Veritas™ Cluster Server Installation Guide

HP-UX 11i v3

5.1 Service Pack 1

Symantec

Veritas Cluster Server Installation Guide

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

Product version: 5.1 SP1

Document version: 5.1SP1.0

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

Documentation

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

https://sort.symantec.com/documents

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

docs@symantec.com

Support agreement resources

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

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

About Symantec Connect

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

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

Contents

Section 1

Installation overview and planning

Chapter 1

Introducing VCS

This chapter includes the following topics:

About Veritas Cluster Server

Veritas™ Cluster Server by Symantec is a high-availability solution for applications and services configured in a cluster. Veritas Cluster Server (VCS) monitors systems and application services, and restarts services when hardware or software fails.

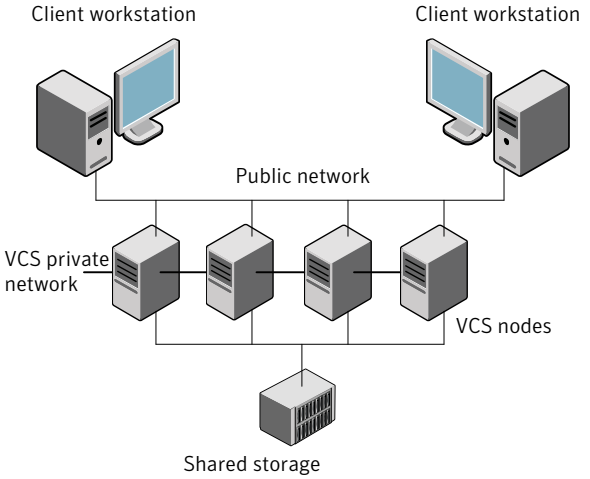
About VCS basics

A single VCS cluster consists of multiple systems that are connected in various combinations to shared storage devices. When a system is part of a VCS cluster, it is a node. VCS monitors and controls applications running in the cluster on nodes, and restarts applications in response to a variety of hardware or software faults.

Applications can continue to operate with little or no downtime. In some cases, such as NFS, this continuation is transparent to high-level applications and users. In other cases, a user might have to retry an operation, such as a Web server reloading a page.

Figure 1-1 illustrates a typical VCS configuration of four nodes that are connected to shared storage.

Figure 1-1 Example of a four-node VCS cluster



Client workstations receive service over the public network from applications running on VCS nodes. VCS monitors the nodes and their services. VCS nodes in the cluster communicate over a private network.

About multiple nodes

VCS runs in a replicated state on each node in the cluster. A private network enables the nodes to share identical state information about all resources. The private network also recognizes active nodes, the nodes that join or leave the cluster, and failed nodes. The private network requires two communication channels to guard against network partitions.

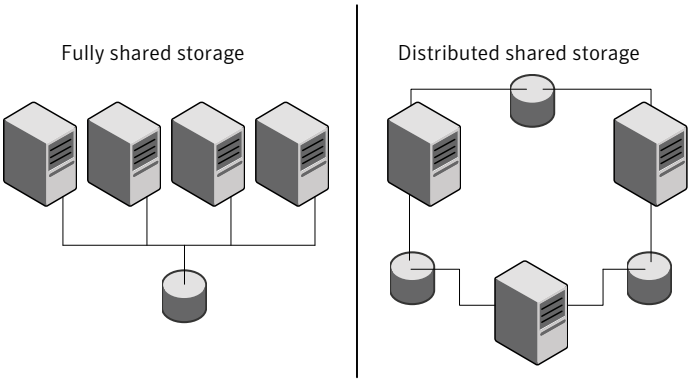
About shared storage

A VCS hardware configuration typically consists of multiple nodes that are connected to shared storage through I/O channels. Shared storage provides multiple systems with an access path to the same data. It also enables VCS to restart applications on alternate nodes when a node fails, which ensures high availability.

VCS nodes can only access physically-attached storage.

Figure 1-2 illustrates the flexibility of VCS shared storage configurations.

Figure 1-2 Two examples of shared storage configurations



About LLT and GAB

VCS uses two components, LLT and GAB, to share data over private networks among systems. These components provide the performance and reliability that VCS requires.

