

   For information on various options available for creating a response file:

   See "About response files" on page 217.

   Note: You must replace the host names in the response file with that of the new systems in the cluster.

   For guidelines on creating a response file:

   See "Guidelines for creating the SF Sybase CE response file" on page 220.

   For a sample response file:

   See "Sample response files for installing and configuring SF Sybase CE" on page 225.

   See "Sample response files for installing and configuring SF Sybase CE" on page 225.

4. Mount the product disc and navigate to the product directory that contains the installation program.

5. Start the installation and configuration:

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

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

6. Configure I/O fencing.

   Note: Before you configure I/O fencing, make sure that you complete the required pre-configuration tasks.

   For instructions on configuring I/O fencing using a response file, see the chapter *Configuring I/O fencing using a response file* in this document.

7. Complete the SF Sybase CE post-installation tasks.

   For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Sample response files for installing and configuring SF Sybase CE

The following sample response file installs and configures SF Sybase CE on two nodes, galaxy and nebula.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{config_cfs}=1;
$CFG{fencingenabled}=0;
$CFG{lltoverudp}=0;
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{opt}{vr}=1;
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SFSYBASECE60";
$CFG{sfsybasece}{menu}=1;
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=24731;
$CFG{vcs_clustername}="clus1720";
$CFG{vcs_lltlink1}{galaxy}="bge1";
$CFG{vcs_lltlink1}{nebula}="bge1";
$CFG{vcs_lltlink2}{galaxy}="bge2";
$CFG{vcs_lltlink2}{nebula}="bge2";
$CFG{vcs_userenpw}=[ qw(JqrJqlQnrMrrPzrLqo) ];
$CFG{vcs_username}=[ qw(admin) ];
$CFG{vcs_userpriv}=[ qw(Administrators) ];
```

The following sample response file only installs SF Sybase CE on two nodes, galaxy and nebula.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{opt}{vr}=1;
```

```
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="SFSYBASECE60";
$CFG{systems}=[ qw(galaxy nebula) ];

1;
```

The following sample response file only configures CFS on two nodes, galaxy and nebula.

```
our %CFG;

$CFG{config_cfs}=1;
$CFG{fencingenabled}=0;
$CFG{lltoverudp}=0;
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{prod}="SFSYBASECE60";
$CFG{sfsybasece}{menu}=1;
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=60037;
$CFG{vcs_clustername}="clus1720";
$CFG{vcs_lltlink1}{galaxy}="bge1";
$CFG{vcs_lltlink1}{nebula}="bge1";
$CFG{vcs_lltlink2}{galaxy}="bge2";
$CFG{vcs_lltlink2}{nebula}="bge2";
$CFG{vcs_userenpw}=[ qw(bMNfMHmJNiNNlVNhMK) ];
$CFG{vcs_username}=[ qw(admin) ];
$CFG{vcs_userpriv}=[ qw(Administrators) ];
```

Chapter 18

Configuring I/O fencing for SF Sybase CE using a response file

This chapter includes the following topics:

Configuring I/O fencing using response files

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

To configure I/O fencing using response files

1. Make sure that SF Sybase CE is configured.
2. Make sure you have completed the preparatory tasks.

   See "About planning to configure I/O fencing" on page 42.
3. Copy the response file to one of the cluster systems where you want to configure I/O fencing.

   See "Sample response file for configuring disk-based I/O fencing" on page 228.
4. Edit the values of the response file variables as necessary.

   See "Response file variables to configure disk-based I/O fencing" on page 243.

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

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

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

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

Review the disk-based I/O fencing response file variables and their definitions.

See "Response file variables to configure disk-based I/O fencing" on page 243.

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

$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="SFSFYBASE60";

$CFG{systems}=[ qw(system1 system2) ];
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="syb_cluster101";
$CFG{fencing_dgname}="fendg";
$CFG{fencing_scsi3_disk_policy}="dmp";
$CFG{fencing_newdg_disks}=
 [ qw(c1t1d0s2 c2t1d0s2 c3t1d0s2) ];
$CFG{fencing_option}=2;
```

Configuring a Sybase cluster under VCS control using a response file

This chapter includes the following topics:

Configuring a Sybase cluster under VCS control with a response file

Observe the following prerequisites prior to configuring a Sybase cluster under VCS with a response file:

- SF Sybase CE must be installed and configured on the system.
- Sybase must be installed.
- The Sybase cluster must already be created.

To configure a Sybase cluster under VCS using a response file

- Use the configuration response file to configure the product:

```
# installsfsybasece -responsefile /opt/VRTS/install/logs/\
installsfsybasece-installernumber/installsfsybasece-installer\
number.response
```

The following sample response file configures SF Sybase CE under VCS control.

```
our %CFG;
```

```
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{vr}=1;
$CFG{prod}="SFSYBASECE60";
$CFG{sfsybasece}{ase_home}="/opt/sybase";
$CFG{sfsybasece}{ase_owner}="sybase";
$CFG{sfsybasece}{ase_quorum}="/quorum";
$CFG{sfsybasece}{ase_sa}="sa";
$CFG{sfsybasece}{ase_server}{galaxy}{SERVER}="inst1";
$CFG{sfsybasece}{ase_server}{nebula}{SERVER}="inst2";
$CFG{sfsybasece}{ase_version}=15;
$CFG{sfsybasece}{menu}=3;
$CFG{sfsybasece}{storage_resource}{database_dontuse}{database01vol}{usage}=
"database devices";
$CFG{sfsybasece}{storage_resource}{master_dontuse}{mastervol}{usage}=
"database devices";
$CFG{sfsybasece}{storage_resource}{proc_dontuse}{proc01vol}{mount}="/mnt1";
$CFG{sfsybasece}{storage_resource}{proc_dontuse}{proc01vol}{usage}=
"database devices";
$CFG{sfsybasece}{storage_resource}{quorum_dontuse}{quorumvol}{usage}=
"quorum device";
$CFG{sfsybasece}{storage_resource}{sybase1_dontuse}{sybasevol}{mount}=
"/opt/sybase";
$CFG{sfsybasece}{storage_resource}{sybase1_dontuse}{sybasevol}{usage}=
"sybase installation";
$CFG{sybase_location}=1;
$CFG{systems}=[ qw(galaxy nebula) ];

1;
```

Chapter 20

Response file variable definitions

This chapter includes the following topics:

Response file variables for installing SF Sybase CE

Table 20-1 lists the response file variables that you can define to install SF Sybase CE.

Table 20-1 Response file variables for installing SF Sybase CE

Variable	List or Scalar	Description
CFG{opt}{install}	Scalar	Required Installs SF Sybase CE packages.
CFG{opt}{systems}	List	Required List of systems on which the product is to be installed.

Table 20-1 Response file variables for installing SF Sybase CE *(continued)*

Variable	List or Scalar	Description
CFG{opt}{installallpkgs} or CFG{opt}{installrecpkgs} or CFG{opt}{installminpkgs}	Scalar	Required Instructs the installer to install SF Sybase CE packages based on the variable that has the value set to 1: ■ installallpkgs: Installs all packages ■ installrecpkgs: Installs recommended packages ■ installminpkgs: Installs minimum packages **Note:** Set only one of these variable values to 1. In addition to setting the value of one of these variables, you must set the variable *$CFG{opt}{install}* to 1.
CFG{opt}{rsh}	Scalar	Optional Defines that remote shell must be used instead of secure shell as the communication method between systems.
CFG{opt}{gco}	Scalar	Optional Defines that the installer must enable the global cluster option. You must set this variable value to 1 if you want to configure global clusters.
CFG{opt}{keyfile}	Scalar	Optional Defines the location of an ssh keyfile that is used to communicate with all remote systems.
CFG{opt}{pkgpath}	Scalar	Optional Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems.

Table 20-1 Response file variables for installing SF Sybase CE *(continued)*

Variable	List or Scalar	Description
CFG{opt}{tmppath}	Scalar	Optional Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp.
CFG{opt}{logpath}	Scalar	Optional Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location.
CFG{opt}{donotinstall} {package}	List	Optional Instructs the installation to not install the optional packages in the list.
$CFG{opt}{vxkeyless}	Scalar	Optional Defines a Boolean value 0 or 1. The value 1 indicates keyless installation. The value 0 indicates that a license key is required for the product. You must set the variable *$CFG{keys}{hostname}* with appropriate values.
CFG{keys} {hostname}	Scalar	Optional List of keys to be registered on the system if the variable *$CFG{opt}{vxkeyless}* is set to 0.

Table 20-1 Response file variables for installing SF Sybase CE *(continued)*

Variable	List or Scalar	Description
$CFG{uploadlogs}	Scalar	Optional Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site.

Response file variables to configure Veritas Storage Foundation for Sybase ASE CE

Table 20-2 lists the response file variables that you can define to configure SF Sybase CE.

Table 20-2 Response file variables specific to configuring Veritas Storage Foundation for Sybase ASE CE

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the packages are already installed. (Required) Set the value to 1 to configure SF Sybase CE.
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{systems}	List	List of systems on which the product is to be configured. (Required)
CFG{prod}	Scalar	Defines the product to be configured. The value is VCS60 for VCS. (Required)

Table 20-2 Response file variables specific to configuring Veritas Storage Foundation for Sybase ASE CE *(continued)*

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

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (csgnic, csgvip, and csgnetmask) must be defined if any are defined. The same is true for the SMTP notification (smtpserver, smtprecp, and smtprsev), the SNMP trap notification (snmpport, snmpcons, and snmpcsev), and the Global Cluster Option (gconic, gcovip, and gconetmask).

Table 20-3 lists the response file variables that specify the required information to configure a basic SF Sybase CE cluster.

Table 20-3 Response file variables specific to configuring a basic SF Sybase CE cluster

Variable	List or Scalar	Description
CFG{vcs_clusterid}	Scalar	An integer between 0 and 65535 that uniquely identifies the cluster. (Required)
CFG{vcs_clustername}	Scalar	Defines the name of the cluster. (Required)
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)

Table 20-4 lists the response file variables that specify the required information to configure LLT over Ethernet.

Table 20-4 Response file variables specific to configuring private LLT over Ethernet

Variable	List or Scalar	Description
CFG{vcs_lltlink#} {"system"}	Scalar	Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (lltlink1 and lltlink2). You can configure up to four LLT links. You must enclose the system name within double quotes. (Required)

Table 20-4 Response file variables specific to configuring private LLT over Ethernet *(continued)*

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

Table 20-5 lists the response file variables that specify the required information to configure LLT over UDP.

Table 20-5 Response file variables specific to configuring LLT over UDP

Variable	List or Scalar	Description
CFG{lltoverudp}=1	Scalar	Indicates whether to configure heartbeat link using LLT over UDP. (Required)
CFG{vcs_udplink<n>_address} {<system1>}	Scalar	Stores the IP address (IPv4 or IPv6) that the heartbeat link uses on node1. You can have four heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective heartbeat links. (Required)

Table 20-5 Response file variables specific to configuring LLT over UDP *(continued)*

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

Table 20-5 Response file variables specific to configuring LLT over UDP *(continued)*

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

Table 20-6 lists the response file variables that specify the required information to configure virtual IP for SF Sybase CE cluster.

Table 20-6 Response file variables specific to configuring virtual IP for SF Sybase CE cluster

Variable	List or Scalar	Description
CFG{vcs_csgnic} {system}	Scalar	Defines the NIC device to use on a system. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_csgvip}	Scalar	Defines the virtual IP address for the cluster. (Optional)
CFG{vcs_csgnetmask}	Scalar	Defines the Netmask of the virtual IP address for the cluster. (Optional)

Table 20-7 lists the response file variables that specify the required information to configure the SF Sybase CE cluster in secure mode.

Table 20-7 Response file variables specific to configuring SF Sybase CE cluster in secure mode

Variable	List or Scalar	Description
CFG{vcs_eat_security}	Scalar	Specifies if the cluster is in secure enabled mode or not.
CFG{opt}{securityonenode}	Scalar	Specifies that the securityonenode option is being used.
CFG{securityonenode_menu}	Scalar	Specifies the menu option to choose to configure the secure cluster one at a time. ■ 1—Configure the first node ■ 2—Configure the other node
CFG{security_conf_dir}	Scalar	Specifies the directory where the configuration files are placed.
CFG{opt}{security}	Scalar	Specifies that the security option is being used.

Table 20-8 lists the response file variables that specify the required information to configure VCS users.

Table 20-8 Response file variables specific to configuring VCS users

Variable	List or Scalar	Description
CFG{vcs_userenpw}	List	List of encoded passwords for VCS users The value in the list can be "Administrators Operators Guests" **Note:** The order of the values for the vcs_userenpw list must match the order of the values in the vcs_username list. (Optional)
CFG{vcs_username}	List	List of names of VCS users (Optional)

Table 20-8 Response file variables specific to configuring VCS users *(continued)*

Variable	List or Scalar	Description
CFG{vcs_userpriv}	List	List of privileges for VCS users **Note:** The order of the values for the vcs_userpriv list must match the order of the values in the vcs_username list. (Optional)

Table 20-9 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 20-9 Response file variables specific to configuring VCS notifications using SMTP

Variable	List or Scalar	Description
CFG{vcs_smtpserver}	Scalar	Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification. (Optional)
CFG{vcs_smtprecp}	List	List of full email addresses (example: user@symantecexample.com) of SMTP recipients. (Optional)
CFG{vcs_smtprsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional)

Table 20-10 lists the response file variables that specify the required information to configure VCS notifications using SNMP.

Table 20-10 Response file variables specific to configuring VCS notifications using SNMP

Variable	List or Scalar	Description
CFG{vcs_snmpport}	Scalar	Defines the SNMP trap daemon port (default=162). (Optional)
CFG{vcs_snmpcons}	List	List of SNMP console system names (Optional)
CFG{vcs_snmpcsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional)

Table 20-11 lists the response file variables that specify the required information to configure SF Sybase CE global clusters.

Table 20-11 Response file variables specific to configuring SF Sybase CE global clusters

Variable	List or Scalar	Description
CFG{vcs_gconic} {system}	Scalar	Defines the NIC for the Virtual IP that the Global Cluster Option uses. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_gcovip}	Scalar	Defines the virtual IP address to that the Global Cluster Option uses. (Optional)
CFG{vcs_gconetmask}	Scalar	Defines the Netmask of the virtual IP address that the Global Cluster Option uses. (Optional)

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

Table 20-12 lists the response file variables that specify the required information to configure disk-based I/O fencing for SF Sybase CE.

Table 20-12 Response file variables specific to configuring disk-based I/O fencing

Variable	List or Scalar	Description
CFG{opt}{fencing}	Scalar	Performs the I/O fencing configuration. (Required)
CFG{fencing_option}	Scalar	Specifies the I/O fencing configuration mode. ■ 2—Sybase Mode fencing ■ 3—Disabled mode ■ 4—Fencing migration when the cluster is online (Required)
CFG {fencing_scsi3_disk_policy}	Scalar	Specifies the I/O fencing mechanism. This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the fencing_scsi3_disk_policy variable and either the fencing_dgname variable or the fencing_newdg_disks variable. (Optional)
CFG{fencing_dgname}	Scalar	Specifies the disk group for I/O fencing. (Optional) **Note:** You must define the fencing_dgname variable to use an existing disk group. If you want to create a new disk group, you must use both the fencing_dgname variable and the fencing_newdg_disks variable.

Table 20-12 Response file variables specific to configuring disk-based I/O fencing *(continued)*

Variable	List or Scalar	Description
CFG{fencing_newdg_disks}	List	Specifies the disks to use to create a new disk group for I/O fencing. (Optional) **Note:** You must define the fencing_dgname variable to use an existing disk group. If you want to create a new disk group, you must use both the fencing_dgname variable and the fencing_newdg_disks variable.

Response file variables to configure SF Sybase CE in VCS

Table 20-13 lists the response file variables that you can define to configure SF Sybase CE in VCS.

Table 20-13 Response file variables specific to configuring SF Sybase CE in VCS

Variable	List or Scalar	Description
CFG{sfsybasece}{ase_home}	Scalar	Defines the SF Sybase CE home directory.
CFG{sfsybasece}{ase_owner}	Scalar	Defines the SF Sybase CE owner name.
CFG{sfsybasece}{ase_quorum}	Scalar	Defines the SF Sybase CE quorum device.
CFG{sfsybasece}{ase_sa}	Scalar	Defines the SF Sybase CE administrator name.
CFG{sfsybasece}{ase_server} {redhat92205}{SERVER}	Scalar	Defines the SF Sybase CE instance name on redhat92205.
CFG{sfsybasece}{ase_server} {rhel694213}{SERVER}	Scalar	Defines the SF Sybase CE instance name on rhel694213.
CFG{sfsybasece}{ase_version}	Scalar	Defines the SF Sybase CEversion.

Table 20-13 Response file variables specific to configuring SF Sybase CE in VCS *(continued)*

Variable	List or Scalar	Description
CFG{sfsybasece}{menu}=3	Scalar	Option for configuring SF Sybase CE under VCS.
CFG{sfsybasece}{storage_resource} {database_dontuse}{database01vol} {usage}	Scalar	Lists the SF Sybase CE database devices that reside on the database_dontuse diskgroup and the database01vol volume.
CFG{sfsybasece}{storage_resource} {master_dontuse}{mastervol} {usage}	Scalar	Lists the SF Sybase CE database devices that reside on the master_dontuse diskgroup and the mastervol volume.
CFG{sfsybasece}{storage_resource} {proc_dontuse}{proc01vol} {mount}	Scalar	Specifies the mount point for the proc_dontuse database device.
CFG{sfsybasece}{storage_resource} {proc_dontuse}{proc01vol} {usage}	Scalar	Lists the SF Sybase CE database devices that reside on the proc_dontuse diskgroup and the proc01vol volume.
CFG{sfsybasece}{storage_resource} {quorum_dontuse}{quorumvol} {usage}	Scalar	Lists the SF Sybase CE quorum devices that reside on the quorum_dontuse diskgroup and the quorumvol volume.
CFG{sfsybasece}{storage_resource} {sybase1_dontuse}{sybasevol} {mount}="/opt/sybase"	Scalar	Specifies the SF Sybase CE installation location under `/opt/sybase`.
CFG{sfsybasece}{storage_resource} {sybase1_dontuse}{sybasevol} {usage}="sybase installation"	Scalar	Specifies the SF Sybase CE installation location that resides on the sybase1_dontuse diskgroup and the sybasevol volume.
CFG{sybase_location}	Scalar	Specifies the SF Sybase CE location type. ■ 1—Location on CFS ■ 2—Location on a local VxFS file system.

Section 6

Adding or removing nodes from an SF Sybase CE cluster

Chapter 21

Adding a node to SF Sybase CE clusters

This chapter includes the following topics:

About adding a node to a cluster

After you install SF Sybase CE and create a cluster, you can add and remove nodes from the cluster.You can create clusters of up to 4 nodes.

You can add a node:

- Using the product installer
- Manually

The following procedure provides a summary of the tasks required to add a node to an existing SF Sybase CE cluster.

To add a node to a cluster

1 Complete the prerequisites and preparatory tasks before adding a node to the cluster.

   See "Before adding a node to a cluster" on page 250.

2 Add a new node to the cluster.

   See "Adding a node to a cluster using the SF Sybase CE installer" on page 253.

   See "Adding the node to a cluster manually" on page 256.

3 Complete the preparatory tasks before adding a node to Sybase.

4 Add the node to Sybase.

5 If you are using the Storage Foundation for Databases (SFDB) tools, you must update the repository database.

The example procedures describe how to add a node to an existing cluster with two nodes.

Before adding a node to a cluster

Before preparing to add the node to an existing SF Sybase CE cluster, perform the required preparations.

- Verify hardware and software requirements are met.
- Set up the hardware.
- Prepare the new node.

To verify hardware and software requirements are met

1 Review hardware and software requirements for SF Sybase CE.

2 Verify the new system has the same identical operating system versions and patch levels as that of the existing cluster

3 Verify the existing cluster is an SF Sybase CE cluster and that SF Sybase CE is running on the cluster.

4 If the cluster is upgraded from the previous version, you must check the cluster protocol version to make sure it has the same version as the node to be added. If there is a protocol mismatch, the node is unable to join the existing cluster.

   Check the cluster protocal version using:

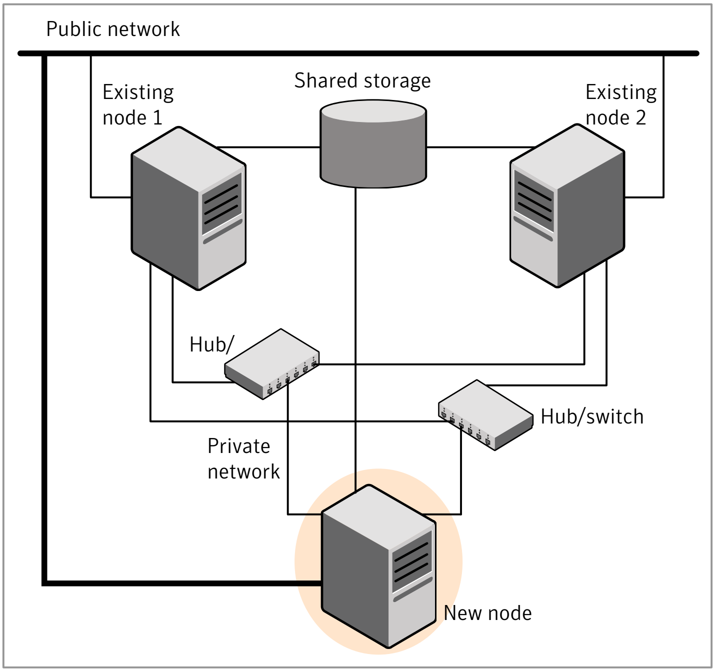
```
# vxdctl protocolversion
Cluster running at protocol 110
```

5 If the cluster protocol is below 110, upgrade it on the masters node using:

```
# vxdctl upgrade [version]
```

Before you configure a new system on an existing cluster, you must physically add the system to the cluster as illustrated in Figure 21-1.

Figure 21-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the SF Sybase CE private Ethernet controllers.

   Perform the following tasks as necessary:

- When you add nodes to a cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a two-node cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 21-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Make sure that you meet the following requirements:

- The node must be connected to the same shared storage devices as the existing nodes.
- The node must have private network connections to two independent switches for the cluster.
  For more information, see the *Veritas Cluster Server Installation Guide*.
- The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster.

Prepare the new node before you add it to an existing SF Sybase CE cluster.

To prepare the new node

1 Verify that the new node meets installation requirements.

```
# ./installsfsybasece -precheck
```

2 Install SF Sybase CE on the new system using the `-install` option to install SF Sybase CE. Do not configure SF Sybase CE when prompted.

3 You can restart the new node after installation is complete. Configure the new node using the configuration from the existing cluster nodes.

```
# ./installsfsybasece system3
```

Adding a node to a cluster

You can use one of the following methods to add a node to an existing SF Sybase CE cluster:

SF Sybase CE installer	See "Adding a node to a cluster using the SF Sybase CE installer" on page 253.
Manual	See "Adding the node to a cluster manually" on page 256.

Note: Before you add the node, make sure that SF Sybase CE is not configured on the node.

Adding a node to a cluster using the SF Sybase CE installer

You can add a node using the `-addnode` option with the SF Sybase CE installer.

The SF Sybase CE installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and packages installed on the new node.
- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:

  `/etc/llttab`

  `/etc/VRTSvcs/conf/sysname`
- Copies the following files on the new node:

  `/etc/llthosts`

  `/etc/gabtab`

  `/etc/VRTSvcs/conf/config/main.cf`
- Copies the following files from the existing cluster to the new node:

  `/etc/vxfenmode`

  `/etc/vxfendg`

  `/etc/vx/.uuids/clusuuid`

  `/etc/default/llt`

  `/etc/default/gab`

  `/etc/default/vxfen`
- Configures fencing.
- Adds the new node to the CVM, ClusterService, and VxSS service groups in the VCS configuration.

  Note: For other service groups configured under VCS, update the configuration for the new node manually.
- Starts SF Sybase CE processes and configures CVM and CFS on the new node.

At the end of the process, the new node joins the SF Sybase CE cluster.

To add the node to an existing cluster using the installer

1. Log in as the root user on one of the nodes of the existing cluster.

2. Run the SF Sybase CE installer with the -addnode option.

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

   ```
   # ./installsfsybasece -addnode
   ```

   The installer displays the copyright message and the location where it stores the temporary installation logs.

3. Enter the name of a node in the existing SF Sybase CE cluster.

   The installer uses the node information to identify the existing cluster.

   ```
   Enter one node of the SFSYBASECE cluster to which
   you would like to add one or more new nodes: system1
   ```

4. Review and confirm the cluster information.

5. Enter the name of the systems that you want to add as new nodes to the cluster.

   ```
   Enter the system names separated by spaces
   to add to the cluster: system3
   ```

   The installer checks the installed products and packages on the nodes and discovers the network interfaces.

6 Enter the name of the network interface that you want to configure as the first private heartbeat link.

If there are IP addresses already configured on the interface, confirm whether you want to use the interface as the first private heartbeat link.

Note: The network interface names used for the private interconnects on the new node must be the same as that of the existing nodes in the cluster. The LLT configuration for the new node must be the same as that of the existing cluster.

```
Enter the NIC for the first private heartbeat
link on system3: [b,q,?] bge1

Enter the NIC for the second private heartbeat
link on system3: [b,q,?] bge2
```

Note: At least two private heartbeat links must be configured for high availability of the cluster.

---

7 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.

The installer verifies the network interface settings and displays the information.

8 Review and confirm the information.

9 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on system3: bge3
```

The installer starts the SF Sybase CE processes and configures CVM and CFS on the new node. The new node is now part of the cluster.

```
SF Sybase CE is configured on the cluster. Do you want to
configure it on the new node(s)? [y,n,q] (y) n
```

To add the new node into the Sybase ASE CE cluster and database:

See "Adding the new instance to the Sybase ASE CE cluster" on page 265.

10 Configure the following service groups manually to include the new node in the VCS configuration:

- The *binmnt* group which contains the Sybase binaries

- The *Sybase* group which contains:
  - The new instance on the added node
  - The database mounts where the database resides
  - The quorum mounts where the quorum device resides.
- See "Adding the new instance to the Sybase ASE CE cluster" on page 265.

11 Confirm that the new node has joined the SF Sybase CE cluster using `lltstat -n` and `gabconfig -a` commands.

Adding the node to a cluster manually

Perform this procedure after you install SF Sybase CE only if you plan to add the node to the cluster manually.

To add the node manually to the cluster

1 Start the Volume Manager.

See "Starting Volume Manager on the new node" on page 256.

2 Configure LLT and GAB.

See "Configuring LLT and GAB on the new node" on page 257.

3 Configure fencing for the new node to match the fencing configuration on the existing cluster.

See "Starting fencing on the new node" on page 262.

4 Start VCS.

See "Starting VCS after adding the new node" on page 264.

5 Configure CVM and CFS.

See "Configuring CVM and CFS on the new node" on page 262.

6 If the ClusterService group is configured on the existing cluster, add the node to the group.

See "Configuring the ClusterService group for the new node" on page 264.

Starting Volume Manager on the new node

Volume Manager uses license keys to control access. As you run the `vxinstall` utility, answer **n** to prompts about licensing. You installed the appropriate license when you ran the `installsfsybasece` program.

To start Volume Manager on the new node

1. To start Veritas Volume Manager on the new node, use the vxinstall utility:

   ```
   # vxinstall
   ```

2. Enter **n** when prompted to set up a system wide disk group for the system.

   The installation completes.

3. Verify that the daemons are up and running. Enter the command:

   ```
   # vxdisk list
   ```

   Make sure the output displays the shared disks without errors.

Configuring LLT and GAB on the new node

Perform the steps in the following procedure to configure LLT and GAB on the new node.

To configure LLT and GAB on the new node

1. Edit the /etc/llthosts file on the existing nodes. Using vi or another text editor, add the line for the new node to the file. The file resembles:

   ```
   0 system1
   1 system2
   2 system3
   ```

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 system3
   set-cluster 101

   link bge1 /dev/bge:1 - ether - -
   link bge2 /dev/bge: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 node. This file must contain a line that resembles the following example:

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

   Where N represents the number of systems in the cluster including the new node. For a three-system cluster, N would equal 3.

5. Edit the /etc/gabtab file on each of the existing systems, changing the content to match the file on the new system.

6. Copy the following files from one of the nodes in the existing cluster to the new node:

   ```
   /etc/sysconfig/llt
   /etc/sysconfig/gab
   /etc/sysconfig/vcs
   ```

   Verify if the attributes in each file are set as follows before using smf on Solaris 10 to start the related processes and to load drivers:

   ```
   LLT_START/LLT_STOP=1
   GAB_START/GAB_STOP=1
   VXFEN_START/VXFEN_STOP=1
   VCS_START/VCS_STOP=1
   ```

7. Use vi or another text editor to create the file `/etc/VRTSvcs/conf/sysname` on the new node. This file must contain the name of the new node added to the cluster.

   For example:

   ```
   system3
   ```

8. Create the Unique Universal Identifier file `/etc/vx/.uuids/clusuuid` on the new node:

   ```
   # uuidconfig.pl -rsh -clus -copy \
   -from_sys system1 -to_sys system3
   ```

9 Start the LLT and GAB drivers on the new node:

```
# svcadm enable llt
```

```
# svcadm enable gab
```

10 On the new node, verify GAB port membership:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen df204 membership 01
```

Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

Table 21-1 uses the following information for the following command examples.

Table 21-1 The command examples definitions

Name	Fully-qualified host name (FQHN)	Function
saturn	saturn.nodes.example.com	The new node that you are adding to the cluster.

Configuring the authentication broker on node saturn

To configure the authentication broker on node saturn

1. Extract the embedded authentication files and copy them to temporary directory:

   ```
   # mkdir -p /var/VRTSvcs/vcsauth/bkup
   ```

   ```
   # cd /tmp; gunzip -c /opt/VRTSvcs/bin/VxAT.tar.gz | tar xvf -
   ```

2. Edit the setup file manually:

   ```
   # /cat /etc/vx/.uuids/clusuuid 2>&1
   ```

   The output is a string denoting the UUID. This UUID (without { and }) is used as the ClusterName for the setup file.

   ```
   {UUID}
   ```

   ```
   # cat /tmp/eat_setup 2>&1
   ```

   The file content must resemble the following example:

   ```
   AcceptorMode=IP_ONLY

   BrokerExeName=vcsauthserver

   ClusterName=UUID

   DataDir=/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER

   DestDir=/opt/VRTSvcs/bin/vcsauth/vcsauthserver

   FipsMode=0

   IPPort=14149

   RootBrokerName=vcsroot_uuid

   SetToRBPlusABorNot=0

   SetupPDRs=1

   SourceDir=/tmp/VxAT/version
   ```

3 Set up the embedded authentication file:

```
# cd /tmp/VxAT/version/bin/edition_number; \
./broker_setup.sh/tmp/eat_setup
```

```
/opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssregctl -s -f
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER/root/.VRTSat/profile \
/VRTSatlocal.conf -b 'Security\Authentication \
\Authentication Broker' -k UpdatedDebugLogFileName \
-v /var/VRTSvcs/log/vcsauthserver.log -t string
```

4 Copy the broker credentials from one node in the cluster to saturn by copying the entire `bkup` directory.

The `bkup` directory content resembles the following example:

```
# cd /var/VRTSvcs/vcsauth/bkup/
```

```
# ls
```

```
CMDSERVER  CPSADM  HAD  VCS_SERVICES  WAC
```

5 Import the VCS_SERVICES domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \
/var/VRTSvcs/vcsauth/data/VCSAUTHSERVER -f /var/VRTSvcs/vcsauth/bkup \
/VCS_SERVICES -p password
```

6 Import the credentials for HAD, CMDSERVER, CPSADM, and WAC.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atutil import -z \
/var/VRTSvcs/vcsauth/data/VCS_SERVICES -f /var/VRTSvcs/vcsauth/bkup \
/HAD -p password
```

7 Start the vcsauthserver process on saturn.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh
```

8 Perform the following tasks:

```
# mkdir /var/VRTSvcs/vcsauth/data/CLIENT
```

```
# mkdir /var/VRTSvcs/vcsauth/data/TRUST
```

```
# export EAT_DATA_DIR='/var/VRTSvcs/vcsauth/data/TRUST'
```

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat setuptrust -b \
localhost:14149 -s high
```

9 Create the `/etc/VRTSvcs/conf/config/.secure` file:

```
# touch /etc/VRTSvcs/conf/config/.secure
```

Starting fencing on the new node

Perform the following steps to start fencing on the new node.

To start fencing on the new node

1 For disk-based fencing, copy the following files from one of the nodes in the existing cluster to the new node:

```
/etc/default/vxfen
/etc/vxfendg
/etc/vxfenmode
```

2 Start fencing on the new node:

For Solaris 10:

```
# svcadm enable vxfen
```

3 On the new node, verify that the GAB port memberships are a and b:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   57c004 membership 012
Port b gen   57c019 membership 012
```

Configuring CVM and CFS on the new node

Modify the existing cluster configuration to configure CVM and CFS for the new node.

To configure CVM and CFS on the new node

1. Make a backup copy of the main.cf file on the existing node, if not backed up in previous procedures. For example:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

2. On one of the nodes in the existing cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

3. Add the new node to the VCS configuration, if not already added:

```
# hasys -add system3
```

4. To enable the existing cluster to recognize the new node, run the following commands on one of the existing nodes:

```
# hagrp -modify cvm SystemList -add system3 2
# hagrp -modify cvm AutoStartList -add system3
# hares -modify cvm_clus CVMNodeId -add system3 2
# haconf -dump -makero
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

5. On the remaining nodes of the existing cluster, run the following commands:

```
# /etc/vx/bin/vxclustadm -m vcs reinit
# /etc/vx/bin/vxclustadm nidmap
```

6 Copy the configuration files from one of the nodes in the existing cluster to the new node:

```
# rcp /etc/VRTSvcs/conf/config/main.cf \
system3:/etc/VRTSvcs/conf/config/main.cf
# rcp /etc/VRTSvcs/conf/config/CFSTypes.cf \
system3:/etc/VRTSvcs/conf/config/CFSTypes.cf
# rcp /etc/VRTSvcs/conf/config/CVMTypes.cf \
system3:/etc/VRTSvcs/conf/config/CVMTypes.cf
```

7 The `/etc/vx/tunefstab` file sets non-default tunables for local-mounted and cluster-mounted file systems.

If you have configured a `/etc/vx/tunefstab` file to tune cluster-mounted file systems on any of the existing cluster nodes, you may want the new node to adopt some or all of the same tunables.

To adopt some or all tunables, review the contents of the file, and copy either the file, or the portions desired, into the `/etc/vx/tunefstab` file on the new cluster node.

Starting VCS after adding the new node

Start VCS on the new node.

To start VCS on the new node

1 Start VCS on the new node:

```
# hastart
```

VCS brings the CVM and CFS groups online.

2 Verify that the CVM and CFS groups are online:

```
# hagrp -state
```

Configuring the ClusterService group for the new node

If the ClusterService group is configured on the existing cluster, add the node to the group by performing the steps in the following procedure on one of the nodes in the existing cluster.

To configure the ClusterService group for the new node

1. On an existing node, for example system1, write-enable the configuration:

   ```
   # haconf -makerw
   ```

2. Add the node system3 to the existing ClusterService group.

   ```
   # hagrp -modify ClusterService SystemList -add system3 2
   ```

   ```
   # hagrp -modify ClusterService AutoStartList -add system3
   ```

3. Modify the IP address and NIC resource in the existing group for the new node.

   ```
   # hares -modify gcoip Device bge0 -sys system3
   ```

   ```
   # hares -modify gconic Device bge0 -sys system3
   ```

4. Save the configuration by running the following command from any node.

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

Adding the new instance to the Sybase ASE CE cluster

To add a new Sybase ASE CE instance to the cluster you must complete the following tasks:

- Creating Sybase user and groups
- Preparing the mount point for Sybase resources on the new node
- Adding a new Sybase ASE CE instance to the Sybase ASE CE cluster
- Bringing the new Sybase ASE CE instance under VCS control

Creating Sybase user and groups

To prepare the new node for a Sybase ASE CE instance, create the Sybase user and groups.

See your Sybase ASE CE documentation.

Preparing the mount point for Sybase resources on the new node

To prepare the new node for installing Sybase, you must prepare mount points on the new node for Sybase binaries, quorum device, and datafiles.

See “Preparing for shared mount point on CFS for Sybase ASE CE binary installation” on page 197.

See “Preparing to create a Sybase ASE CE cluster” on page 198.

Create the mount point for the file system with the Sybase binary files.

For example:

```
# mkdir -p /sybase
# chown -R sybase:sybase /sybase
```

Create the mount point for the file system with the Sybase quorum device.

For example:

```
# mkdir -p /quorum
# chown -R sybase:sybase /quorum
```

Create the mount point for the file system with the Sybase datafiles.

For example:

```
# mkdir -p /sybdata
# chown -R sybase:sybase /sybdata
```

Adding a new Sybase ASE CE instance to the Sybase ASE CE cluster

For a CFS shared installation of Sybase ASE CE binaries, the new Sybase ASE CE instance on the new node can share the existing cluster's Sybase ASE CE binaries.

For a local VxFS installation of Sybase ASE CE binaries, you need to create diskgroups for binaries and install Sybase ASE CE binaries on the new node.

To configure the new node

1 From an existing node in the cluster, write enable the cluster configuration:

```
# haconf -makerw
```

2 In case of Sybase binaries on CFS, add the new node to the VCS service group for the Sybase binaries:

```
# hagrp -modify binmnt SystemList -add system3

# hagrp -modify binmnt AutoStartList -add system3
```

3 In case of Sybase binaries on local VxFS, add the name of the DiskGroup for the new node.

```
# hares -modify sybase_install_dg DiskGroup
sybase_new_diskgroup -sys system3
```

```
# hares -modify sybase_install_mnt BlockDevice
/dev/vx/dsk/sybase_new_diskgroup/sybase_new_volume -sys system3
```

```
# hares -modify sybase_install_vol DiskGroup
sybase_new_diskgroup -sys system3
```

```
# hares -modify sybase_install_vol Volume
sybase_new_volume -sys system3
```

4 Save the configuration changes.

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

5 Bring the VCS group for Sybase binaries group online on the new node:

```
# hagrp -online binmnt -sys system3
```

To add the new node to the Sybase ASE CE cluster

- Follow the procedures in your Sybase ASE CE documentation.

Bringing the new Sybase ASE CE instance under VCS control

After adding a new instance to the Sybase ASE CE cluster you must bring it under VCS control.

To configure the new instance under VCS control

1 From an existing node in the cluster, write enable the cluster configuration:

```
# haconf -makerw
```

2 Add the node to the VCS service group for managing Sybase resources:

```
# hagrp -modify sybasece SystemList -add system3 2
```

```
# hagrp -modify sybasece AutoStartList -add system3
```

3 Add the new instance to the VCS resource used to manage Sybase instances:

```
# hares -modify ase Server ase3 -sys system3
```

4 Save the configuration changes.

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

5 Bring the Sybase service group online on the new node:

```
# hagrp -online sybasece -sys system3
```

Note: Before you bring the Sybase service group online, make sure you have manually created the Run file for the added instance on the added node, with appropriate instance information.

This completes the addition of the new node to the cluster. You now have a three node cluster.

Chapter 22

Removing a node from SF Sybase CE clusters

This chapter includes the following topics:

About removing a node from a cluster

You can remove one or more nodes from an SF Sybase CE cluster.

Overview of tasks for removing a node from a cluster:

- Prepare the node to be removed.
  - Take offline service groups and resources which support Sybase.
  - Remove database instances and software from the node.
  - Stop applications that use File System or Cluster File System mount points not configured under VCS.

  See "Removing a node from a cluster" on page 270.
- Remove the node from the cluster.
  - Stop VCS on the node to be removed.
  - Unmount the File System and Cluster File System file systems not configured under VCS.
  - Uninstall SF Sybase CE from the node.

See "Removing a node from a cluster" on page 270.

- Modify the VCS configuration files on the existing nodes.
  See "Modifying the VCS configuration files on existing nodes" on page 271.
- Remove the security credentials from the node if it is part of a secure cluster.

The Veritas product installer does not support removing a node. You must remove a node manually. The example procedures describe how to remove a node from a cluster with three nodes.

Removing a node from a cluster

Perform the following steps to remove a node from a cluster. The procedure can be done from any node remaining in the cluster or from a remote host.

To prepare to remove a node from a cluster

1 Take the Sybase ASE CE service group offline (if under VCS control) on the node you want to remove.

```
# hagrp -offline sybase_group -sys system3
```

2 Remove the Sybase ASE CE database instance from the node.

For instructions, see the Sybase ASE CE documentation.

3 Take the *binmnt* service group offline (if under VCS control) on the node you want to remove.

```
# hagrp -offline binmnt_group -sys system3
```

4 Stop the applications that use VxFS/CFS mount points and are not configured under VCS. Use native application commands to stop the applications.

5 Uninstall Sybase ASE CE from the node.

For instructions, see the Sybase ASE CE documentation.

To remove a node from a cluster

1 Stop VCS on the node:

```
# hastop -local
```

2 Unmount the VxFS/CFS file systems that are not configured under VCS.

```
# umount mount_point
```

3 Uninstall SF Sybase CE from the node using the SF Sybase CE installer.

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

```
# ./uninstallsfsybasece system3
```

The installer stops all SF Sybase CE processes and uninstalls the SF Sybase CE packages.

4 Modify the VCS configuration files on the existing nodes to remove references to the deleted node.

See "Modifying the VCS configuration files on existing nodes" on page 271.

Modifying the VCS configuration files on existing nodes

Modify the configuration files on the remaining nodes of the cluster to remove references to the deleted nodes.

The process involves:

- Editing the /etc/llthosts file
- Editing the /etc/gabtab file
- Modifying the VCS configuration to remove the node

For an example main.cf:

To edit the /etc/llthosts file

◆ On each of the existing nodes, edit the `/etc/llthosts` file to remove lines that contain references to the removed nodes.

For example, if system3 is the node removed from the cluster, remove the line "2 system3" from the file:

```
0 system1
1 system2
2 system3
```

Change to:

```
0 system1
1 system2
```

To edit the /etc/gabtab file

- Modify the following command in the `/etc/gabtab` file to reflect the number of systems after the node is removed:

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

  where N is the number of remaining nodes in the cluster.

  For example, with two nodes remaining, the file resembles:

  ```
  /sbin/gabconfig -c -n2
  ```

Modify the VCS configuration file main.cf to remove all references to the deleted node.

Use one of the following methods to modify the configuration:

- Edit the `/etc/VRTSvcs/conf/config/main.cf` file
  This method requires application down time.
- Use the command line interface
  This method allows the applications to remain online on all remaining nodes.

The following procedure uses the command line interface and modifies the sample VCS configuration to remove references to the deleted node. Run the steps in the procedure from one of the existing nodes in the cluster. The procedure allows you to change the VCS configuration while applications remain online on the remaining nodes.

To modify the VCS configuration using the CLI

1. Back up the `/etc/VRTSvcs/conf/config/main.cf` file.

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

   ```
   # cp main.cf main.cf.3node.bak
   ```

2. Change the cluster configuration to read-write mode:

   ```
   # haconf -makerw
   ```

3. Remove the node from the AutoStartList attribute of the service group by specifying the remaining nodes in the desired order:

   ```
   # hagrp -modify cvm AutoStartList system1 system2
   ```

4 Remove the deleted node from the system list of any other parent service groups to CVM that exist on the cluster before removing CVM. For example, to delete the node system3:

```
# hagrp -modify syb_grp SystemList -delete system3
# hagrp -modify Sybase SystemList -delete system3
# hagrp -modify cvm SystemList -delete system3
# hares -modify cvm_clus CVMNodeId -delete system3
```

5 If you have a local VxFS configuration, will also need to remove the diskgroup of node to be removed from *binmnt*.