LLT (Low Latency Transport) provides fast, kernel-to-kernel communications, and monitors network connections.

GAB (Group Membership and Atomic Broadcast) provides the global message order that is required to maintain a synchronized state among the nodes. It monitors disk communications such as the VCS heartbeat utility.

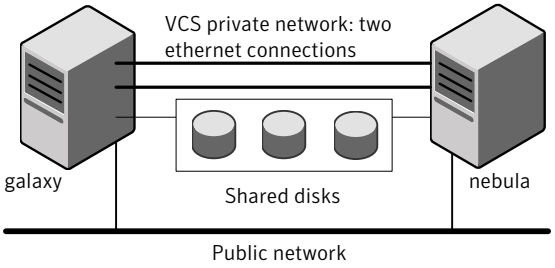
About network channels for heartbeating

For the VCS private network, two network channels must be available to carry heartbeat information. These network connections also transmit other VCS-related information.

Each HP-UX cluster configuration requires at least two network channels between the systems. The requirement for two channels protects your cluster against network partitioning. For more information on network partitioning, refer to the *Veritas Cluster Server Administrator's Guide*.

Figure 1-3 illustrates a two-node VCS cluster where the nodes galaxy and nebula have two private network connections.

Figure 1-3 Two Ethernet connections connecting two nodes



About preexisting network partitions

A preexisting network partition refers to a failure in the communication channels that occurs while the systems are down and VCS cannot respond. When the systems start, VCS seeding reduces vulnerability to network partitioning, regardless of the cause of the failure.

About VCS seeding

To protect your cluster from a preexisting network partition, VCS uses a seed. A seed is a function of GAB that determines whether or not all nodes have joined a cluster. For this determination, GAB requires that you declare the number of nodes in the cluster. Note that only seeded nodes can run VCS.

GAB automatically seeds nodes under the following conditions:

- An unseeded node communicates with a seeded node
- All nodes in the cluster are unseeded but can communicate with each other

When the last system starts and joins the cluster, the cluster seeds and starts VCS on all nodes. You can then bring down and restart nodes in any combination. Seeding remains in effect as long as at least one instance of VCS is running somewhere in the cluster.

Perform a manual seed to run VCS from a cold start when one or more systems of the cluster are unavailable. VCS does not start service groups on a system until it has a seed.

About VCS features

VCS offers the following features that you can configure during VCS configuration:

VCS notifications See "About VCS notifications" on page 25.

VCS global clusters	See "About global clusters" on page 25.
I/O fencing	See "About I/O fencing" on page 25.

About VCS notifications

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

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

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

About global clusters

Global clusters provide the ability to fail over applications between geographically distributed clusters when disaster occurs. You require a separate license to configure global clusters. You must add this license during the installation. The installer only asks about configuring global clusters if you have used the global cluster license.

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

About I/O fencing

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

The fencing operation determines the following:

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

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

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

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

Coordinator disk	I/O fencing that uses coordinator disks is referred to as disk-based I/O fencing. Disk-based I/O fencing ensures data integrity in a single cluster.
Coordination point server (CP server)	I/O fencing that uses at least one CP server system is referred to as server-based I/O fencing. Server-based I/O fencing ensures data integrity in multiple clusters. In virtualized environments that do not support SCSI-3 PR, VCS supports non-SCSI3 server-based I/O fencing.

Note: Symantec recommends that you use I/O fencing to protect your cluster against split-brain situations.

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

About VCS optional components

You can add the following optional components to VCS:

Symantec Product Authentication Service	See "About Symantec Product Authentication Service (AT)" on page 26.
Veritas Operations Manager	See "Veritas Operations Manager" on page 27.
Cluster Manager (Java console)	See "About Cluster Manager (Java Console)" on page 27.
VCS Simulator	See About VCS Simulator on page 28.

About Symantec Product Authentication Service (AT)

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

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

- Root broker

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

- Authentication brokers
  Authentication brokers serve as intermediate registration and certification authorities. Authentication brokers have root-signed certificates. Each node in VCS serves as an authentication broker.

See Symantec Product Authentication Service documentation for more information.

See "Preparing to configure the clusters in secure mode" on page 89.