```
# hares -modify sybase_install_dg DiskGroup -delete \
sybase_new_diskgroup
```

6 Remove the node from the SystemList attribute of the service group:

7 Remove the node from the CVMNodeId attribute of the service group:

```
# hares -modify cvm_clus CVMNodeId -delete system3
```

8 Remove the deleted node from the NodeList attribute of all CFS mount resources:

```
# hares -modify CFSMount NodeList -delete system3
```

9 Remove the deleted node from the cluster system list:

```
# hasys -delete system3
```

10 Save the new configuration to disk:

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

11 Verify that the node is removed from the VCS configuration.

```
# grep -i system3 /etc/VRTSvcs/conf/config/main.cf
```

If the node is not removed, use the VCS commands as described in this procedure to remove the node.

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node saturn. Perform the following steps.

To remove the security credentials

1. Stop the AT process.

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \
   stop
   ```

2. Remove the credentials.

   ```
   # rm -rf /var/VRTSvcs/vcsauth/data/
   ```

Section 7

Configuration of disaster recovery environments

Chapter 23

Setting up a replicated global cluster

This chapter includes the following topics:

Replication in the SF Sybase CE environment

You can set up a primary SF Sybase CE cluster for replication to a secondary SF Sybase CE cluster by configuring global VCS service groups and using a replication technology. The Sybase ASE CE 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 Veritas Volume Replicator (VVR), which provides host-based volume replication. Using VVR you can replicate data volumes on a shared disk group in SF Sybase CE. Hardware-based replication is not supported at this time.

About setting up a global cluster in an SF Sybase CE environment

Configuring a global SF Sybase CE cluster requires the coordination of many component setup tasks. The following procedures provide guidelines.

Tasks required to set up a global cluster:

- Configure a cluster at the primary site.
  See "Configuring an SF Sybase CE global cluster at the primary site" on page 279.
- Configure a cluster at the secondary site.
  See "Configuring an SF Sybase CE cluster at the secondary site" on page 281.
- Configure replication on clusters at both sites.
  See "Configuring replication for SF Sybase CE clusters at both sites" on page 283.
- Configure VCS service groups for replication.
  See "Modifying the ClusterService group for a global SF Sybase CE cluster" on page 283.
- See "Defining the remote SF Sybase CE cluster and heartbeat objects" on page 285.
- See "Configuring the VCS service groups for global SF Sybase CE clusters" on page 288.
- Test the HA/DR configuration.
- Upon successful testing, bring the environment into production.

SF Sybase CE HA/DR configuration tasks may require adjustments depending upon your particular starting point, environment, and configuration, as the details of your configuration may differ from the examples given in the procedures. Review the installation requirements and sample cluster configuration files for primary and secondary clusters.

Review the requirements information to make sure your configuration is supported for SF Sybase CE.

- For product licensing information:
  See "About Veritas product licensing" on page 47.
- For supported hardware and software:
  Sybase documentation for additional requirements pertaining to your version of Sybase.
- To confirm the compatibility of your hardware, see the current compatibility list in the Symantec Technical Support website:
  http://www.symantec.com/docs/TECH170013

SF Sybase CE supports the following replication technologies through the use of Veritas replication agents:

Table 23-1 Supported replication options for SF Sybase CE global clusters

Replication technology	Supported modes	Supported software
Veritas Volume Replicator (VVR) Supporting agents ■ RVGShared ■ RVGSharedPri ■ RVGLogOwner	■ Asynchronous replication ■ Synchronous replication	Host-based replication

You can use the Veritas replication agents listed in the table above for global clusters that run SF Sybase CE. 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 Sybase CE nodes. The agents make sure that the system which has the resource online also has safe and exclusive access to the configured devices.

For instructions for configuring AT in a global cluster:

See the *Veritas Cluster Server Administrator's Guide*

Configuring an SF Sybase CE global cluster at the primary site

You can use an existing SF Sybase CE cluster or you can install a new SF Sybase CE cluster for your primary site.

For planning information:

See "Planning for disaster recovery" on page 45.

If you are using an existing cluster as the primary and you want to set up a global cluster, skip the steps below and proceed to configure your secondary cluster.

See "Configuring an SF Sybase CE cluster at the secondary site" on page 281.

Note: You must have a GCO license enabled for a global cluster. If you are using VVR for replication, you must have a VVR license enabled.

If you do not have an existing cluster and you are setting up two new sites for an SF Sybase CE global cluster, follow the steps below.

To set up the cluster and database at the primary site

1. Install and configure servers and storage.
2. Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option enabled for a global cluster. If you are using VVR for replication, you must have it enabled.
3. Install and configure SF Sybase CE.

   For preparation:

   See "About preparing to install and configure SF Sybase CE" on page 55.

   For installation:

   See "Configuring the SF Sybase CE components using the script-based installer" on page 90.

   For configuration:

   See "About installing SF Sybase CE " on page 63.
4. Verify the CVM group is online on all nodes in the primary cluster:

   ```
   # hagrp -state cvm
   ```

5. Prepare systems and storage for a global cluster. Identify the hardware and storage requirements before installing Sybase ASE CE software.

   You will need to set up:

   - Shared storage for Sybase ASE CE binaries which is not replicated
   - Shared storage for the quorum device which is not replicated
   - Replicated storage for database files
6. Install and configure the Sybase ASE CE binaries:

   See "Before installing Sybase ASE CE" on page 195.

   Note the following configuration requirements:

   - The quorum device must be on non-replicated shared storage.

- The binary versions on the secondary site must be exactly same as those in primary site, including the ESD versions.
- Configure Sybase Binaries mounts/volumes under VCS control manually on the secondary site.

7 Identify the disks that will be replicated, create the required CVM disk group, volume, and file system.

8 Create the database on the file system you created in the previous step.

9 Configure the VCS service groups for the database.

See "Preparing to configure the Sybase instances under VCS control" on page 200.

10 Verify that all VCS service groups are online.

Configuring an SF Sybase CE cluster at 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.
- You must use the same OS user and group IDs for your database for installation and configuration on both the primary and secondary clusters.

To set up the cluster on secondary site

1 Install and configure servers and storage.

2 Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster. If you are using VVR for replication, you must have it enabled.

3 Install and configure SF Sybase CE.

For preparation:

See "About preparing to install and configure SF Sybase CE" on page 55.

For installation:

See "About installing SF Sybase CE " on page 63.

For configuration:

See "Configuring the SF Sybase CE components using the script-based installer" on page 90.

4 Prepare systems and storage for a global cluster. Identify the hardware and storage requirements before installing Sybase ASE CE software.

You will need to set up:

- Shared storage for Sybase ASE CE binaries which is not replicated
- Shared storage for the quorum device which is not replicated
- Replicated storage for database files

5 Install and configure the Sybase ASE CE binaries:

See "Before installing Sybase ASE CE" on page 195.

Note the following configuration requirements:

- The quorum device must be on non-replicated shared storage.
- The binary versions on the secondary site must be exactly same as those in primary site, including the ESD versions.
- Configure Sybase Binaries mounts/volumes under VCS control manually on the secondary site.

To set up the database for the secondary site

◆ Do not create the database. The database will be replicated from the primary site.

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 files when the failover occurs and the secondary is promoted to become the primary site.

See "To create the disk group, volume and mount point for the datafiles" on page 199.

Configuring the Sybase ASE CE cluster on the secondary site

Before bringing Sybase ASE CE online at the secondary site, you must configure the Sybase ASE CE cluster on the secondary site.

- Modify the the Sybase ASE CE configuration files to match the secondary site environment.
- Build the new quorum device for the secondary site.
- For configuration details: See "Configuring the Sybase ASE CE cluster on the secondary site" on page 314.

Configuring replication for SF Sybase CE clusters at both sites

You must configure replication for the database files. Once replication is configured, make sure it is functioning correctly by testing before proceeding.

To configure replication at both sites

1. At both sites, identify the disks on which the database resides at the primary site and associate them with the corresponding disks at the secondary site.

   See " Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): setting up the primary site" on page 290.

2. Start replication between the sites.

   See "Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): starting replication" on page 298.

Modifying the ClusterService group for a global SF Sybase CE cluster

You have configured VCS service groups for SF Sybase CE on each cluster. Each cluster requires an additional virtual IP address associated with the cluster for cross-cluster communication. The VCS installation and creation of the ClusterService group typically involves defining this IP address.

Configure a global cluster by setting:

- Heartbeat
- Wide area cluster (wac)

- GCO IP (gcoip)
- remote cluster resources

See the *Veritas Cluster Server Administrator's Guide* for complete details on global clustering.

Modifying the global SF Sybase CE cluster configuration using the wizard

The global clustering wizard completes the following tasks:

- Validates the ability of the current configuration to support a global cluster environment.
- Creates the components that enable the separate clusters, each of which contains a different set of GAB memberships, to connect and operate as a single unit.
- Creates the ClusterService group, or updates an existing ClusterService group.

Run the global clustering configuration wizard on each of the clusters; you must have the global clustering license in place on each node in the cluster.

To modify the ClusterService group for global clusters using the global clustering wizard

1. On the primary cluster, start the GCO Configuration wizard:

   ```
   # /opt/VRTSvcs/bin/gcoconfig
   ```

2. The wizard discovers the NIC devices on the local system and prompts you to enter the device to be used for the global cluster. Specify the name of the device and press Enter.
3. If you do not have NIC resources in your configuration, the wizard asks you whether the specified NIC will be the public NIC used by all the systems. Enter **y** if it is the public NIC; otherwise enter **n**. If you entered **n**, the wizard prompts you to enter the names of NICs on all systems.

4 Enter the virtual IP address for the local cluster.

5 If you do not have IP resources in your configuration, the wizard prompts you for the netmask associated with the virtual IP. The wizard detects the netmask; you can accept the suggested value or enter another one.

The wizard starts running commands to create or update the ClusterService group. Various messages indicate the status of these commands. After running these commands, the wizard brings the ClusterService failover group online on any one of the nodes in the cluster.

Defining the remote SF Sybase CE cluster and heartbeat objects

After configuring global clustering, add the remote cluster object to define the IP address of the cluster on the secondary site, and the heartbeat object to define the cluster-to-cluster heartbeat.

Heartbeats monitor the health of remote clusters. VCS can communicate with the remote cluster only after you set up the heartbeat resource on both clusters.

To define the remote cluster and heartbeat

1 On the primary site, enable write access to the configuration:

```
# haconf -makerw
```

2 On the primary site, define the remote cluster and its virtual IP address.

In this example, the remote cluster is syb_cluster102 and its IP address is 10.11.10.102:

```
# haclus -add syb_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 syb_cluster101 and its IP address is 10.10.10.101:

```
# haclus -add syb_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 enable you to define the virtual IP address for the remote cluster.

For example:

```
# hahb -modify Icmp ClusterList syb_cluster102
# hahb -modify Icmp Arguments 10.11.10.102 -clus syb_cluster102
```

6 Save the configuration and change the access to read-only on the local cluster:

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

7 Complete step 4-6 on the secondary site using appropriate values to define the cluster on the primary site and its IP as the remote cluster for the secondary cluster.

8 Verify cluster status with the `hastatus -sum` command on both clusters.

```
# hastatus -sum
```

9 Display the global setup by executing haclus -list command.

```
# haclus -list
     syb_cluster101
     syb_cluster102
```

Example of heartbeat additions to the main.cf file on the primary site:

```
.
.
remotecluster syb_cluster102 (
Cluster Address = "10.11.10.102"
)
heartbeat Icmp (
    ClusterList = { syb_cluster102 }
    Arguments @syb_cluster102 = { "10.11.10.102" }
    )

system system1 (
    )
.
.
```

Example heartbeat additions to the main.cf file on the secondary site:

```
.
.
remotecluster syb_cluster101 (
    Cluster Address = "10.10.10.101"
    )

heartbeat Icmp (
    ClusterList = { syb_cluster101 }
    Arguments @syb_cluster101 = { "10.10.10.101" }
    )

system system3 (
    )
.
.
```

See the *Veritas Cluster Server Administrator's Guide* for details for configuring the required and optional attributes of the heartbeat object.

Configuring the VCS service groups for global SF Sybase CE clusters

To configure VCS service groups for global clusters

1. Configure and enable global groups for databases and resources.
   - Configure VCS service groups at both sites.
   - Configure the replication agent at both sites.
   - Make the database service group (sybasece) a global service group, enabling failover across clusters.
   - For example:
     See "Modifying the VCS Configuration on the Primary Site" on page 304.
2. To test real data in an environment where HA/DR has been configured, schedule a planned migration to the secondary site for testing purposes.

   For example:

   See "Migrating the role of primary site to the secondary site" on page 318.
3. Upon successful testing, bring the environment into production.

For more information about VCS replication agents:

See the *Veritas Cluster Server Bundled Agents Guide*

For complete details on using VVR in a shared disk environment:

See the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide*.

Chapter 24

Configuring a global cluster using VVR

This chapter includes the following topics:

About configuring a global SF Sybase CE cluster using VVR for replication

Before configuring clusters for global clustering, make sure both clusters have product and database software installed and configured.

Verify that you have the correct installation options enabled, whether you are using keyless licensing or installing keys manually. You must have the GCO option for a global cluster and VVR enabled.

See "About Veritas product licensing" on page 47.

After setting up two clusters running SF Sybase CE, you can configure a global cluster environment with VVR. You must modify both cluster configurations to support replication in the global cluster environment.

Configuring SF Sybase CE for global clusters requires:

- Setting up both clusters as part of a global cluster environment.
  See "About setting up a global cluster in an SF Sybase CE environment" on page 278.
- Setting up replication for clusters at both sites.
  See " Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): setting up the primary site" on page 290.
  See "Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): setting up the secondary site" on page 293.
- Starting replication of the database.
  See "Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): starting replication" on page 298.
- Configuring VCS for replication on clusters at both sites.
  See "Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): configuring cluster resources" on page 300.

For sample primary and secondary cluster configuration files:

See "Sample main.cf for a primary CVM VVR site" on page 387.

See "Sample main.cf for a secondary CVM VVR site" on page 393.

Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): setting up the primary site

Setting up replication with VVR in a global cluster environment involves the following tasks:

- If you have not already done so, create a disk group to hold data volume, SRL, and RVG on the storage on the primary site. For example:
  See "To create the disk group, volume and mount point for the datafiles" on page 199.
- Creating the Storage Replicator Log (SRL) in the disk group for the database.
  See "Creating the data and SRL volumes on the primary site" on page 291.
- Creating the Replicated Volume Group (RVG) on the primary site.

See "Setting up the Replicated Volume Group (RVG) on the primary site" on page 292.

- Editing the /etc/vx/vras/.rdg files on the primary site after creating the data and SRL volumes on the secondary site.
  See "Editing the /etc/vx/vras/.rdg files" on page 294.

Creating the data and SRL volumes on the primary site

Create the data volume if you do not have one already.

- The data volume on the secondary site has the same name and the same size as the data volume on the primary site.
- The data volume and SRL volume should exist in the same disk group.
- Mirror the data volume in the absence of hardware-based mirroring.

To create the data volume on the primary site

- ◆ In the disk group created for the Sybase ASE CE database, create a volume for data. In the example, the *syb_vol* volume on the primary site is 12 GB:

```
# vxassist -g sybdata_101 make syb_vol 12000M nmirror=2 disk1 disk2
```

Create the SRL. The SRL is a volume in the RVG. The RVG also holds the data volumes for replication.

- The SRL on the secondary site has the same name and the same size as the SRL on the primary site.
- If possible, create SRLs on disks without other volumes.
- Mirror SRLs and in the absence of hardware-based mirroring.

In the example procedure below, *sybdata_101* is the disk group and *syb_vol* is the data volume to be replicated.

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 CVM master or the slave:

   ```
   # vxdctl -c mode
   ```

3 On the CVM master node, issue the following command:

```
# vxassist -g sybdata_101 make syb_srl 1500M nmirror=2 disk4 disk5
```

Note: Assume that for the example setup that *disk4* and *disk5* are already added and are part of the same disk group. They are used in this step for mirroring and creation of the SRL.

---

4 If the SRL volume is not already started, start the SRL volume by starting all volumes in the disk group:

```
# vxvol -g sybdata_101 startall
```

Setting up the Replicated Volume Group (RVG) on the primary site

Before creating the RVG on the primary site, make sure the volumes and CVM group are active and online.

To review the status of replication objects on the primary site

1 Verify the volumes you intend to include in the group are active.

2 Review the output of the `hagrp -state cvm` command to verify that the CVM group is online.

3 On each site, verify vradmin is running:

```
#  ps -ef |grep vradmin
    root  536594  598036   0 12:31:25      0  0:00 grep vradmin
```

If vradmin is not running start it:

```
# vxstart_vvr
VxVM VVR INFO V-5-2-3935 Using following ports:
heartbeat: 4145
vradmind: 8199
vxrsyncd: 8989
data: Anonymous-Ports
To change, see vrport(1M) command
#  ps -ef |grep vradmin
    root  536782       1   0 12:32:47      -  0:00 /usr/sbin/vradmind
    root 1048622  598036   0 12:32:55      0  0:00 grep vradmin
# netstat -an |grep 4145
tcp4       0      0  *.4145                  *.*          LISTEN
udp4       0      0  *.4145                  *.*
```

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

To create the primary RVG

1. Determine which node is the CVM master node by entering:

   ```
   # vxdctl -c mode
   ```

2. To create the *syb_rvg* RVG, run the following on the master node:

   ```
   # vradmin -g sybdata_101 createpri syb_rvg syb_vol syb_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 *syb_vol*.

Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): setting up 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 to hold the data volume, SRL, and RVG on the storage on the secondary site. You must match the names and sizes of these volumes with the names and sizes of the volumes on the primary site.
  See "To create the disk group, volume and mount point for the datafiles" on page 199.
  See "Creating the data and SRL volumes on the secondary site" on page 294.
- Edit the /etc/vx/vras/.rdg file on the secondary site.
  See "Editing the /etc/vx/vras/.rdg files" on page 294.
- 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 295.

- Create the replication objects on the secondary site.
See "Setting up the disk group on secondary site for replication" on page 296.

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 match the sizes and names of the corresponding volumes in the primary site before you create the disk group.
- The disk group must match the size and name of the disk group at 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 Sybase ASE CE database, create a volume for data. In the example, the *syb_vol* volume on the primary site is 12 GB:

```
# vxassist -g sybdata_101 make syb_vol 12000M 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 sybdata_101 make syb_srl 1500M nmirror=2 disk4 disk6
```

Editing the /etc/vx/vras/.rdg files

Editing the /etc/vx/vras/.rdg file on the secondary site enables VVR to replicate the disk group from the primary site to the secondary site. On each node, VVR uses the /etc/vx/vras/.rdg file to check the authorization to replicate the RVG on the primary site to the secondary site. The file on each node in the secondary site must contain the primary disk group ID, and likewise, the file on each primary system must contain the secondary disk group ID.

To edit the /etc/vx/vras/.rdg files

1 On a node in the primary site, display the primary disk group ID:

```
# vxprint -l diskgroup

.....
```

2 On each node in the secondary site, edit the /etc/vx/vras/.rdg file and enter the primary disk group ID on a single line.

3 On each cluster node of the primary cluster, edit the /etc/vx/vras/.rdg file and enter the secondary disk group ID on a single line.

Setting up IP addresses for RLINKs on each cluster

Creating objects with the vradmin command requires resolvable virtual IP addresses that set network RLINK connections as host names of the primary and secondary sites.

To set up IP addresses for RLINKS on each cluster

1 Using the following command, determine whether a node is the CVM master or the slave:

```
# vxdctl -c mode
```

You must configure rlinks on the CVM master node.

2 For each RVG running on each cluster, set up a virtual IP address on one of the nodes of the cluster. These IP addresses are part of the RLINK.

The example assumes for the cluster on the primary site:

- The public network interface is bge0:1
- The virtual IP address is 10.10.9.101
- The net mask is 255.255.255.0
- ```
  # ifconfig bge0:1 plumb
  # ifconfig bge0:1 inet 10.10.9.101 netmask 255.255.255.0
  # ifconfig bge0:1 up
  ```

3 Use the same commands with appropriate values for the interface, IP address, and net mask on the secondary site.

The example assumes for the secondary site:

- The public network interface is bge0:1
  ```

- virtual IP address is 10.11.9.102
- net mask is 255.255.255.0

4 Define the virtual IP addresses to correspond to a host name in the virtual cluster on the primary site and a host name in the virtual cluster on the secondary site.

   Update the /etc/hosts file on all the nodes on both the primary and secondary sites.

   The examples assume:

   - syb_cluster101_priv has IP address 10.10.9.101
   - syb_cluster102_priv has IP address 10.11.9.102

5 Use the ping command to verify the links are functional.

Setting up the disk group on secondary site for replication

Create the replication objects on the secondary site from the master node of the primary site, using the `vradmin` command.

To set up the disk group on the secondary site for replication

1 Issue the command in the following format from the cluster on the primary site:

```
# vradmin -g dg_pri addsec rvg_pri pri_host sec_host
```

   where:

   - dg_pri is the disk group on the primary site that VVR will replicate. For example: *sybdata_101*
   - rvg_pri is the RVG on the primary site. For example: *syb_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 syb_cluster101_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 syb_cluster102_priv

   For example, the command to add the cluster on the primary site to the Replicated Data Set (RDS) is:

```
# vradmin -g sybdata_101 addsec syb_rvg syb_clus101_priv
syb_cluster102_priv
```

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_syb_clus102_priv_syb_rvg* and the "secondary" RLINK created is *rlk_syb_clus101_priv_syb_rvg*.

2 Verify the list of RVGs in the RDS by executing the following command.

```
# vradmin -g sybdata_101 -l printrvg
```

For example:

```
# vradmin -g sybdata_101 -l printrvg
Replicated Data Set: syb_rvg
Primary:
HostName: syb_cluster101_priv <localhost>
RvgName: syb_rvg
DgName: sybdata_101
datavol_cnt: 1
vset_cnt: 0
srl: syb_srl
RLinks:
name=rlk_syb_cluster102_priv_syb_rvg, detached=on,synchronous=off
Secondary:
HostName: 10.190.99.197
RvgName: syb_rvg
DgName: sybdata_101
datavol_cnt: 1
vset_cnt: 0
srl: syb_srl
RLinks:
name=rlk_syb_cluster101_syb_rvg, detached=on, synchronous=off
```

Note: Once the replication is started the value of the detached flag will change the status from ON to OFF.

Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): starting replication

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 Storage 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 sybdata_101 -a startrep syb_rvg
      syb_clus102_priv
```

Starting replication using full synchronization with Storage Checkpoint

Use the `vradmin` command with the Storage Checkpoint option to start replication using full synchronization with Storage Checkpoint.

To start replication using full synchronization with Storage 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 Storage 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 sybdata_101 -c syb_ckpt syncrvg syb_rvg
   syb_clus102_priv
   ```

2. To start replication after full synchronization, enter the following command:

   ```
   # vradmin -g sybdata_101 -c syb_ckpt startrep syb_rvg
   syb_clus102_priv
   ```

Verifying replication status

Verify that replication is properly functioning.

To verify replication status

1. Check the status of VVR replication:

   ```
   # vradmin -g disk_group_name repstatus rvg_name
   ```

2 Review the `flags` output for the status. The output may appear as `connected` and `consistent`. For example:

```
# vxprint -g sybdata_101 -l rlk_syb_cluster102_pri_syb_rvg
  Rlink: rlk_syb_cluster102_pri_syb_rvg
  info: timeout=500 packet_size=8400 rid=0.1078
      latency_high_mark=10000 latency_low_mark=9950
      bandwidth_limit=none
  state: state=ACTIVE
      synchronous=off latencyprot=off srlprot=autodcm
  .
  .
  protocol: TCP/IP
  checkpoint: syb_ckpt
  flags: write enabled attached consistent connected
 asynchronous
```

Configuring a global SF Sybase CE cluster using Veritas Volume Replicator (VVR): configuring cluster resources

After configuring both clusters for global clustering and setting up the Sybase ASE CE database for replication, configure VCS to provide high availability for the database. Specifically, configure VCS agents to control the cluster resources, including the replication resources.

To view the sample main.cf files on your system:

```
# cd /etc/VRTSagents/ha/conf/Sybase/
```

```
# ls cvmvvr*
```

The following sample main.cf files illustrate the VCS configuration changes after setting up an existing Sybase ASE CE database for replication:

See “Sample main.cf for a primary CVM VVR site” on page 387.

See “Sample main.cf for a secondary CVM VVR site” on page 393.

Note: The example procedures illustrate the configuration process using a manual file editing method. If you are using the Java Console, some steps do not apply in the same order.

About modifying the VCS configuration for replication

The following resources must be configured or modified for replication:

Table 24-1 Cluster resources required for replication

Cluster resources	Configuration required
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 408.
RVGSharedPri resource	Add the RVGSharedPri resource to the existing Sybase ASE CE database service group. The CVMVolDg resource must be removed from the existing Sybase ASE CE database service group.

Table 24-1 Cluster resources required for replication *(continued)*

Cluster resources	Configuration required
Sybase ASE CE database service group	The existing Sybase ASE CE database service group is a parallel group consisting of the Sybase ASE CE database resource, CVMVolDg resource, and CFSMount resource (if the database resides in a cluster file system). Define the Sybase ASE CE service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.

For detailed examples of service group modification:

See "Configuration examples before and after modification" on page 302.

For more information on service replication resources:

See the *Veritas™ Cluster Server Bundled Agents Reference Guide*.

Configuration examples before and after modification

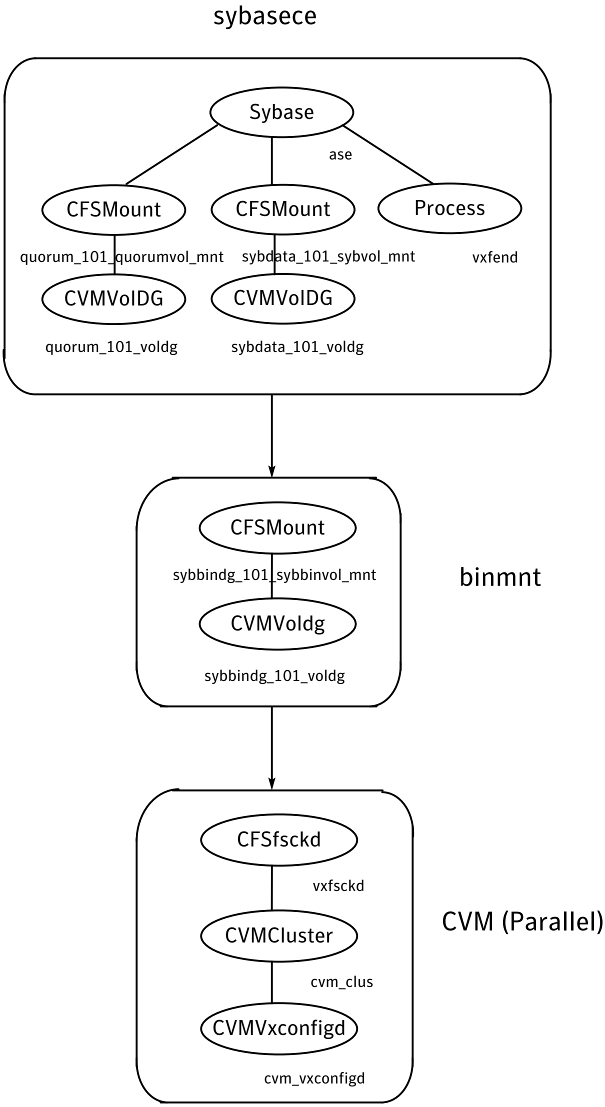
Review the following illustrations that display the changes to the VCS configuration, after setting up replication on the existing Sybase ASE CE database.

- Configuration before modification:
  Figure 24-1
- Configuration after modification:
  Figure 24-2

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.

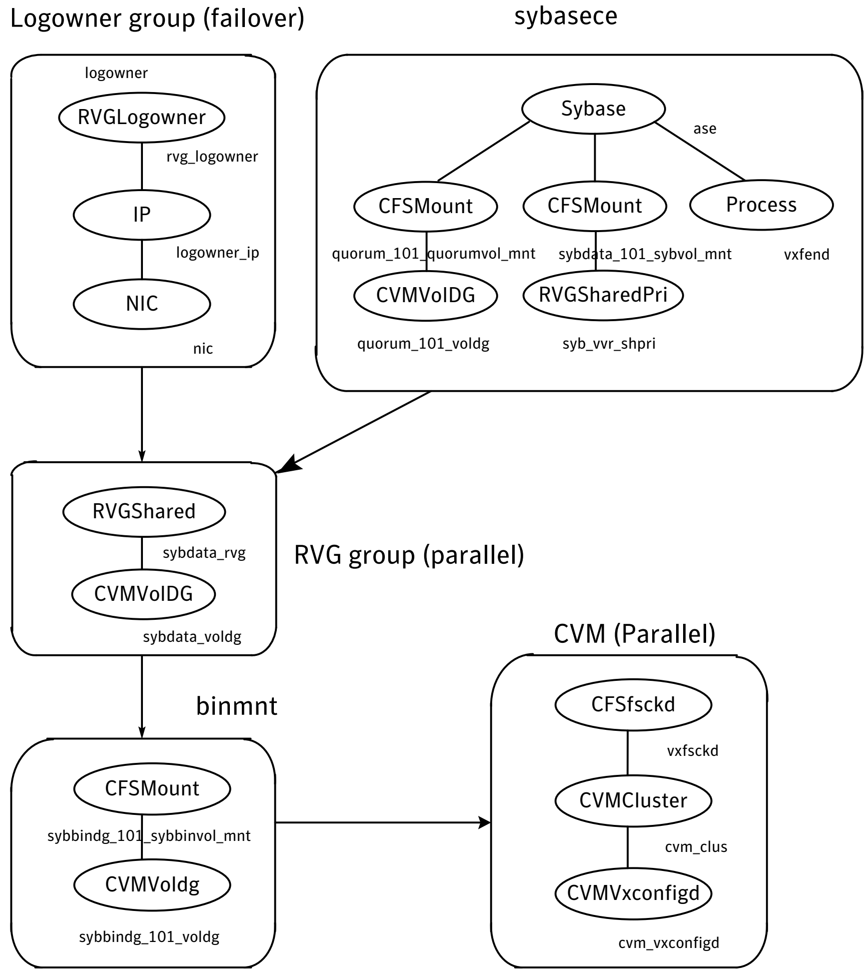
Configuration before modification for replication:

Figure 24-1 Illustration of dependencies before modification for replication



Configuration after modification for replication:

Figure 24-2 Illustration of dependencies after modification for replication



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 Sybase ASE CE 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 Sybase ASE CE database service group to the newly created RVG group.

Note: The example procedure illustrates the configuration process using a manual file editing method. If you are using the Java Console, some steps do not apply in the same order.

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 Sybase CE installation.

   See "Sample main.cf for a primary CVM VVR site" on page 387.

   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 = { system1 = 0, system2 = 1 }
       AutoStartList = { system1,system2 }
       )
   ```

```
    IP logowner_ip (
        Device = bge0
        Address = "10.10.9.101"
        NetMask = "255.255.255.0"
        )

    NIC nic (
        Device = bge0
        NetworkType = ether
        )

 RVGLogowner logowner (
     RVG = syb_rvg
     DiskGroup = sybdata_101
     )
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 = { system1 = 0, system2 = 1 }
     Parallel = 1
     AutoStartList = { system1,system2 }
     )

RVGShared sybdata_rvg (
     RVG = syb_rvg
     DiskGroup = sybdata_101
     )
     CVMVolDg sybdata_voldg (
         CVMDiskGroup = sybdata_101
         CVMActivation = sw
         )
requires group cvm online local firm
sybdata_rvg requires sybdata_voldg
```

6 Modify the Sybase ASE CE service group using the appropriate values for your cluster and nodes:

- Define the Sybase ASE CE 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 attribute in bold in the example that follows.

  Note: This action must be performed on the primary or secondary site, but not on both.

  Note: If you are using the Java Console, the secondary cluster must be configured before you can configure a service group as a global group.

- Add the ClusterFailOverPolicy cluster attribute. Symantec recommends using the Manual value. See the attribute in bold 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.

The following is an example of an Sybase ASE CE database service group configured for replication:

```
group sybasece (
    SystemList = { system1 = 0, system2 = 1 }
    ClusterList = { syb_cluster101 = 0, syb_cluster102 = 1 }
    Parallel = 1
    ClusterFailOverPolicy = Manual
    Authority = 1
    AutoStartList = { system1,system2 }
    OnlineRetryLimit = 3
    TriggerResStateChange = 1
    OnlineRetryInterval = 120
    )

    CFSMount sybdata_101_syb_vol_mnt (
        MountPoint = "/sybdata"
        BlockDevice = "/dev/vx/dsk/sybdata_101/syb_vol"
        )

    RVGSharedPri syb_vvr_shpri (
       RvgResourceName = sybdata_rvg
```

```
            OnlineRetryLimit = 0
            )

        Process vxfend (
            PathName = "/sbin/vxfend"
            Arguments = "-m sybase -k /tmp/vcmp_socket"
            )

Syabase ase (
    Sid @system1 = ase1
    Sid @system2 = ase2
    Owner = sybase
    Home = "/sybase"
    Version = 15
    SA = sa
    Quorum_dev = "/quorum/q.dat"
    )
requires group RVGgroup online local firm
sybdata_101_syb_vol_mnt requires syb_vvr_shpri
ase requires vxfend
ase requires sybdata_101_syb_vol_mnt
ase requires quorum_101_quorumvol_mnt
quorum_101_quorumvol_mnt requires quorum_101_voldg
```

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 Sybase ASE CE 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.

Note: The example precedure illustrates the confguration process using a manual file editing method. If you are using the Java Console, some steps do not apply in the same order.

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 Sybase CE installation to see the CVM configuration.

   See “Sample main.cf for a secondary CVM VVR site” on page 393.

   In our example, the secondary site has syb_cluster102 consisting of the nodes system3 and system4. 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 = { system3 = 0, system4 = 1 }
    AutoStartList = { system3, system4 }
    )

    IP logowner_ip (
       Device = bge0
       Address = "10.11.9.102"
       NetMask = "255.255.255.0"
       )

NIC nic (
       Device = bge0
       NetworkType = ether
       )

   RVGLogowner logowner (
       RVG = syb_rvg
       DiskGroup = sybdata_101
       )

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 = { system3 = 0, system4 = 1 }
    Parallel = 1
    AutoStartList = { system3, system4 }
    )

RVGShared sybdata_rvg (
    RVG = syb_rvg
    DiskGroup = sybdata_101
    )

    CVMVolDg sybdata_voldg
        CVMDiskGroup = sybdata_101
        CVMActivation = sw
        )
requires group cvm online local firm
sybdata_rvg requires sybdata_voldg
```

7 Add an Sybase ASE CE service group. Use the Sybase ASE CE service group on the primary site as a model for the Sybase ASE CE service group on the secondary site.

- Define the Sybase ASE CE service group as a global group by specifying the clusters on the primary and secondary sites as values for the ClusterList group attribute.

  Note: This action must be performed on the primary or secondary site, but not on both.

- Assign this global group the same name as the group on the primary site; for example, sybasece.
- 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 Sybase ASE CE group on the secondary site:

```
.
group sybase (
    SystemList = { system3 = 0, system4 = 1 }
    ClusterList = { syb_cluster102 = 0, syb_cluster101 = 1 }
    Parallel = 1
    OnlineRetryInterval = 300
    ClusterFailOverPolicy = Manual
    Authority = 1
  # AutoStart = 0 here so faulting will not happen
    AutoStartList = { system3, system4 }
    )

    CFSMount sybdata_101_syb_vol_mnt (
        MountPoint = "/sybdata"
        BlockDevice = "/dev/vx/dsk/sybdata_101/syb_vol"
        )

RVGSharedPri syb_vvr_shpri (
        RvgResourceName = sybdata_rvg
        OnlineRetryLimit = 0
        )

         CFSMount quorum_101_quorumvol_mnt (
             MountPoint = "/quorum"
             BlockDevice = "/dev/vx/dsk/quorum_101/quorumvol"
             )

         CVMVolDg quorum_101_voldg (
             CVMDiskGroup = quorum_101
             CVMVolume = { quorumvol }
             CVMActivation = sw
             )

Sybase ase (
     Sid @system3 = ase1
     Sid @system4 = ase2
     Owner = sybase
     Home = "/sybase"
     Version = 15
```

```
          SA = sa
          Quorum_dev = "/quorum/q.dat"
          )
requires group RVGgroup online local firm
sybdata_101_syb_vol_mnt requires syb_vvr_shpri
ase requires vxfend
ase requires sybdata_101_syb_vol_mnt
ase requires quorum_101_quorumvol_mnt
quorum_101_quorumvol_mnt requires quorum_101_voldg
```

8 Save and close the `main.cf` file.

9 Use the following command to verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file:

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

10 Stop and restart VCS.

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

Wait for port h to stop on all nodes, and then restart VCS with the new configuration on all primary nodes:

```
# hastart
```

11 Verify that VCS brings all resources online. On one node, enter the following command:

```
# hagrp -display
```

The Sybase ASE CE, RVG, and CVM groups are online on both nodes of the primary site. The RVGLogOwner and ClusterService groups are 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 Sybase ASE CE group which must be offline.

12 Verify the service groups and their resources that are brought online. On one node, enter the following command:

```
# hagrp -display
```

The Sybase ASE CE service group is offline on the secondary site, but the ClusterService, CVM, RVG log owner, and RVG groups are online.

This completes the setup for an SF Sybase CE global cluster using VVR for replication. Symantec recommends testing a global cluster before putting it into production.

Configuring the Sybase ASE CE cluster on the secondary site

Before bringing Sybase ASE CE online at the secondary site, you must configure the Sybase ASE CE cluster on the secondary site.

To configure Sybase ASE CE cluster on the secondary site

1 Modify the the Sybase ASE CE configuration files to match the secondary site environment.

2 When replication is complete, suspend replication.

3 Mount the corresponding file system at the secondary site.

4 Install and configure the Sybase ASE CE binaries:

See "Before installing Sybase ASE CE" on page 195.

Note: The quorum device must be on non-replicated shared storage.

---

5 Copy the the following from the primary to the secondary site:

- interfaces

- configuration file (ase.cfg)
- inp files (QIase*****.inp)
- RUN files

After copying, edit them to reflect the secondary site environment.

6 Start the database once manually before proceeding to bring it under VCS control. You must rebuild the quorum as well as copy the cluster ID of the datafile to the quorum on secondary site. This is needed only for the first time you bring the database online on the secondary site.

Use the following command:

```
# su - sybase; source $SYBASE/SYBASE.sh; /$SYBASE/ASE-15_0/bin/ \
dataserver --instance=blue1 -Q /qrmmnt/qrm -F \
/sybase_home/QIblueclus19442.inp \
--buildquorum=force --create-cluster-id=quorum
```

If you do not perform this task, you will receive the following error on the secondary site:

```
Unique cluster id on quorum device does not match master device.
You may be using the wrong master device. If this is the correct
master, pass 'create-cluster-id' on the command line to pair the
devices.
```

The buildquorum is required to reflect the secondary site settings for the Sybase database.

7. Configure the VCS service groups for the database.

   See "Configuring a Sybase ASE CE cluster under VCS control using the SF Sybase CE installer" on page 206.

   Verify that all VCS service groups are online.

   For sample configurations:

   See "Sample main.cf for a primary CVM VVR site" on page 387.

   aSee "Sample main.cf for a secondary CVM VVR site" on page 393.

   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.

8. Stop the Sybase ASE service group on the secondary site, unmount the file system, and establish replication.

Note: Make sure the private interconnects which are used for the Sybase ASE CE cluster on the secondary site are also plumbed and pingable amongst the nodes.

Managing a global SF Sybase CE cluster using Veritas Volume Replicator (VVR)

For information on using the VCS commands for global clusters:

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

If you have two SF Sybase CE clusters configured to use VVR for replication, the following administrative functions are available:

Table 24-2

Migration of the role of the primary site to the remote site	Migration of the role of the primary site to the remote site 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.

Table 24-2 *(continued)*

Takeover of the primary site role by the secondary site	Takeover of the primary site role by the secondary site 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.

VCS agents 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.

Table 24-3

VCS replication agents bundled with VVR	Description
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.

VCS provides agents for other array-based or application-based solutions.For more information about the RVG and RVGPrimary agents.

See the *Veritas™ Cluster Server Bundled Agents Reference Guide*.

Note: The RVGSnapshot agent is not supported for SF Sybase CE.

Migrating the role of primary site to the secondary site

After configuring the replication objects within VCS, you can use VCS commands to migrate the role of the cluster on the primary site to the remote cluster. In the procedure below, VCS takes the replicated database service group, *database_grp*, offline on the primary site and brings it online on the secondary site; the secondary site now assumes the role of the primary site.

Note: The `hagrp -switch` command cannot migrate a parallel group within a cluster or between clusters in a global cluster environment.

To migrate the role of primary site to the remote site

1. From the primary site, use the following command to take the Sybase service group offline on all nodes.

   ```
   # hagrp -offline database_grp -any
   ```

   Wait for VCS to take all Sybase service groups offline on the primary site.

2. Verify that the RLINK between the primary and secondary is up to date. Use the `vxrlink -g` command with the status option and specify the RLINK for the primary cluster. You can use the command from any node on the primary cluster.

   For example:

   ```
   # vxrlink -g data_disk_group status rlk_syb_cluster102_priv_syb_rvg
   ```

   Where rlk_syb_cluster101_priv_*syb_rvg* is the RLINK.

3. On the secondary site, which is now the new primary site, bring the Sybase service group online on all nodes:

   ```
   # hagrp -online database_grp -any
   ```

After migrating the role of the primary site to the secondary site, you can use VCS commands to migrate the role of the cluster on the new primary site to the original primary site. In the procedure below, VCS takes the replicated database service group, *database_grp*, offline on the new primary (former secondary) site and brings it online on the original primary site; the original primary site now resumes the role of the primary site.

Note: The `hagrp -switch` command cannot migrate a parallel group within a cluster or between clusters in a global cluster environment.

To migrate the role of new primary site back to the original primary site

1. Make sure that all Sybase resources are online, and switch back the group *database_grp* to the original primary site.

   Issue the following command on the remote site:

   ```
   # hagrp -offline database_grp -any
   ```

2. Verify that the RLINK between the primary and secondary is up to date. Use the `vxrlink -g` command with the status option and specify the RLINK for the primary cluster. You can use the command from any node on the current primary cluster.

   For example:

   ```
   # vxrlink -g data_disk_group status rlk_syb_cluster101_priv_syb_rvg
   ```

   Where *rlk_syb_cluster101_priv_syb_rvg* is the RLINK.

3. Make sure that *database_grp* is offline on the new primary site. Then, execute the following command on the original primary site to bring the *database_grp* online:

   ```
   # hagrp -online database_grp -any
   ```

Taking over the primary role by the remote cluster

Takeover occurs when the remote cluster on the secondary site starts the application that uses replicated data. This situation may occur if the secondary site perceives the primary site as dead, or when the primary site becomes inaccessible (perhaps for a known reason). For a more detailed description of concepts of taking over the primary role:

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

Before enabling the secondary site to take over the primary role, the administrator on the secondary site must "declare" the type of failure at the remote (primary, in this case) site and designate the failure type using one of the options for the `haclus` command.

Table 24-4 Options for the remote cluster to take over the primary role

Takeover options	Description
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.
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".

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 syb_cluster101
   ```

2. After declaring the state of the remote cluster, bring the *database_grp* service group online on the secondary site. For example:

   ```
   # hagrp -online -force database_grp -any
   ```

To resynchronize after an outage

1. On the original primary site, create a snapshot of the RVG before resynchronizing it in case the current primary site fails during the resynchronization. Assuming the disk group is *data_disk_group* and the RVG is *syb_rvg*, type:

   ```
   # vxrvg -g data_disk_group -F snapshot syb_rvg
   ```

   See the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide* for details on RVG snapshots.

2. Resynchronize the RVG. From any 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 syb_vvr_shpri fbsync -sys system3
   ```

3. Perform one of the following commands, depending on whether the resynchronization of data from the current primary site to the original primary site is successful:

   - If the resynchronization of data is successful, use the `vxrvg` command with the `snapback` option to reattach the snapshot volumes on the original primary site to the original volumes in the specified RVG:

     ```
     # vxrvg -g data_disk_group snapback syb_rvg
     ```

   - A failed attempt at the resynchronization of data (for example, a disaster hits the primary RVG when resynchronization is in progress) could generate inconsistent data.

You can restore the contents of the RVG data volumes from the snapshot taken in step 1:

```
# vxrvg -g data_disk_group snaprestore syb_rvg
```

Troubleshooting Veritas Volume Replicator (VVR) components of SF Sybase CE

If the rlink is not up to date, use the `hares -action` command with the `resync` action token to synchronize the RVG.

To update the rlink

- Enter the following command example on any node in the primary cluster, specifying the RVGSharedPri resource:

  ```
  # hares -action syb_vvr_shpri resync -sys system1
  ```

Section 8

Uninstallation of SF Sybase CE

Chapter 25

Preparing to uninstall SF Sybase CE from a cluster

This chapter includes the following topics:

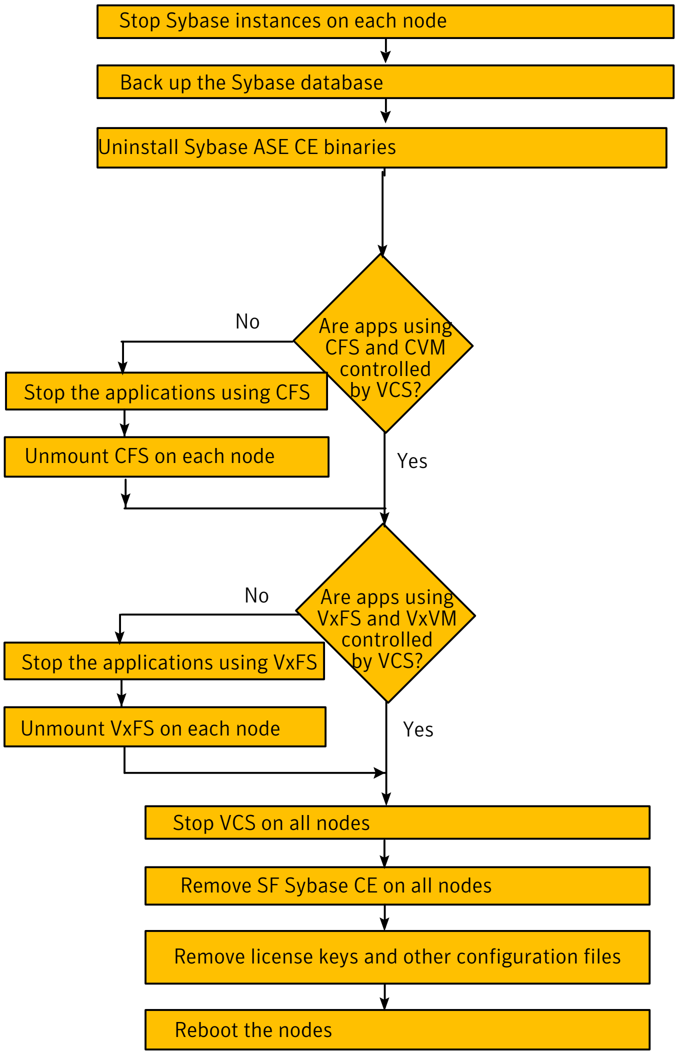
About uninstalling SF Sybase CE from a cluster

You can uninstall SF Sybase CE using the uninstallsfsybasece.

Note: After you uninstall SF Sybase CE, you cannot access the Sybase database as Veritas Volume Manager and Veritas File System are uninstalled from the cluster. Make sure that you back up the Sybase database before you uninstall SF Sybase CE.

Figure 25-1 illustrates the steps that are required to uninstall SF Sybase CE from a cluster.

Figure 25-1 SF Sybase CE uninstallation



Options for uninstalling SF Sybase CE

Table 25-1 lists the available options for uninstalling SF Sybase CE:

Table 25-1 Options for uninstalling SF Sybase CE

Options	Description
SF Sybase CE uninstallation program	Use the uninstallsfsybasece program to uninstall SF Sybase CE.
Response file	Use a response file to automate or perform an unattended uninstallation of SF Sybase CE. See "Uninstalling SF Sybase CE using a response file" on page 339.

Preparing to uninstall SF Sybase CE from a cluster

Perform the steps in the following procedure before you uninstall SF Sybase CE from a cluster.

To prepare to uninstall SF Sybase CE from a cluster

1. Stop applications that use the Sybase ASE CE database.

   See "Stopping applications that use the Sybase database" on page 328.

2. Stop Sybase instances.

   See "Stopping Sybase instances" on page 328.

3. Back up the Sybase database.

   See "Backing up the Sybase database" on page 329.

4. Uninstalling Sybase ASE CE (optional)

   See "Uninstalling Sybase ASE CE (optional)" on page 329.

5. Remove root disk encapsulation.

   See "Removing root disk encapsulation" on page 330.

6. Stop the applications that use CFS (outside of VCS control).

   See "Stopping the applications that use CVM or CFS (outside of VCS control)" on page 331.

7. Unmount CFS file systems (outside of VCS control).

   See "Unmounting CFS file systems (outside of VCS control)" on page 331.

8. Stop VCS.

   See "Stopping VCS" on page 332.

9 Stop the applications that use VxFS (outside of VCS control).

See “Stopping the applications that use VxVM or VxFS (outside of VCS control)” on page 332.

10 Unmount VxFS file systems (outside of VCS control).

See “Unmounting VxFS file systems (outside of VCS control)” on page 333.

Stopping applications that use the Sybase database

Stop the applications that are dependent on service groups that contain Sybase resources.

To stop applications that use the Sybase database

1 Review the dependencies between service groups:

```
# hagrp -dep
```

2 Stop the service groups on each node:

```
# hagrp -offline app_group -sys node_name
```

Stopping Sybase instances

You need to stop Sybase CE and the Sybase instances on the cluster nodes where you want to uninstall SF Sybase CE. Before you stop the Sybase instances, stop the applications that are dependent on the service groups that contain Sybase.

The procedure in this section provides instructions to stop the instances on a two-node cluster; the nodes are system1 and system2. Depending on the VCS configuration, the procedure to stop Sybase instances may vary.

To stop Sybase instances

1 Log in as the superuser on one of the nodes in the cluster.

2 On each node, take the Sybase resources in the VCS configuration file (main.cf) offline.

```
# hagrp -offline Sybase_group -sys node_name
```

For example:

```
# /opt/VRTSvcs/bin/hagrp -offline sybasece -sys system1

# /opt/VRTSvcs/bin/hagrp -offline sybasece -sys system2
```

These commands stop the Sybase resources under VCS control.

3 Verify that the state of the Sybase and CVM service groups are offline and online respectively.

```
# /opt/VRTSvcs/bin/hagrp -state
Group       Attribute             System     Value
binmnt       State                 system1     |ONLINE|
binmnt       State                 system2     |ONLINE|
cvm          State                 system1     |ONLINE|
cvm          State                 system2     |ONLINE|
sybasece     State                 system1     |OFFLINE|
sybasece     State                 system2     |OFFLINE|
```

Backing up the Sybase database

If you plan to retain the Sybase database, you must back up the Sybase database.

For instructions on backing up the Sybase database, see the Sybase documentation.

Uninstalling Sybase ASE CE (optional)

Uninstall Sybase ASE CE before uninstalling SF Sybase CE. For information about the Sybase ASE CE uninstall utility, see the Sybase ASE CE product documentation.

To uninstall Sybase ASE CE

1. Log in as the Sybase user.

   Note: In case of CFS binary installation, log in to any node. In case of Sybase ASE CE binary installation on local VxFS, you must uninstall from each node in cluster.

   ---

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 uninstall utility.

   ```
   # /cd $SYBASE_HOME/sybuninstallASESuite/uninstall
   ```

4. Run `uninstall`.

   ```
   # ./uninstall
   ```

Removing root disk encapsulation

Perform this step only if you plan to remove the VxVM and VVR packages.

If you have VxVM and VVR installed, you need to indicate to the installer whether or not you want to remove the VxVM packages from all nodes in the cluster. If you want to remove these packages, you need to ensure that the root disk is not encapsulated. The uninstallation fails if you choose to remove these packages while the root disk is encapsulated.

The root disk is under VxVM control if `/dev/vx/dsk/rootdg/rootvol` is listed as being mounted as the root (/) file system. If so, unmirror and unencapsulate the root disk as described in the following procedure.

To remove root disk encapsulation

1. Use the vxplex command to remove all the plexes of the volumes rootvol, swapvol, usr, var, opt and home that are on disks other than the root disk.

   For example, the following command removes the plexes mirrootvol-01, and mirswapvol-01 that are configured on a disk other than the root disk:

   ```
   # vxplex -o rm dis mirrootvol-01 mirswapvol-01
   ```

   Note: Do not remove the plexes on the root disk that correspond to the original disk partitions.

   ---

2. Convert all the encapsulated volumes in the root disk to make them accessible directly through disk partitions instead of through volume devices. There must be at least one other disk in the rootdg disk group in addition to the root disk for vxunroot to succeed.

   ```
   # /etc/vx/bin/vxunroot
   ```

3. To check if the root disk is unencapsulated:

   ```
   # df -v /
   ```

   Following the removal of encapsulation, the system is restarted from the unencapsulated root disk.

Stopping the applications that use CVM or CFS (outside of VCS control)

You need to stop the applications that use CVM volumes or CFS mount points not controlled by VCS.

To stop the applications that use CVM or CFS (outside of VCS control)

1. Stop the applications that use a CFS mount point. The procedure varies for different applications. Use the procedure appropriate for the application.
2. Verify that no processes use the CFS mount point:

   ```
   # fuser -c mount_point
   ```

Unmounting CFS file systems (outside of VCS control)

You need to unmount CFS file systems that are not under VCS control on all nodes.

To unmount CFS file systems not under VCS control

1. Determine the file systems that need to be unmounted by checking the output of the mount command. The command lists all the mounted clustered file systems. Consult the main.cf file for identifying the files that are under VCS control.

   ```
   # mount -v | grep vxfs | grep cluster
   ```

2. Unmount each file system that is not controlled by VCS:

   ```
   # umount mount_point
   ```

Stopping VCS

Stop VCS to take the service groups on all nodes offline.

To stop VCS

1. Log in as the superuser on one of the cluster nodes.
2. Stop VCS on all nodes:

   ```
   # hastop -all
   ```

3. Verify the output of the `gabconfig -a` command to ensure that VCS has been stopped.

   In this command output, the VCS engine or high availability daemon (HAD) port h is not displayed. This output indicates that VCS has been stopped.

   ```
   # /sbin/gabconfig -a
   GAB Port Memberships
   ===============================================================
   Port a gen 5c3d0b membership 01
   Port b gen 5c3d10 membership 01
   ```

Stopping the applications that use VxVM or VxFS (outside of VCS control)

You need to stop all applications that use VxVM volumes or VxFS mount points not under VCS control.

To stop the applications that use VxVM or VxFS (outside of VCS control)

1 Stop the applications that use a VxFS mount point. The procedure varies for different applications. Use the procedure that is appropriate for your application.

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/vfstab directory.

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
```

Uninstalling SF Sybase CE from a cluster

This chapter includes the following topics:

Uninstalling SF Sybase CE from a cluster

You can remove the SF Sybase CE packages from all nodes in the SF Sybase CE cluster using the uninstallsfsybasece. The uninstallsfsybasece can be accessed from the product disc or from the `/opt/VRTS/install` directory.

Perform the steps in the following procedure to remove SF Sybase CE from a cluster.

To remove SF Sybase CE from a cluster

1 Remove the SF Sybase CE packages. You can remove the packages using the uninstallation program or using the response file.

  Using the uninstallation program:

  See "Removing the SF Sybase CE packages" on page 336.

  Using the response file:

  See "Uninstalling SF Sybase CE using a response file" on page 339.

2 Remove other configuration files (optional).

  See "Removing other configuration files (optional)" on page 338.

3 Reboot the nodes.

```
# shutdown -g0 -y -i6
```

Removing the SF Sybase CE packages

The uninstallsfsybasece 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 Sybase CE packages.
- Removes the language packages, if installed.

Note: The following directories remain after uninstallation: `/opt/VRTS`, `/opt/VRTSperl`, `/etc/VRTSvcs`, `/var/VRTSvcs`. They contain logs and configuration information for future reference. You may or may not remove them.

To remove the SF Sybase CE packages

1 Log in as the superuser on any node in the cluster.

2 Navigate to the directory that contains the uninstallsfsybasece:

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

3 Start the uninstallsfsybasece:

```
# ./uninstallsfsybasece [-rsh]
```

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

4 If you have VxVM installed, indicate whether or not you want to remove the VxVM packages from all nodes in the cluster. Enter **y** only if the root disk is outside of VxVM control.

The uninstallsfsybasece performs the following tasks:

- Checks the operating system on each node
- Verifies the system-to-system communication
- Verifies the licenses
- Checks for the SF Sybase CE 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 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.

6 To check if the root disk is under VxVM control:

```
# df -v /
```

The root disk is under VxVM control if /dev/vx/dsk/rootvol is listed as being mounted as the root (/) file system. If so, unmirror and unencapsulate the root disk as described in the following

- Use the vxplex command to remove all the plexes of the volumes rootvol, swapvol, usr, var, opt and home that are on disks other than the root disk.

  For example, the following command removes the plexes mirrootvol-01, and mirswapvol-01 that are configured on a disk other than the root disk:

  ```
  # vxplex -o rm dis mirrootvol-01 mirswapvol-01
  ```

  Note: Do not remove the plexes on the root disk that correspond to the original disk partitions.

- Convert all the encapsulated volumes in the root disk to make them accessible directly through disk partitions instead of through volume devices. There must be at least one other disk in the rootdg disk group in addition to the root disk for vxunroot to succeed.

  ```
  # /etc/vx/bin/vxunroot
  ```

  Following the removal of encapsulation, the system is restarted from the unencapsulated root disk.

7. If you invoked the uninstallsfsybasece from a remote system in the same subnet, enter the name of the systems from which you want to uninstall SF Sybase CE.

   If you invoked the uninstallsfsybasece from a node in the SF Sybase CE cluster, review the cluster information and confirm to uninstall SF Sybase CE.

   The uninstallsfsybasece performs the following task:

   - Checks the operating system on each node
   - Verifies the system-to-system communication
   - Verifies the licenses
   - Checks for the SF Sybase CE 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.

8. Confirm to uninstall SF Sybase CE.

   The program performs the following tasks:

   - Stops the agents and performs verifications on each node to proceed with uninstallation
   - Stops the SF Sybase CE processes and uninstalls the SF Sybase CE packages
   - Displays the location of the uninstallation summary, response file, and log files for reference.

Removing other configuration files (optional)

You can remove the Veritas configuration files and the packages that are left after running the uninstallsfsybasece.

To remove residual Veritas configuration files (optional)

1 List all VRTS packages that can be removed.

```
# pkginfo -l |grep -i vrts
```

2 Run the `pkgrm pkgname` command to remove the remaining VRTS packages.

3 Move the residual Veritas configuration files to the `vrts.bkp` directory:

```
# cd /var
# mkdir vrts.bkp
# mv *VRTS* vrts.bkp
# mv vx vrts.bkp
# cd /var/opt
# mkdir vrts.bkp
# mv *VRTS* vrts.bkp
# cd /opt
# mkdir vrts.bkp
# mv *VRTS* vrts.bkp
# cd /etc
# mkdir vrts.bkp
# mv vx *llt* *fen* *gab* *vcs* vrts.bkp
```

You can remove the vrts.bkp directories at a later time.

Uninstalling SF Sybase CE using a response file

Perform the steps in the following procedure to uninstall SF Sybase CE using a response file.

To uninstall SF Sybase CE using a response file

1 Make sure that you have completed the pre-uninstallation tasks.

2 Create a response file using one of the available options.

For information on various options available for creating a response file:

See "About response files" on page 217.

Note: You must replace the host names in the response file with that of the systems from which you want to uninstall SF Sybase CE.

For a sample response file:

See "Sample response file for uninstalling SF Sybase CE" on page 341.

3 Navigate to the directory containing the SF Sybase CE uninstallation program:

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

4 Start the uninstallation:

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

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

5 Reboot the nodes:

```
# shutdowm -g0 -y -i6
```

6 Optionally, remove residual configuration files, if any.

See "Removing other configuration files (optional)" on page 338.

Response file variables to uninstall SF Sybase CE

Table 26-1 lists the response file variables that you can define to uninstall SF Sybase CE.

Table 26-1 Response file variables specific to uninstalling SF Sybase CE

Variable	List or Scalar	Description
CFG{opt}{uninstall}	Scalar	Uninstalls SF Sybase CE packages. (Required)
CFG{systems}	List	List of systems on which the product is to be uninstalled. (Required)
CFG{prod}	Scalar	Defines the product to be uninstalled. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)

Table 26-1 Response file variables specific to uninstalling SF Sybase CE *(continued)*

Variable	List or Scalar	Description
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for uninstalling SF Sybase CE

The following sample response file uninstalls SF Sybase CE from nodes, galaxy and nebula.

```
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="SFSYBASECE60";
$CFG{systems}=[ qw(galaxy nebula) ];

1;
```

Rebooting the nodes

Reboot each node after you uninstall SF Sybase CE:

```
# shutdown -g0 -y -i6
```

Section 9

Installation reference

SF Sybase CE installation packages

This appendix includes the following topics:

- SF Sybase CE installation packages

SF Sybase CE installation packages

Table A-1 lists the package name and contents for each SF Sybase CE package.

Table A-1 List of SF Sybase CE packages

package	Content	Configuration
VRTSgab	Depends on VRTSllt. Contains the binaries for Veritas Cluster Server group membership and atomic broadcast services.	Minimum
VRTSllt	Contains the binaries for Veritas Cluster Server low-latency transport.	Minimum
VRTSamf	Contains the binaries for the Veritas Asynchronous Monitoring Framework kernel driver functionality for the process and mount based agents.	Minimum
VRTSperl	Contains Perl for Veritas.	Minimum
VRTSspt	Contains the binaries for Veritas Software Support Tools.	Recommended

Table A-1 List of SF Sybase CE packages *(continued)*

package	Content	Configuration
VRTSvcs	Depends on VRTSvxfen, VRTSgab, and VRTSllt. Contains the following components: ■ Contains the binaries for Veritas Cluster Server. ■ Contains the binaries for Veritas Cluster Server manual pages. ■ Contains the binaries for Veritas Cluster Server English message catalogs. ■ Contains the binaries for Veritas Cluster Server utilities. These utilities include security services.	Minimum
VRTSvcsag	Depends on VRTSvcs. Contains the binaries for Veritas Cluster Server bundled agents.	Minimum
VRTSvcsea	Required for VCS with the high availability agent for Sybase. VRTSvcsea contains the binaries for Veritas high availability agents for DB2, Sybase, and Oracle.	Recommended
VRTSvlic	Contains the binaries for Symantec License Utilities.	Minimum
VRTSvxfen	Depends on VRTSgab. Contains the binaries for Veritas I/O fencing.	Minimum
VRTScavf	Veritas Cluster Server Agents for Storage Foundation Cluster File System	Minimum
VRTSfssdk	Veritas File System Software Developer Kit For VxFS APIs, the package contains the public Software Developer Kit (SDK), which includes headers, libraries, and sample code. The SDK is required if some user programs use VxFS APIs.	All
VRTSglm	Veritas Group Lock Manager for Storage Foundation Cluster File System	Minimum
VRTSob	Veritas Enterprise Administrator	Recommended
VRTSvxfs	Veritas File System binaries	Minimum

Table A-1 List of SF Sybase CE packages *(continued)*

package	Content	Configuration
VRTSvxvm	Veritas Volume Manager binaries	Minimum
VRTSaslapm	Volume Manager ASL/APM	Minimum
VRTSsfcpi60	Veritas Storage Foundation Common Product Installer The Storage Foundation Common Product installer package contains the scripts that perform the following functions: installation, configuration, upgrade, uninstallation, adding nodes, and removing nodes. You can use this script to simplify the native operating system installations, configurations, and upgrades.	Minimum
VRTSsfmh	Veritas Storage Foundation Managed Host	Recommended
VRTSfsadv	Veritas File System Advanced Features by Symantec	Minimum

Appendix B

Installation scripts

This appendix includes the following topics:

- About installation scripts
- Installation script options
- About using the postcheck option

About installation scripts

Veritas Storage Foundation and High Availability Solutions products 6.0 provides several installation scripts. You can find these scripts at the root of the product media in the scripts directory.

An alternative to the `installer` script is to use a product-specific installation script. If you obtained a Veritas product from the Symantec download site, which does not include the installer, use the appropriate product installation script.

The following product installation scripts are available:

Veritas Cluster Server (VCS)	`installvcs`
Veritas Storage Foundation (SF)	`installsf`
Veritas Storage Foundation and High Availability (SFHA)	`installsfha`
Veritas Storage Foundation Cluster File System High Availability (SFCFSHA)	`installsfcfsha`
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`
Veritas Storage Foundation for Sybase ASE CE (SF Sybase CE)	`installsfsybasece`

Veritas Volume Manager	`installvm`
Veritas File System	`installfs`
Veritas Dynamic Multi-pathing	`installdmp`
Symantec VirtualStore	`installsvs`

To use the installation script, enter the script name at the prompt. For example, to install Veritas Storage Foundation, type `./installsf` at the prompt.

Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

To stop the processes

- Use the `-stop` option to stop the product installation script.

  For example, to stop the product's processes, enter the following command:

  ```
  # ./installer -stop
  ```

To start the processes

- Use the `-start` option to start the product installation script.

  For example, to start the product's processes, enter the following command:

  ```
  # ./installer -start
  ```

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

Installation program has improved failure handling

The product installer has improved ability to recover from failed installations, as follows:

- A recovery file is created if an installation fails due to a failed network connection. This file enables the install program to resume from the point where the installation failed.
- New options are available to start or stop the Veritas processes without requiring a full installation or configuration.

Installation script options

Table B-1 shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Veritas Storage Foundation product scripts, except where otherwise noted.

See "About installation scripts" on page 349.

Table B-1 Available command line options

Command Line Option	Function
system1 system2...	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
–addnode	Adds a node to a high availability cluster.
–allpkgs	Displays all packages and patches required for the specified product. The packages and patches are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network.
–comcleanup	The `-comcleanup` option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated.
–configure	Configures the product after installation.
–fencing	Configures I/O fencing in a running cluster.
–hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–install	The `-install` option is used to install products on systems.
–installallpkgs	Specifies that all packages are installed.
–installminpkgs	Specifies that the minimum package set is installed.
–installrecpkgs	Specifies that the required package set is installed.
–jumpstart *dir_path*	Produces a sample finish file for Solaris JumpStart installation. The *dir_path* indicates the path to the directory in which to create the finish file.
–keyfile *ssh_key_file*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
–license	Registers or updates product licenses on the specified systems.
–logpath *log_path*	Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved.
–makeresponsefile	Use the `-makeresponsefile` option only to generate response files. No actual software installation occurs when you use this option.
–minpkgs	Displays the minimal packages and patches required for the specified product. The packages and patches are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
–nolic	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–pkginfo	Displays a list of packages and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS packages.
–pkgpath *package_path*	Designates the path of a directory that contains all packages to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–pkgset	Discovers and displays the package group (minimum, recommended, all) and packages that are installed on the specified systems.
–pkgtable	Displays product's packages in correct installation order by group.
–postcheck	Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.
–precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.
–recpkgs	Displays the recommended packages and patches required for the specified product. The packages and patches are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
–redirect	Displays progress details without showing the progress bar.
–requirements	The `-requirements` option displays required OS version, required packages and patches, file system space, and other system requirements in order to install the product.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
–responsefile *response_file*	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
-rolling_upgrade	Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly.
–rollingupgrade_phase1	The `-rollingupgrade_phase1` option is used to perform rolling upgrade Phase-I. In the phase, the product kernel packages get upgraded to the latest version
–rollingupgrade_phase2	The `-rollingupgrade_phase2` option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent packages upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version."
–rootpath *root_path*	Specifies an alternative root directory on which to install packages. On Solaris operating systems, `-rootpath` passes `-R path` to `pkgadd` command.
–rsh	Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.
–serial	Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.

Table B-1 Available command line options *(continued)*

Command Line Option	Function
-settunables	Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the `-tunablesfile` option.
–start	Starts the daemons and processes for the specified product.
–stop	Stops the daemons and processes for the specified product.
–tmppath *tmp_path*	Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where packages are copied on remote systems before installation.
–uninstall	The `-uninstall` option is used to uninstall products from systems.
-tunablesfile	Specify this option when you specify a tunables file. The tunables file should include tunable parameters.
–upgrade	Specifies that an existing version of the product exists and you plan to upgrade it.
–version	Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.

About using the postcheck option

You can use the installer's post-check to determine installation-related problems and to aid in troubleshooting.

Note: This command option requires downtime for the node.

When you use the `postcheck` option, it can help you troubleshoot the following VCS-related issues:

- The heartbeat link does not exist.
- The heartbeat link cannot communicate.
- The heartbeat link is a part of a bonded or aggregated NIC.
- A duplicated cluster ID exists.
- The VRTSllt pkg version is not consistent on the nodes.
- The llt-linkinstall value is incorrect.
- The llthosts(4) or llttab(4) configuration is incorrect.
- the `/etc/gabtab` file is incorrect.
- The incorrect GAB linkinstall value exists.
- The VRTSgab pkg version is not consistent on the nodes.
- The `main.cf` file or the `types.cf` file is invalid.
- The `/etc/VRTSvcs/conf/sysname` file is not consistent with the hostname.
- The cluster UUID does not exist.
- The `uuidconfig.pl` file is missing.
- The VRTSvcs pkg version is not consistent on the nodes.
- The `/etc/vxfenmode` file is missing or incorrect.
- The `/etc/vxfendg file` is invalid.
- The vxfen link-install value is incorrect.
- The VRTSvxfen pkg version is not consistent.

The `postcheck` option can help you troubleshoot the following SFHA or SFCFSHA issues:

- Volume Manager cannot start because the `/etc/vx/reconfig.d/state.d/install-db` file has not been removed.
- Volume Manager cannot start because the `Volboot` file is not loaded.
- Volume Manager cannot start because no license exists.

- Cluster Volume Manager cannot start because the CVM configuration is incorrect in the `main.cf` file. For example, the Autostartlist value is missing on the nodes.
- Cluster Volume Manager cannot come online because the node ID in the `/etc/llthosts` file is not consistent.
- Cluster Volume Manager cannot come online because Vxfen is not started.
- Cluster Volume Manager cannot start because gab is not configured.
- Cluster Volume Manager cannot come online because of a CVM protocol mismatch.
- Cluster Volume Manager group name has changed from "cvm", which causes CVM to go offline.

See “Performing a postcheck on a node” on page 128.

Appendix C

Sample installation and configuration values

This appendix includes the following topics:

- SF Sybase CE installation and configuration information
- SF Sybase CE worksheet

SF Sybase CE installation and configuration information

The SF Sybase CE installation and configuration program prompts you for information about SF Sybase CE. It also provides default values for some information which you can choose to use. The worksheets provide sample values that you can use as examples of the information required for an SF Sybase CE installation and configuration.

Symantec recommends using the worksheets provided to record values for your systems before you begin the installation and configuration process.

SF Sybase CE worksheet

Table C-1 contains the sample values that may be used when you install and configure SF Sybase CE. Enter the SF Sybase CE values for your systems in the following table:

Table C-1 SF Sybase CE worksheet

Installation information	Sample value	Assigned value
Number of nodes in the cluster	2	
Host names for Primary cluster	system1 and system2	
Host names for added or removed node	system3	
SF Sybase CE License key	License keys are in the format: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXX	
Required SF Sybase CE packages vs. all SF Sybase CE	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	syb_cluster101	
Primary cluster ID number	101	
Private network links 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. Do not use the network interface card that is used for the public network, which is typically bge0.	bge1,bge2	
Cluster Manager NIC (Primary NIC)	bge0	
Cluster Manager IP	10.10.12.1, 10.10.12.2	

Table C-1 SF Sybase CE worksheet *(continued)*

Installation information	Sample value	Assigned value
Netmask for the virtual IP address	255.255.240.0	
Mode for Authentication Service: ■ Automatic mode ■ Semiautomatic mode using encrypted files ■ Semiautomatic mode without using encrypted files Default option is automatic mode.	Automatic mode	
User name Adding users is required if when using secure cluster mode. Otherwise it is optional.	smith	
User password	password	
User privilege 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.	admin	
Domain-based address of the SMTP server The SMTP server sends notification email about the events within the cluster.	smtp.symantecexample.com	

Table C-1 SF Sybase CE worksheet *(continued)*

Installation information	Sample value	Assigned value
Email address of each SMTP recipient to be notified	john@symantecexample.com	
Minimum severity of events for SMTP email notification 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	E	
Email address of SMTP notification recipients	admin@symantecexample.com	
SNMP trap daemon port number the console	162	
System name for the SNMP console	system2	
Minimum severity level of events for SMTP notification 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	i	

Table C-1 SF Sybase CE worksheet *(continued)*

Installation information	Sample value	Assigned value
CVM enclosure-based naming Requires Dynamic Multi-pathing (DMP).	yes	
Default disk group You can select the name of a default disk group of a system for running Veritas Volume Manager commands which require a disk group to be specified.	vxfencoordg	
The name of three disks that form the coordinator disk group.	■ c1t1d0s2 ■ c2t1d0s2 ■ c3t1d0s2	
Vxfen disk group	vxfencoordg	

Appendix D

Tunable files for installation

This appendix includes the following topics:

About setting tunable parameters using the installer or a response file

You can set non-default product and system tunable parameters using a tunables file. With the file, you can set tunables such as the I/O policy or toggle native multi-pathing. The tunables file passes arguments to the installer script to set tunables. With the file, you can set the tunables for the following operations:

- When you install, configure, or upgrade systems.

  ```
  # ./installer -tunablesfile tunables_file_name
  ```

  See "Setting tunables for an installation, configuration, or upgrade" on page 366.

- When you apply the tunables file with no other installer-related operations.

  ```
  # ./installer -tunablesfile tunables_file_name -settunables [
  system1 system2 ...]
  ```

See "Setting tunables with no other installer-related operations" on page 367.

- When you apply the tunables file with an un-integrated response file.

```
# ./installer -responsefile response_file_name -tunablesfile
tunables_file_name
```

See "Setting tunables with an un-integrated response file" on page 368.

For more information on response files, see the *chapter: About response files*.

You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 370.

Setting tunables for an installation, configuration, or upgrade

You can use a tunables file for installation procedures to set non-default tunables. You invoke the installation script with the `tunablesfile` option. The tunables file passes arguments to the script to set the selected tunables. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 370.

Note: Certain tunables only take effect after a system reboot.

To set the non-default tunables for an installation, configuration, or upgrade

1. Prepare the tunables file.

   See "Preparing the tunables file" on page 369.

2. Make sure the systems where you want to install SF Sybase CE meet the installation requirements.
3. Complete any preinstallation tasks.
4. Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.
5. Mount the product disc and navigate to the directory that contains the installation program.
6. Start the installer for the installation, configuration, or upgrade. For example:

   ```
   # ./installer -tunablesfile /tmp/tunables_file
   ```

   Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with no other installer-related operations

You can use the installer to set tunable parameters without any other installer-related operations. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 370.

Note: Certain tunables only take effect after a system reboot.

To set tunables with no other installer-related operations

1 Prepare the tunables file.

See "Preparing the tunables file" on page 369.

2 Make sure the systems where you want to install SF Sybase CE meet the installation requirements.

3 Complete any preinstallation tasks.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-settunables` option.

```
# ./installer -tunablesfile tunables_file_name -settunables [
sys123 sys234 ...]
```

Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 370.

Note: Certain tunables only take effect after a system reboot.

To set tunables with an un-integrated response file

1 Make sure the systems where you want to install SF Sybase CE meet the installation requirements.

2 Complete any preinstallation tasks.

3 Prepare the tunables file.

See "Preparing the tunables file" on page 369.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-settunables` option.

```
# ./installer -responsefile response_file_name -tunablesfile
tunables_file_name -settunables
```

Where *response_file_name* is the full path name for the response file and *tunables_file_name* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

For more information on response files, see the *chapter: About response files*.

Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

Format the tunable parameter as follows:

```
$TUN{"tunable_name"}{"system_name"|"*"}=value_of_tunable;
```

For the *system_name*, use the name of the system, its IP address, or a wildcard symbol. The *value_of_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```
#
# Tunable Parameter Values:
#
our %TUN;

$TUN{"tunable1"}{"*"}=1024;
$TUN{"tunable3"}{"sys123"}="SHA256";

1;
```

Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See “Tunables value parameter definitions” on page 370.

Each line for the parameter value starts with $TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{"dmp_daemon_count"}{"node123"}=16;
```

In this example, you are changing the dmp_daemon_count value from its default of 10 to 16. You can use the wildcard symbol "*" for all systems. For example:

```
$TUN{"dmp_daemon_count"}{"*"}=16;
```

Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Veritas Storage Foundation and High Availability Solutions Tuning Guide* for detailed information on product tunable ranges and recommendations .

Table D-1 describes the supported tunable parameters that can be specified in a tunables file.

Table D-1 Supported tunable parameters

Tunable	Description
dmp_cache_open	(Veritas Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_daemon_count	(Veritas Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_delayq_interval	(Veritas Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_fast_recovery	(Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_health_time	(Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Table D-1 Supported tunable parameters *(continued)*

Tunable	Description
dmp_log_level	(Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_low_impact_probe	(Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_lun_retry_timeout	(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_fabric	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_ownership	(Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_multipathing	(Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_support	(Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_path_age	(Veritas Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Table D-1 Supported tunable parameters *(continued)*

Tunable	Description
dmp_pathswitch_blks_shift	(Veritas Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_idle_lun	(Veritas Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_threshold	(Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_cycles	(Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_interval	(Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_policy	(Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_state	(Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_retry_count	(Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_scsi_timeout	(Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Table D-1 Supported tunable parameters *(continued)*

Tunable	Description
dmp_sfg_threshold	(Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_stat_interval	(Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
max_diskq	(Veritas File System) Specifies the maximum disk queue generated by a single file. The installer sets only the system default value of max_diskq. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_ahead	(Veritas File System) The 0 value disables read ahead functionality, the 1 value (default) retains traditional sequential read ahead behavior, and the 2 value enables enhanced read ahead for all reads. The installer sets only the system default value of read_ahead. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_nstream	(Veritas File System) The number of parallel read requests of size read_pref_io that can be outstanding at one time. The installer sets only the system default value of read_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_pref_io	(Veritas File System) The preferred read request size. The installer sets only the system default value of read_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
vol_checkpt_default	(Veritas File System) Size of VxVM checkpoints (sectors). This tunable requires system reboot to take effect.
vol_cmpres_enabled	(Veritas Volume Manager) Allow enabling compression for VERITAS Volume Replicator.
vol_cmpres_threads	(Veritas Volume Manager) Maximum number of compression threads for VERITAS Volume Replicator.

Table D-1 Supported tunable parameters *(continued)*

Tunable	Description
vol_default_iodelay	(Veritas Volume Manager) Time to pause between I/O requests from VxVM utilities (10ms units). This tunable requires system reboot to take effect.
vol_fmr_logsz	(Veritas Volume Manager) Maximum size of bitmap Fast Mirror Resync uses to track changed blocks (KBytes). This tunable requires system reboot to take effect.
vol_max_adminio_poolsz	(Veritas Volume Manager) Maximum amount of memory used by VxVM admin I/O's (bytes). This tunablle rquires system reboot to take effect.
vol_max_nmpool_sz	(Veritas Volume Manager) Maximum name pool size (bytes).
vol_max_rdback_sz	(Veritas Volume Manager) Storage Record readback pool maximum (bytes).
vol_max_wrspool_sz	(Veritas Volume Manager) Maximum memory used in clustered version of VERITAS Volume Replicator (bytes).
vol_maxio	(Veritas Volume Manager) Maximum size of logical VxVM I/O operations (sectors). This tunable requires system reboot to take effect.
vol_maxioctl	(Veritas Volume Manager) Maximum size of data passed into the VxVM ioctl calls (bytes). This tunable requires system reboot to take effect.
vol_maxparallelio	(Veritas Volume Manager) Number of I/O operations vxconfigd can request at one time. This tunable requires system reboot to take effect.
vol_maxspecialio	(Veritas Volume Manager) Maximum size of a VxVM I/O operation issued by an ioctl call (sectors). This tunable requires system reboot to take effect.
vol_min_lowmem_sz	(Veritas Volume Manager) Low water mark for memory (bytes).
vol_nm_hb_timeout	(Veritas Volume Manager) Veritas Volume Replicator timeout value (ticks).
vol_rvio_maxpool_sz	(Veritas Volume Manager) Maximum memory requested by VERITAS Volume Replicator (bytes).

Table D-1 Supported tunable parameters *(continued)*

Tunable	Description
vol_stats_enable	(Veritas Volume Manager) Enable VxVM I/O stat collection.
vol_subdisk_num	(Veritas Volume Manager) Maximum number of subdisks attached to a single VxVM plex. This tunable requires system reboot to take effect.
voldrl_max_drtregs	(Veritas Volume Manager) Maximum number of dirty VxVM regions that can exist on a non-sequential DRL. This tunable requires system reboot to take effect.
voldrl_max_seq_dirty	(Veritas Volume Manager) Maximum number of dirty regions in sequential mode. This tunable requires system reboot to take effect.
voldrl_min_regionsz	(Veritas Volume Manager) Minimum size of a VxVM Dirty Region Logging (DRL) region (sectors). This tunable requires system reboot to take effect.
voldrl_volumemax_drtregs	(Veritas Volume Manager) Max per volume dirty regions in log-plex DRL.
voldrl_volumemax_drtregs_20	(Veritas Volume Manager) Max per volume dirty regions in DCO version 20.
voldrl_dirty_regions	(Veritas Volume Manager) Number of regions cached for DCO version 30.
voliomem_chunk_size	(Veritas Volume Manager) Size of VxVM memory allocation requests (bytes). This tunable requires system reboot to take effect.
voliomem_maxpool_sz	(Veritas Volume Manager) Maximum amount of memory used by VxVM (bytes). This tunable requires system reboot to take effect.
voliot_errbuf_dflt	(Veritas Volume Manager) Size of a VxVM error trace buffer (bytes). This tunable requires system reboot to take effect.
voliot_iobuf_default	(Veritas Volume Manager) Default size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect.

Table D-1 Supported tunable parameters *(continued)*

Tunable	Description
voliot_iobuf_limit	(Veritas Volume Manager) Maximum total size of all VxVM I/O trace buffers (bytes). This tunable requires system reboot to take effect.
voliot_iobuf_max	(Veritas Volume Manager) Maximum size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect.
voliot_max_open	(Veritas Volume Manager) Maximum number of VxVM trace channels available for vxtrace commands. This tunable requires system reboot to take effect.
volpagemod_max_memsz	(Veritas Volume Manager) Maximum paging module memory used by Instant Snapshots (Kbytes).
volraid_rsrtransmax	(Veritas Volume Manager) Maximum number of VxVM RAID-5 transient reconstruct operations in parallel. This tunable requires system reboot to take effect.
vx_era_nthreads	(Veritas File System) Maximum number of threads VxFS will detect read_ahead patterns on. This tunable requires system reboot to take effect.
vx_bc_bufhwm	(Veritas File System) VxFS metadata buffer cache high water mark. This tunable requires system reboot to take effect.
vxfs_mbuf	(Veritas File System) Maximum memory used for VxFS buffer cache. This tunable requires system reboot to take effect.
vxfs_ninode	(Veritas File System) Number of entries in the VxFS inode table. This tunable requires system reboot to take effect.
write_nstream	(Veritas File System) The number of parallel write requests of size write_pref_io that can be outstanding at one time. The installer sets only the system default value of write_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
write_pref_io	(Veritas File System) The preferred write request size. The installer sets only the system default value of write_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.

Appendix E

SF Sybase CE sample configuration files

This appendix includes the following topics:

About sample main.cf files

You can examine the VCS configuration file, main.cf, to verify the SF Sybase CE installation and configuration.

- The main.cf file is located in the folder /etc/VRTSvcs/conf/config.
- After an SF Sybase CE installation, several sample main.cf file types can be viewed in the following directory: /etc/VRTSagents/ha/conf/Sybase
- All sample configurations assume that the Veritas High Availability Agent for Sybase binaries are installed on local disks and that they are managed by the operating system. These file systems must be specified in the file /etc/fstab
- For the following configuration samples, please note the "cluster" definition in all of the configurations should specify UseFence=SCSI3.

Sample main.cf files for Sybase ASE CE configurations

Sample main.cf file examples are provided for the following Sybase ASE CE configurations:

- Basic cluster configuration
  - With shared mount point on CFS for Sybase binary installation

- With local mount point on VxFS for Sybase binary installation
- Replicating data between two clusters
  - For a primary site in a CVM VVR configuration
  - For a secondary site in a CVM VVR configuration

Sample main.cf for a basic Sybase ASE CE cluster configuration under VCS control with shared mount point on CFS for Sybase binary installation

This sample main.cf is for a single site with a basic cluster configuration with shared mount point on CFS for Sybase binary installation.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_cfs_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase/

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "SybaseTypes.cf"

cluster syb_cluster101 (
    UserNames = { admin = HopHojOlpKppNxpJom }
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    UseFence=SCSI3
    )

system system1 (
    )

system system2 (
    )

// binmounts group for configuring CFS mounts for Sybase binaries.

group binmnt (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
```

```
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    CFSMount sybbindg_101_sybbinvol_mnt (
         MountPoint = "/sybase"
         BlockDevice = "/dev/vx/dsk/sybbindg_101/sybbin_vol"
         )

    CVMVolDg sybbindg_101_voldg (
         CVMDiskGroup = sybbindg_101
         CVMVolume = { sybbin_vol }
         CVMActivation = sw
         )

 requires group cvm online local firm
 sybbindg_101_sybbinvol_mnt requires sybbindg_101_voldg


 // resource dependency tree
 //
 // group binmnt
 // {
 // CFSMount sybbindg_101_sybbinvol_mnt
 //     {
 //     CVMVolDg sybbindg_101_voldg
 //     }
 // }

// cvm group for CVM and CFS specific agents.

group cvm (
    SystemList = { system1 = 0, system2 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system1, system2 }
    )

    CFSfsckd vxfsckd (
        )

    CVMCluster cvm_clus (
        CVMClustName = sfsyb_90
```

```
        CVMNodeId = { system1 = 0, system2 = 1 }
        CVMTransport = gab
        CVMTimeout = 200
        )

    CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )

 cvm_clus requires cvm_vxconfigd
 vxfsckd requires cvm_clus


 // resource dependency tree
 //
 // group cvm
 // {
 // CFSfsckd vxfsckd
 //     {
 //     CVMCluster cvm_clus
 //         {
 //         CVMVxconfigd cvm_vxconfigd
 //         }
 //     }
 // }

// sybasece group for:
// 1. CVM volumes for Sybase database and quorum device
// 2. CFS mount for Sybase database and quorum device
// 3. Process agent for vxfend process.
// 4. Sybase database instance.

group sybasece (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    CFSMount quorum_101_quorumvol_mnt (
        MountPoint = "/quorum"
```

```
        BlockDevice = "/dev/vx/dsk/quorum_101/quorumvol"
        )

    CFSMount sybdata_101_sybvol_mnt (
        MountPoint = "/sybdata"
        BlockDevice = "/dev/vx/dsk/sybdata_101/sybvol"
        )

    CVMVolDg quorum_101_voldg (
        CVMDiskGroup = quorum_101
        CVMVolume = { quorumvol }
        CVMActivation = sw
        )

    CVMVolDg sybdata_101_voldg (
        CVMDiskGroup = sybdata_101
        CVMVolume = { sybvol }
        CVMActivation = sw
        )

   Process vxfend (
        PathName = "/sbin/vxfend"
        Arguments = "-m sybase -k /tmp/vcmp_socket"
        )

   Sybase ase (
        Server @system1 = ase1
        Server @system2 = ase2
        Owner = sybase
        Home = "/sybase"
        Version = 15
        SA = sa
        Quorum_dev = "/quorum/q.dat"
        )

requires group binmnt online local firm
ase requires quorum_101_quorumvol_mnt
ase requires sybdata_101_sybvol_mnt
ase requires vxfend
quorum_101_quorumvol_mnt requires quorum_101_voldg
sybdata_101_sybvol_mnt requires sybdata_101_voldg
```

```
// resource dependency tree
//
// group sybasece
// {
// Sybase ase
//     {
//     CFSMount quorum_101_quorumvol_mnt
//         {
//         CVMVolDg quorum_101_voldg
//         }
//     CFSMount sybdata_101_sybvol_mnt
//         {
//         CVMVolDg sybdata_101_voldg
//         }
//     Process vxfend
//     }
// }
```

Sample main.cf for a basic Sybase ASE CE cluster configuration with local mount point on VxFS for Sybase binary installation

This sample main.cf is for a single site with a basic cluster configuration with local mount point on VxFS for Sybase binary installation.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_vxfs_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase/

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "SybaseTypes.cf"

cluster syb_cluster101 (
    UserNames = { admin = HopHojOlpKppNxpJom }
    Administrators = { admin }
    HacliUserLevel = COMMANDROOT
    UseFence=SCSI3
    )
```

```
system system1 (
    )

system system2 (
    )

// binmounts group for configuring VxFS mounts for Sybase binaries.

group binlocalmnt (
    SystemList = { system1 = 0, system2 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    DiskGroup sybbindg_101_voldg (
         DiskGroup = sybbindg
         )

    Mount sybbindg_101_sybbinvol_mnt (
         MountPoint = "/sybase"
         BlockDevice = "/dev/vx/dsk/sybbindg_101/sybbin_vol"
         FSType = vxfs
         FsckOpt = "-y"
         )

    Volume sybbindg_101_vol (
         DiskGroup = sybbindg
         Volume = sybbinvol
         )

 requires group cvm online local firm
 sybbindg_101_sybbinvol_mnt requires sybbindg_101_vol
 sybbindg_101_vol requires sybbindg_101_voldgdg


 // resource dependency tree
 //
 // group binlocalmnt
 // {
 // Mount sybbindg_101_sybbinvol_mnt
```

```
 //     {
 //     Volume sybbindg_vol
 //         {
 //         DiskGroup sybbindg_101_voldg
 //         }
 //     }
 // }

// cvm group for CVM and CFS specific agents.

group cvm (
    SystemList = { system1 = 0, system2 = 1 }
    AutoFailOver = 0
    Parallel = 1
    AutoStartList = { system1, system2 }
    )

    CFSfsckd vxfsckd (
        )

    CVMCluster cvm_clus (
        CVMClustName = syb_cluster101
        CVMNodeId = { system1 = 0, system2 = 1 }
        CVMTransport = gab
        CVMTimeout = 200
        )

    CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )

 cvm_clus requires cvm_vxconfigd
 vxfsckd requires cvm_clus


 // resource dependency tree
 //
 // group cvm
 // {
 // CFSfsckd vxfsckd
 //     {
 //     CVMCluster cvm_clus
```

```
 //          {
 //          CVMVxconfigd cvm_vxconfigd
 //          }
 //      }
 // }

// sybasece group for:
// 1. CVM volumes for Sybase database and quorum device
// 2. CFS mount for Sybase database and quorum device
// 3. Process agent for vxfend process.
// 4. Sybase database instance.

group sybasece (
    SystemList = { system1 = 0, system2 = 1 }
    Parallel = 1
    AutoStartList = { system1, system2 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    CFSMount quorum_101_quorumvol_mnt (
        MountPoint = "/quorum"
        BlockDevice = "/dev/vx/dsk/quorum_101/quorumvol"
        )

    CFSMount sybdata_101_sybvol_mnt (
        MountPoint = "/sybdata"
        BlockDevice = "/dev/vx/dsk/sybdata_101/sybvol"
        )

    CVMVolDg quorum_101_voldg (
        CVMDiskGroup = quorum_101
        CVMVolume = { quorumvol }
        CVMActivation = sw
        )

    CVMVolDg sybdata_101_voldg (
        CVMDiskGroup = sybdata_101
        CVMVolume = { sybvol }
        CVMActivation = sw
        )

   Process vxfend (
```

```
       PathName = "/sbin/vxfend"
       Arguments = "-m sybase -k /tmp/vcmp_socket"
       )

  Sybase ase (
       Server @system1 = ase1
       Server @system2 = ase2
       Owner = sybase
       Home = "/sybase"
       Version = 15
       SA = sa
       Quorum_dev = "/quorum/q.dat"
       )

requires group binlocalmnt online local firm
ase requires quorum_101_quorumvol_mnt
ase requires sybdata_101_sybvol_mnt
ase requires vxfend
quorum_101_quorumvol_mnt requires quorum_101_voldg
sybdata_101_sybvol_mnt requires sybdata_101_voldg


// resource dependency tree
//
// group sybasece
// {
// Sybase ase
//     {
//     CFSMount quorum_101_quorumvol_mnt
//         {
//         CVMVolDg quorum_101_voldg
//         }
//     CFSMount sybdata_101_sybvol_mnt
//         {
//         CVMVolDg sybdata_101_voldg
//         }
//     Process vxfend
//     }
// }
```

Sample main.cf for a primary CVM VVR site

This sample main.cf is for a primary site in a CVM VVR configuration. It is one of two sample main.cfs for replicating data between two clusters.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_cvmvvr_primary_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "SybaseTypes.cf"

cluster syb_cluster101 (
        UserNames = { admin = HopHojOlpKppNxpJom }
        ClusterAddress = "10.180.88.188"
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        UseFence=SCSI3
        )

remotecluster syb_cluster102 (
        ClusterAddress = "10.190.99.199"
        )

heartbeat Icmp (
        ClusterList = { syb_cluster102 }
        Arguments @syb_cluster102 = { "10.190.99.199" }

        )
system system1 (
        )

system system2 (
        )


group ClusterService (
        SystemList = { system1 = 0, system2 = 1 }
        AutoStartList = { system1, system2 }
        OnlineRetryLimit = 3
```

```
                OnlineRetryInterval = 120
                )

                Application wac (
                        StartProgram = "/opt/VRTSvcs/bin/wacstart"
                        StopProgram = "/opt/VRTSvcs/bin/wacstop"
                        MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
                        RestartLimit = 3
                        )

                IP gcoip (
                        Device = bge0
                        Address = "10.180.88.188"
                        NetMask = "255.255.255.0"
                        )

                NIC csgnic (
                        Device = bge0
                        )

                gcoip requires csgnic
                wac requires gcoip


                // resource dependency tree
                //
                //      group ClusterService
                //      {
                //      Application wac
                //          {
                //          IP gcoip
                //              {
                //              NIC csgnic
                //              }
                //          }
                //      }


        group RVGgroup (
                SystemList = { system1 = 0, system2 = 1 }
                Parallel = 1
                AutoStartList = { system1, system2 }
                )
```

```
        CVMVolDg sybdata_voldg (
                CVMDiskGroup = sybdata_101
                CVMActivation = sw
                )

        RVGShared sybdata_rvg (
                RVG = syb_rvg
                DiskGroup = sybdata_101
                )

        requires group binmnt online local firm
        sybdata_rvg requires sybdata_voldg



group binmnt (
        SystemList = { system1 = 0, system2 = 1 }
        Parallel = 1
        AutoStartList = { system1, system2 }
        OnlineRetryLimit = 3
        OnlineRetryInterval = 120
        )

        CFSMount sybbindg_101_sybbinvol_mnt (
                MountPoint = "/sybase"
                BlockDevice = "/dev/vx/dsk/sybbindg_101/sybbin_vol"
                )
        CVMVolDg sybbindg_101_voldg (
                CVMDiskGroup = sybbindg_101
                CVMVolume = { sybbin_vol }
                CVMActivation = sw
                )
        requires group cvm online local firm
        sybbindg_101_sybbinvol_mnt requires sybbindg_101_voldg

group cvm (
        SystemList = { system1 = 0, system2 = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { system1, system2 }
        )
```

```
        CFSfsckd vxfsckd (
                )

        CVMCluster cvm_clus (
                CVMClustName = syb_cluster101
                CVMNodeId = { system1 = 0, system2 = 1 }
                CVMTransport = gab
                CVMTimeout = 200
                )

        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )

        cvm_clus requires cvm_vxconfigd
        vxfsckd requires cvm_clus


        // resource dependency tree
        //
        //      group cvm
        //      {
        //      CFSfsckd vxfsckd
        //          {
        //          CVMCluster cvm_clus
        //              {
        //              CVMVxconfigd cvm_vxconfigd
        //              }
        //          }
        //      }


group logowner (
        SystemList = { system1 = 0, system2 = 1 }
        AutoStartList = { system1, system2 }
        )

        IP logowner_ip (
                Device = bge0
                Address = "10.10.9.101"
                NetMask = "255.255.255.0"
                )
```

```
        NIC nic (
                Device = bge0
                )

        RVGLogowner rvg_logowner (
                RVG = syb_rvg
                DiskGroup = sybdata_101
                )

        requires group RVGgroup online local firm
        logowner requires logowner_ip
        logowner_ip requires nic


        // resource dependency tree
        //
        //      group logowner
        //      {
        //      RVGLogowner rvg_logowner
        //          {
        //          IP logowner_ip
        //              {
        //              NIC nic
        //              }
        //          }
        //      }

group sybasece (
        SystemList = { system1 = 0, system2 = 1 }
        Parallel = 1
        ClusterList = { syb_cluster101 = 0, syb_cluster102 = 1 }
        AutoStartList = { system1, system2 }
        ClusterFailOverPolicy = Manual
        Authority = 1
        OnlineRetryLimit = 3
        TriggerResStateChange = 1
        OnlineRetryInterval = 120
        )

        CFSMount quorum_101_quorumvol_mnt (
                MountPoint = "/quorum"
                BlockDevice = "/dev/vx/dsk/quorum_101/quorumvol"
```

```
        )

CFSMount sybdata_101_sybvol_mnt (
        MountPoint = "/sybdata"
        BlockDevice = "/dev/vx/dsk/sybdata_101/sybvol"
        )

CVMVolDg quorum_101_voldg (
        CVMDiskGroup = quorum_101
        CVMVolume = { quorumvol }
        CVMActivation = sw
        )

Process vxfend (
        PathName = "/sbin/vxfend"
        Arguments = "-m sybase -k /tmp/vcmp_socket"
        )

RVGSharedPri syb_vvr_shpri (
        RvgResourceName = sybdata_rvg
        OnlineRetryLimit = 0
        )

Sybase ase (
        Server @system1 = ase1
        Server @system2 = ase2
        Owner = sybase
        Home = "/sybase"
        Version = 15
        SA = sa
        Quorum_dev = "/quorum/q.dat"
        )

requires group RVGgroup online local firm
sybdata_101_sybvol_mnt requires syb_vvr_shpri
ase requires vxfend
ase requires sybdata_101_sybvol_mnt
ase requires quorum_101_quorumvol_mnt
quorum_101_quorumvol_mnt requires quorum_101_voldg

// resource dependency tree
//
//      group sybasece
```

```
//      {
//      Sybase ase
//          {
//          CFSMount sybdata_101_sybvol_mnt
//              {
//              RVGSharedPri syb_vvr_shpri
//              }
//          Process vxfend
//          CFSMount quorum_101_quorumvol_mnt
//              {
//              CVMVolDg quorum_101_voldg
//              }
//          }
//      }
```

Sample main.cf for a secondary CVM VVR site

This sample main.cf is for a secondary site in a CVM VVR configuration. It is the second of two sample main.cfs for replicating data between two clusters.

The following are the configuration details for this Sybase ASE CE configuration sample main.cf:

- File name: sybasece_cvmvvr_secondary_main.cf
- File location: /etc/VRTSagents/ha/conf/Sybase

```
This is main.cf for CVM VVR configuration on Secondary site.
---------------------------------------------------------------

include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
include "SybaseTypes.cf"

cluster syb_cluster102 (
        UserNames = { admin = HopHojOlpKppNxpJom }
        ClusterAddress = "10.190.99.199"
        Administrators = { admin }
        HacliUserLevel = COMMANDROOT
        UseFence=SCSI3
        )

remotecluster syb_cluster101 (
        ClusterAddress = "10.180.88.188"
```

```
        )

heartbeat Icmp (
        ClusterList = { syb_cluster101 }
        Arguments @syb_cluster101 = { "10.180.88.188" }
        )

system system3 (
        )

system system4 (
        )

group ClusterService (
        SystemList = { system3 = 0, system4 = 1 }
        AutoStartList = { system3, system4 }
        OnlineRetryLimit = 3
        OnlineRetryInterval = 120
        )

        Application wac (
                StartProgram = "/opt/VRTSvcs/bin/wacstart"
                StopProgram = "/opt/VRTSvcs/bin/wacstop"
                MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
                RestartLimit = 3
                )

        IP gcoip (
                Device = bge0
                Address = "10.190.99.199"
                NetMask = "255.255.255.0"
                )

        NIC csgnic (
                Device = bge0
                )

        gcoip requires csgnic
        wac requires gcoip

 // resource dependency tree
 //
 // group ClusterService
```

```
// {
// Application wac
//     {
//     IP gcoip
//         {
//         NIC csgnic
//         }
//     }
// }


group RVGgroup (
        SystemList = { system3 = 0, system4 = 1 }
        Parallel = 1
        AutoStartList = { system3, system4 }
        )

        CVMVolDg sybdata_voldg (
                CVMDiskGroup = sybdata_101
                CVMActivation = sw
                )

        RVGShared sybdata_rvg (
                RVG = syb_rvg
                DiskGroup = sybdata_101
                )

        requires group binmnt online local firm
        sybdata_rvg requires sybdata_voldg


group binmnt (
        SystemList = { system3 = 0, system4 = 1 }
        Parallel = 1
        AutoStartList = { system3, system4 }
        OnlineRetryLimit = 3
        OnlineRetryInterval = 120
        )

        CFSMount sybbindg_101_sybbinvol_mnt (
                MountPoint = "/sybase"
                BlockDevice = "/dev/vx/dsk/sybbindg_101/sybbin_vol"
                )
```

```
        CVMVolDg sybbindg_101_voldg (
                CVMDiskGroup = sybbindg_101
                CVMVolume = { sybbin_vol }
                CVMActivation = sw
                )
        requires group cvm online local firm
        sybbindg_101_sybbinvol_mnt requires sybbindg_101_voldg

group cvm (
        SystemList = { system3 = 0, system4 = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { system3, system4 }
        )

        CFSfsckd vxfsckd (
                )

        CVMCluster cvm_clus (
                CVMClustName = syb_cluster102
                CVMNodeId = { system3 = 0, system4 = 1 }
                CVMTransport = gab
                CVMTimeout = 200
                )

        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )

        cvm_clus requires cvm_vxconfigd
        vxfsckd requires cvm_clus


        // resource dependency tree
        //
        //      group cvm
        //      {
        //      CFSfsckd vxfsckd
        //          {
        //          CVMCluster cvm_clus
        //              {
        //              CVMVxconfigd cvm_vxconfigd
```

```
        //              }
        //          }


group logowner (
        SystemList = { system3 = 0, system4 = 1 }
        AutoStartList = { system3, system4 }
        )

        IP logowner_ip (
                Device = bge0
                Address = "10.11.9.102"
                NetMask = "255.255.255.0"
                )

        NIC nic (
                Device = bge0
                )

        RVGLogowner rvg_logowner (
                RVG = syb_rvg
                DiskGroup = sybdata_101
                )

        requires group RVGgroup online local firm
        logowner requires logowner_ip
        logowner_ip requires nic


 // resource dependency tree
 //
 // group logowner
 // {
 // RVGLogowner rvg_logowner
 //     {
 //     IP logowner_ip
 //         {
 //         NIC nic
 //         }
 //     }
 // }

group sybasece (
```

```
SystemList = { system3 = 0, system4 = 1 }
Parallel = 1
ClusterList = { syb_cluster102 = 0, syb_cluster101 = 1 }
AutoStartList = { system3, system4 }
OnlineRetryLimit = 3
OnlineRetryInterval = 120
)

CFSMount quorum_101_quorumvol_mnt (
        MountPoint = "/quorum"
        BlockDevice = "/dev/vx/dsk/quorum_101/quorumvol"
        )

CVMVolDg quorum_101_voldg (
        CVMDiskGroup = quorum_101
        CVMVolume = { quorumvol }
        CVMActivation = sw
        )

CFSMount sybdata_101_sybvol_mnt (
        MountPoint = "/sybdata"
        BlockDevice = "/dev/vx/dsk/sybdata_101/sybvol"
        )

Process vxfend (
        PathName = "/sbin/vxfend"
        Arguments = "-m sybase -k /tmp/vcmp_socket"
        )

RVGSharedPri syb_vvr_shpri (
        RvgResourceName = sybdata_rvg
        OnlineRetryLimit = 0
        )

Sybase ase (
        Server @system3 = ase1
        Server @system4 = ase2
        Owner = sybase
        Home = "/sybase"
        Version = 15
        SA = sa
        Quorum_dev = "/quorum/q.dat"
        )
```

```
requires group RVGgroup online local firm
sybdata_101_sybvol_mnt requires syb_vvr_shpri
ase requires vxfend
ase requires sybdata_101_sybvol_mnt
ase requires quorum_101_quorumvol_mnt
quorum_101_quorumvol_mnt requires quorum_101_voldg
```

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 Sybase or a Web server, or a configuration component such as an IP address or mounted file system.

Attributes are either optional or required, although sometimes the attributes that are optional in one configuration may be required in other configurations. Many optional attributes have predefined or default values, which you should change as required. A variety of internal use only attributes also exist. Do not modify these attributes—modifying them can lead to significant problems for your clusters. Attributes have type and dimension. Some attribute values can accept numbers, others can accept alphanumeric values or groups of alphanumeric values, while others are simple boolean on/off values.

The entry points and attributes for each SF Sybase CE agent are described in this appendix.

VCS agents included within SF Sybase CE

SF Sybase CE includes the following VCS agents:

- CVMCluster agent
- CVMVxconfigd agent
- CVMVolDg agent
- CFSMount agent

An SF Sybase CE installation automatically configures the CVMCluster resource and the CVMVxconfigd resource.

You must configure the CVMVolDg agent for each disk group that is used by an agent for Sybase service group. Configure a disk group for only a single agent for Sybase service group. If the database uses cluster file systems, configure the CFSMount agent for each volume in the disk group.

Use the information in this appendix about the entry points and attributes of the listed agents to make necessary configuration changes. For information on how to modify the VCS configuration:

See the *Veritas Cluster Server Administrator's Guide*

VCS agent for Sybase included within SF Sybase CE

SF Sybase CE includes an additional agent for Sybase.

See the *Veritas Cluster Server Agent for Sybase Installation and Configuration Guide* for more information on the Sybase agent.

CVMCluster agent

The CVMCluster agent controls system membership on the cluster port that is associated with Veritas Volume Manager (VxVM).

The CVMCluster agent performs the following functions:

- Joins a node to the CVM cluster port.
- Removes a node from the CVM cluster port.
- Monitors the node's cluster membership state.

Entry points for CVMCluster agent

Table 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	Description
CVMClustName	Name of the cluster. ■ Type and dimension: string-scalar
CVMNodeAddr	List of host names and IP addresses. ■ Type and dimension: string-association
CVMNodeId	Associative list. The first part names the system; the second part contains the LLT ID number for the system. ■ Type and dimension: string-association

Table F-2 CVMCluster agent attributes *(continued)*

Attribute	Description
CVMTransport	Specifies the cluster messaging mechanism. ■ Type and dimension: string-scalar ■ Default = gab **Note:** Do not change this value.
PortConfigd	The port number that is used by CVM for vxconfigd-level communication. ■ Type and dimension: integer-scalar
PortKmsgd	The port number that is used by CVM for kernel-level communication. ■ Type and dimension: integer-scalar
CVMTimeout	Timeout in seconds used for CVM cluster reconfiguration. ■ Type and dimension: integer-scalar ■ Default = 200

CVMCluster agent type definition

The following type definition is included in the file, `CVMTypes.cf`:

```
type CVMCluster (
        static 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 Sybase CE environment. GAB, the required cluster communication messaging mechanism, does not use them.

CVMCluster agent sample configuration

The following is an example definition for the CVMCluster service group:

```
CVMCluster cvm_clus (
        Critical = 0
        CVMClustName = syb_cluster101
        CVMNodeId = { system1 = 0, system2 = 1 }
        CVMTransport = gab
        CVMTimeout = 200
         )
```

CVMVxconfigd agent

The CVMVxconfigd agent starts and monitors the vxconfigd daemon. The vxconfigd daemon maintains disk and disk group configurations, communicates configuration changes to the kernel, and modifies the configuration information that is stored on disks. CVMVxconfigd must be present in the CVM service group.

The CVMVxconfigd agent is an OnOnly agent; the agent starts the resource when the cluster starts up and VCS restarts the resource when necessary. The Operations attribute specifies these default aspects of startup.

Symantec recommends starting the vxconfigd daemon with the `syslog` option, which enables logging of debug messages. Note that the SF Sybase CE installation configures the `syslog` option for the CVMVxconfigd agent.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CVMVxconfigd agent

Table F-3 describes the entry points for the CVMVxconfigd agent.

Table F-3 CVMVxconfigd entry points

Entry Point	Description
Online	Starts the `vxconfigd` daemon
Offline	N/A
Monitor	Monitors whether `vxconfigd` daemon is running
imf_init	Initializes the agent to interface with the AMF kernel module. This function runs when the agent starts up.
imf_getnotification	Gets notification about the `vxconfigd` process state. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification. If the `vxconfigd` process fails, the function initiates a traditional CVMVxconfigd monitor entry point.
imf_register	Registers or unregisters the `vxconfigd` process id (pid) with the AMF kernel module. This function runs after the resource goes into steady online state.

Attribute definition for CVMVxconfigd agent

Table F-4 describes the modifiable attributes of the CVMVxconfigd resource type.

Table F-4 CVMVxconfigd agent attribute

Attribute	Description
CVMVxconfigdArgs	List of the arguments that are sent to the `online` entry point. Symantec recommends always specifying the `syslog` option. ■ Type and dimension: keylist

Table F-4 CVMVxconfigd agent attribute *(continued)*

Attribute	Description
IMF	This resource-type level attribute determines whether the CVMVxconfigd agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 0—Does not perform intelligent resource monitoring ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. ■ Type and dimension: integer-association For more details of IMF attribute for the agent type, refer to the *Veritas Cluster Server Administrator's Guide*.

CVMVxconfigd agent type definition

The following type definition is included in the CVMTypes.cf file:

```
type CVMVxconfigd (
        static int FaultOnMonitorTimeouts = 2
```

```
static int RestartLimit = 5
static str ArgList[] { CVMVxconfigdArgs }
static str Operations = OnOnly
keylist CVMVxconfigdArgs
)
```

CVMVxconfigd agent sample configuration

The following is an example definition for the `CVMVxconfigd` resource in the CVM service group:

```
CVMVxconfigd cvm_vxconfigd (
        Critical = 0
        CVMVxconfigdArgs = { syslog }
        )
```

For a more extensive main.cf that includes the CVMVxconfigd resource:

See "About sample main.cf files" on page 377.

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.

The CVMVolDg agent manages the CVM disk groups and CVM volumes and volume sets within the disk groups by performing the following functions:

- Imports the shared disk group from the CVM master node
- Starts the volumes and volume sets in the disk group
- Monitors the disk group, volumes, and volume sets
- Optionally, deports the disk group when the dependent applications are taken offline. The agent deports the disk group only if the appropriate attribute is set.

Configure the CVMVolDg agent for each disk group used by a Sybase service group. A disk group must be configured to only one Sybase service group.If cluster file systems are used for the database, configure the CFSMount agent for each volume or volume set 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. Imports the shared disk group from the CVM master node, if the disk group is not already imported. 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 activation mode of the shared disk group to "off." If the `CVMDeportOnOffline` attribute is set to 1 and if the shared disk group does not contain open volumes on any node in the cluster, the disk group is deported from the CVM master node.
Monitor	Monitors specified critical volumes in the diskgroup. The CVMVolume attribute specifies these volumes. SF Sybase CE requires specifying at least one volume in a disk group. The agent takes a volume set offline if the file system metadata volume of a volume set is discovered to be offline in a monitor cycle. **Note:** If the CFSMount resource goes offline and the file system on the volume set is unmounted, the agent retains the online state of the volume set even if the file system metadata volume in the volume set is offline. This is because the CVMVolDg agent is unable to determine whether or not the volumes that are offline are metadata volumes.
Clean	Removes the temporary files created by the online entry point.

Attribute definition for CVMVolDg agent

Table F-6 describes the user-modifiable attributes of the CVMVolDg resource type.

Table F-6 CVMVolDg agent attributes

Attribute	Description
CVMDiskGroup (required)	Shared disk group name. ■ Type and dimension: string-scalar

Table F-6 CVMVolDg agent attributes *(continued)*

Attribute	Description
CVMVolume (required)	Lists critical volumes in the disk group. SF Sybase CE requires specifying at least one volume in the disk group. ■ Type and dimension: string-keylist
CVMActivation (required)	Activation mode for the disk group. ■ Type and dimension: string-scalar ■ Default = `sw (shared-write)` This is a localized attribute.
CVMDeportOnOffline (optional)	Indicates whether or not the shared disk group must be deported when the last online CVMVolDg resource for a disk group is taken offline. The value 1 indicates that the agent will deport the shared disk group from the CVM master node, if not already deported, when the last online CVMVolDg resource for the disk group is taken offline. The value 0 indicates that the agent will not deport the shared disk group when the CVMVolDg resource is taken offline. ■ Type and dimension: integer-scalar ■ Default = 0 **Note:** If multiple CVMVolDg resources are configured for a shared disk group, set the value of the attribute to either 1 or 0 for all of the resources. The CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported. The deport operation fails if the shared disk group contains open volumes.

CVMVolDg agent type definition

The CVMTypes.cf file includes the CVMVolDg type definition:

```
type CVMVolDg (
        static keylist RegList = { CVMActivation, CVMVolume }
        static int OnlineRetryLimit = 2
        static int OnlineTimeout = 400
        static str ArgList[] = { CVMDiskGroup, CVMVolume, CVMActivation,
        CVMVolumeIoTest, CVMDGAction, CVMDeportOnOffline }
        str CVMDiskGroup
```

```
        str CVMDGAction
        keylist CVMVolume
        str CVMActivation
        keylist CVMVolumeIoTest
        int CVMDeportOnOffline
        temp int voldg_stat
)

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 Sybase service group requires a CVMVolDg resource type to be defined. The following is a sample configuration:

```
CVMVolDg cvmvoldg1 (
 Critical = 0
 CVMDiskgroup = testdg
 CVMVolume = { vol1, vol2, mvol1, mvol2, snapvol, vset1 }
 CVMVolumeIoTest = { snapvol, vset1 }
 CVMActivation @system1 = sw
 CVMActivation @system2 = sw
 CVMDeportOnOffline = 1
)

CVMVolDg sybbindg_101_voldg (
  CVMDiskGroup = sybbindg_101
  CVMVolume = { sybbin_vol }
  CVMActivation = sw
  )
```

CFSMount agent

The CFSMount agent brings online, takes offline, and monitors a cluster file system mount point.

The agent executable is located in /opt/VRTSvcs/bin/CFSMount/CFSMountAgent.

The CFSMount type definition is described in the /etc/VRTSvcs/conf/config/CFSTypes.cf file.

This agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification. For more information about the Intelligent Monitoring Framework (IMF) and intelligent resource monitoring, refer to the *Veritas Cluster Server Administrator's Guide*.

Entry points for CFSMount agent

Table 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.
imf_init	Initializes the agent to interface with the AMF kernel driver, which is the IMF notification module for the agent. This function runs when the agent starts up.
imf_getnotification	Gets notification about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification.
imf_register	Registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into steady state (online or offline).

Attribute definition for CFSMount agent

Table F-8 lists user-modifiable attributes of the CFSMount Agent resource type.

Table F-8 CFSMount Agent attributes

Attribute	Description
MountPoint	Directory for the mount point. ■ Type and dimension: string-scalar
BlockDevice	Block device for the mount point. ■ Type and dimension: string-scalar
NodeList	List of nodes on which to mount. If NodeList is NULL, the agent uses the service group system list. ■ Type and dimension: string-keylist

Table F-8 CFSMount Agent attributes *(continued)*

Attribute	Description
IMF	Resource-type level attribute that determines whether the CFSMount agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 0—Does not perform intelligent resource monitoring ■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources ■ 3—Performs intelligent resource monitoring for both online and for offline resources Default: 0 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 1 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver. The value of the RegisterRetyLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3. ■ Type and dimension: integer-association

Table F-8 CFSMount Agent attributes *(continued)*

Attribute	Description

MountOpt
(optional)
	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`
	■ Type and dimension: string-scalar

Policy (optional)	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. ■ Type and dimension: string-scalar

CFSMount agent type definition

The `CFSTypes.cf` file includes the CFSMount agent type definition:

```
type CFSMount (
   static keylist RegList = { MountOpt, Policy, NodeList, ForceOff, SetPrimary }
   static keylist SupportedActions = { primary }
   static int FaultOnMonitorTimeouts = 1
   static int OnlineWaitLimit = 1
   static str ArgList[] = { MountPoint, BlockDevice, MountOpt, Primary, AMFMountType }
   str MountPoint
   str MountType
   str BlockDevice
   str MountOpt
   keylist NodeList
   keylist Policy
   temp str Primary
   str SetPrimary
   temp str RemountRes
   temp str AMFMountType
   str ForceOff
)
```

CFSMount agent sample configuration

Each Sybase service group requires a CFSMount resource type to be defined:

```
CFSMount sybbindg_mnt (
        MountPoint = "/sybase"
        BlockDevice = "/dev/vx/dsk/sybbindg/sybbinvol"
        Primary = system2;
        )
```

To see CFSMount defined in a more extensive example:

See "About sample main.cf files" on page 377.

Process agent

The Process agent starts, stops, and monitors a process that you specify. You can use the agent to make a process highly available or to monitor it.

Agent functions

Online	Starts the process with optional arguments.
Offline	Terminates the process with a SIGTERM. If the process does not exit, a SIGKILL is sent.
Monitor	Checks to see if the process is running by scanning the process table for the name of the executable pathname and argument list.
Clean	Terminates all ongoing resource actions and takes the resource offline, forcibly when necessary.

State definitions

ONLINE	Indicates that the specified process is running in the specified user context. For Solaris 10, the process can run in global and non-global zones when you specify the ContainerName attribute. The agent only reports the process as online if the value configured for PathName attribute exactly matches the process listing from the ps output.
OFFLINE	Indicates that the specified process is not running in the specified user context.
FAULTED	Indicates that the process has terminated unexpectedly.
UNKNOWN	Indicates that the agent can not determine the state of the process.

Attributes

Table F-9 Required attribute

Required attribute	Description
PathName	Complete pathname to access an executable program. This path includes the program name. If a script controls the process, the PathName defines the complete path to the shell. This attribute must not exceed 80 characters. Type and dimension: string-scalar Example: "/usr/lib/sendmail"

Table F-10 Optional attributes

Optional attribute	Description
Arguments	Passes arguments to the process. If a script controls the process, the script is passed as an argument. Separate multiple arguments with a single space. A string cannot accommodate more than one space between arguments, nor allow for leading or trailing whitespace characters. This attribute must not exceed 80 characters. Type and dimension: string-scalar Example: "bd -q1h"
ContainerName	Non-global zone support for Solaris 10 and above. Defines the name of the non-global zone. Type and dimension: string-scalar Example: "zone1"
ContainerType	Do not change. For internal use only.

Resource type definition

```
type Process (
    static keylist SupportedActions = { "program.vfd", getcksum }
    static str ContainerType = Zone
    static str ArgList[] = { ContainerName, PathName, Arguments }
    str ContainerName
    str PathName
    str Arguments
)
```

Sample configurations

```
Process vxfend (
        PathName = "/sbin/vxfend"
        Arguments = "-m sybase -k /tmp/vcmp_socket"
        )
```

Monitoring options for the Sybase agent

The Veritas agent for Sybase provides two levels of application monitoring: basic and detail.

In the basic monitoring mode, the agent for Sybase monitors the Sybase daemon processes to verify whether they are running.

For Sybase cluster edition, the agent uses `qrmutil` utility that Sybase provides to get the status of the Sybase instance. If the state returned by `qrmutil` utility is 'failure pending', the agent panics the node. When the Sybase agent detects that the configured Sybase server is not running on a system, based on the value of the OnlineRetryLimit attribute of the Sybase service group, the service group is restarted on the same system on which the group faulted.

For example:

```
# qrmutil --quorum_dev=/quorum/quorum.dat --monitor=ase1
Executing 'monitor' command for instance 'ase1'
Instance 'ase1' has a failure pending.
# echo $?
99
```

In this example instance ‘ase1’ has a failure pending state. The agent will panic the node running the instance ‘ase1’. The node will automatically rejoin the cluster after reboot.

In the detail monitoring mode, the agent performs a transaction on a test table in the database to ensure that Sybase 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.

See “About setting up detail monitoring for the agentfor Sybase” on page 203.

Sybase resource type

The type definitions and attribute definitions for the Sybase resource type are described as follows.

Type definition for the Sybase agent

The resource type definition for the agent for Sybase is as follows.

```
type Sybase (
        static boolean AEPTimeout = 1
        static keylist SupportedActions = { "checkpoint_all" }
```

```
        str Server
        str Owner
        str Home
        str Version
        str SA
        str SApswd
        str Run_ServerFile
        int DetailMonitor = 0
        str User
        str UPword
        str Db
        str Table
        str Monscript = "/opt/VRTSagents/ha/bin/Sybase/SqlTest.pl"
        boolean WaitForRecovery = 0
        str Quorum_dev
        str interfaces_File
        int ShutdownWaitLimit = 60
        int DelayAfterOnline = 10
        int DelayAfterOffline = 2
        static int ToleranceLimit = 1
        static str ArgList[] = { Server, Owner, Home, Version, SA,
        SApswd, User, UPword, Db, Table, Monscript, DetailMonitor,
        WaitForRecovery, Run_ServerFile, Quorum_dev, State,
        interfaces_File, ShutdownWaitLimit, DelayAfterOnline,
        DelayAfterOffline }
        static int IMF{} = { Mode=3, MonitorFreq=5, RegisterRetryLimit=3 }
        static str IMFRegList[] = { Server, Owner, Quorum_dev }
        static int ContainerOpts{} = { RunInContainer=1, PassCInfo=0 }
        static str AgentDirectory = "/opt/VRTSagents/ha/bin/Sybase"
)
```

Attribute definitions for the Sybase agent

Review the description of the Sybase agent attributes. The agent attributes are classified as required, optional, and internal.

Table F-11 lists the required attributes.

Table F-11 Required attributes

Required Attributes	Definition
Server	The $DSQUERY ASE name. Only one server should be configured in a Sybase service group. The advantage of configuring Sybase resources in a separate service group is, each Sybase data server can failover independently. Type and dimension: string-scalar Default value: No default value
Owner	Sybase user as the defined owner of executables and database files in any of the sources (such as NIS+, /etc/hosts, and so on) specified in the /etc/nsswitch.conf file for passwd entry. The Sybase executables and database files are accessed in the context of this user. Type and dimension: string-scalar
Home	The $SYBASE path to Sybase binaries and configuration files. Type and dimension: string-scalar Default value: No default value
Version	Version of Sybase ASE. Type and dimension: string-scalar Default value: No default value **Caution:** Once the Sybase resource is online in VCS, you must not modify the Home and Version attributes. For the Sybase cluster edition, setting invalid values for Home and Version attributes when the resource is in Online state causes the node to panic.
SA	Sybase database administrator. This attribute is required to connect to the ASE for shutdown. Type and dimension: string-scalar Default value: No default value

Table F-11 Required attributes *(continued)*

Required Attributes	Definition
SApswd	Encrypted password for Sybase database administrator. This password is required to connect to the ASE for shutdown. Type and dimension: string-scalar Default value: No default value See "Encrypting passwords for Sybase" on page 203. **Note:** You need not specify a value for this attribute if the SA user does not require a password.

Table F-12 lists the optional attributes.

Table F-12 Optional attributes

Optional Attributes	Definition
DetailMonitor	Specifies whether the Sybase server is monitored in detail. A positive integer value indicates that the resource monitors the Sybase server in detail. Value 0 denotes it does not. Default is 0. Type and dimension: int-scalar **Note:** The DetailMonitor attribute is deprecated in VCS 6.0. Instead, LevelTwoMonitorFreq attribute of Sybase agent may be used. The default value of LevelTwoMonitorFreq attribute is 0 (zero).
User	The database user, in the context of which, the transactions are performed on the database. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value. Type and dimension: string-scalar Default value: No default value **Note:** By default, SqlTest.pl script has the execute permission set. If you specify custom detail monitor script, ensure that custom detail monitor script also has the execute permissions set.

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
UPword	Encrypted password for the database user. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value. However, you need not specify a value for this attribute if the database user does not require a password. See "Encrypting passwords for Sybase" on page 203. intercType and dimension: string-scalar Default value: No default value **Note:** By default, SqlTest.pl script has the execute permission set. If you specify custom detail monitor script, ensure that custom detail monitor script also has the execute permissions set.
Db	Name of the database used for detailed monitoring. The table used by the detail monitor script resides in this database. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value. Type and dimension: string-scalar Default value: No default value **Note:** By default, SqlTest.pl script has the execute permission set. If you specify custom detail monitor script, ensure that custom detail monitor script also has the execute permissions set.
Table	Name of the table on which the detail monitoring script performs the transactions. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value. Type and dimension: string-scalar Default value: No default value **Note:** By default, SqlTest.pl script has the execute permission set. If you specify custom detail monitor script, ensure that custom detail monitor script also has the execute permissions set.

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
Monscript	The path to the detail monitor script; the default value for this attribute is the path for the script, SqlTest.pl, provided with the agent. You must specify a value for this attribute if LevelTwoMonitorFreq is set to a positive integer value. Type and dimension: string-scalar Default value: No default value **Note:** By default, SqlTest.pl script has the execute permission set. If you specify custom detail monitor script, ensure that custom detail monitor script also has the execute permissions set.
Run_ServerFile	Specifies the location of the RUN_SERVER file for the Sybase instance. The default location of this file is used if no value is specified for this attribute. Type and dimension: string-scalar Default value: No default value

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
IMF	

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
	This resource-type level attribute determines whether the Sybase agent must perform intelligent resource monitoring. You can also override the value of this attribute at resource-level. This attribute includes the following keys: ■ Mode: Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows: ■ 0—Does not perform intelligent resource monitoring ■ 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources ■ 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources ■ 3—Performs intelligent resource monitoring for both online and for offline resources Default: 3 ■ MonitorFreq: This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer. Default: 5 You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring. If the value is 0, the agent does not perform poll-based process check monitoring. After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows: ■ After every (MonitorFreq x MonitorInterval) number of seconds for online resources ■ After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources ■ RegisterRetryLimit: If you enable intelligent resource monitoring, the agent invokes the sybase_imf_register agent function to register the resource with the AMFkernel driver. The value of the RegisterRetryLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes. Default: 3

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
	Type and dimension: Integer-association.
interfaces_File	Specifies the location of interfaces file, including the directory name and the file name for the Sybase instance. If this attribute is configured, [-I interfaces file] option is used when connecting to the isql session. If this attribute is not configured, the agent does not use the -I option. Type and dimension: string-scalar Default value: No default value For example: /sybase/my_interfaces_file **Note:** It is assumed that you have modified the RUN_ServerFile with the non-default interface file location if the interfaces_File attribute is configured.
DelayAfterOnline	Specifies the number of seconds that elapse after the Online entry point is complete and before the next monitor cycle is invoked. Type and dimension: integer-scalar Default value: 10
DelayAfterOffline	Specifies the number of seconds that elapse after the Offline entry point is complete and before the next monitor cycle is invoked. Type and dimension: integer-scalar Default value: 2
ShutdownWaitLimit	Maximum number of seconds for which the agent waits for the Sybase instance to stop after issuing the `shutdown with wait` command, and before attempting to issue the `kill -15 <data server-pid>` command, if required. Type and dimension: integer-scalar Default value: 60

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
ContainerOpts (Only Solaris 10)	This resource-type level attribute specifies the container options for the Sybase instances that run in the context of Solaris containers (zones or projects). This attribute has the following keys, which can take values 0 or 1: ■ RunInContainer (RIC) Set the key value as 1 for the Sybase agent to monitor Sybase instances running in the context of Solaris container. Set the key value as 0 if you do not want to run the Sybase resource in the context of Solaris container. Default is 1. ■ PassCInfo (PCI) Set the key value as 1 for the Sybase resource to get the container information defined in the VCS service group's ContainerInfo attribute. Set the key value as 0 if you do not want to get the container information. Default is 1. ■ PassLoadInfo (PLI) Set the key value as 1 for the Sybase resource to get the load dimensions defined in the VCS service group's Load attribute. Set the key value as 0 if you do not want to get the load information. Default is 0. See *Veritas Cluster Server Administrator's Guide* and the *Veritas Storage Foundation and High Availability Solutions Virtualization Guide*. Type and dimension: static-assoc-int
Quorum_dev	The quorum device manages the cluster membership, stores cluster configuration data and contains information shared among server instances and nodes. It must be a disk accessible to all nodes in the cluster. Specify fully qualified quorum device name. **Note:** This attribute should be specified only for cluster edition. For example: ■ /dev/vx/rdsk/Sybase_install_dg/quorum_vol ■ /quorum/qfile Type and dimension: String-scalar Default value: No default value

Table F-12 Optional attributes *(continued)*

Optional Attributes	Definition
Run_ServerFile	Specifies the location of the RUN_SERVER file of the Sybase instance. The default location of the file is used if no value is specified for this attribute. Type and dimension: String-scalar Default value: No default value

Table F-13 lists the internal attribute for Sybase agent.

This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table F-13 Internal attribute

Internal attribute	Definition
AgentDirectory	Specifies the location of the binaries, scripts, and other files related to the agent for Sybase. Type and dimension: static-string

Appendix G

Compatability issues when installing Storage Foundation for Sybase ASE CE with other products

This appendix includes the following topics:

- Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present
- Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present
- Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx, VRTSicsco, and VRTSat.

Index

T