Veritas Operations Manager

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

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

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

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

About Cluster Manager (Java Console)

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

See *Veritas Cluster Server Administrator's Guide*.

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

About VCS Simulator

VCS Simulator enables you to simulate and test cluster configurations. Use VCS Simulator to view and modify service group and resource configurations and test failover behavior. VCS Simulator can be run on a stand-alone system and does not require any additional hardware. You can install VCS Simulator only on a Windows operating system.

VCS Simulator runs an identical version of the VCS High Availability Daemon (HAD) as in a cluster, ensuring that failover decisions are identical to those in an actual cluster.

You can test configurations from different operating systems using VCS Simulator. For example, you can run VCS Simulator to test configurations for VCS clusters on Windows, AIX, HP-UX, Linux, and Solaris operating systems. VCS Simulator also enables creating and testing global clusters.

You can administer VCS Simulator from the Java Console or from the command line.

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

Symantec Operations Readiness Tools

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

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

To access SORT, go to:

http://sort.symantec.com

About configuring VCS clusters for data integrity

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

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

- Broken set of private networks
  If a system in a two-node cluster fails, the system stops sending heartbeats over the private interconnects. The remaining node then takes corrective

action. The failure of the private interconnects, instead of the actual nodes, presents identical symptoms and causes each node to determine its peer has departed. This situation typically results in data corruption because both nodes try to take control of data storage in an uncoordinated manner.

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

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

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

See "About planning to configure I/O fencing" on page 98.

About I/O fencing for VCS in virtual machines that do not support SCSI-3 PR

In a traditional I/O fencing implementation, where the coordination points are coordination point servers (CP servers) or coordinator disks, Veritas Clustered Volume Manager and Veritas I/O fencing modules provide SCSI-3 persistent reservation (SCSI-3 PR) based protection on the data disks. This SCSI-3 PR protection ensures that the I/O operations from the losing node cannot reach a disk that the surviving sub-cluster has already taken over.

See the *Veritas Cluster Server Administrator's Guide* for more information on how I/O fencing works.

In virtualized environments that do not support SCSI-3 PR, VCS attempts to provide reasonable safety for the data disks. VCS requires you to configure non-SCSI3 server-based I/O fencing in such environments. Non-SCSI3 fencing uses CP servers as coordination points with some additional configuration changes to support I/O fencing in such environments.

See "Setting up non-SCSI3 server-based I/O fencing using installvcs program" on page 162.

See "Setting up non-SCSI3 fencing in virtual environments manually" on page 244.

About I/O fencing components

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

- Data disks—Store shared data
  See "About data disks" on page 30.
- Coordination points—Act as a global lock during membership changes
  See "About coordination points" on page 30.

About data disks

Data disks are standard disk devices for data storage and are either physical disks or RAID Logical Units (LUNs).

These disks must support SCSI-3 PR and must be part of standard VxVM disk groups. VxVM is responsible for fencing data disks on a disk group basis. Disks that are added to a disk group and new paths that are discovered for a device are automatically fenced.

About coordination points

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

Note: Typically, a fencing configuration for a cluster must have three coordination points. Symantec also supports server-based fencing with a single CP server as its only coordination point with a caveat that this CP server becomes a single point of failure.

The coordination points can be disks, servers, or both.

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

  Dynamic Multi-pathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. On cluster nodes with HP-UX 11i v3, you must use DMP devices or iSCSI devices

for I/O fencing. The following changes in HP-UX 11i v3 require you to not use raw devices for I/O fencing:

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

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

- Coordination point servers

  The coordination point server (CP server) is a software solution which runs on a remote system or cluster. CP server provides arbitration functionality by allowing the VCS cluster nodes to perform the following tasks:

  - Self-register to become a member of an active VCS cluster (registered with CP server) with access to the data drives
  - Check which other nodes are registered as members of this activeVCS cluster
  - Self-unregister from this active VCS cluster
  - Forcefully unregister other nodes (preempt) as members of this active VCS cluster

  In short, the CP server functions as another arbitration mechanism that integrates within the existing I/O fencing module.

  Note: With the CP server, the fencing arbitration logic still remains on the VCS cluster.

  Multiple VCS clusters running different operating systems can simultaneously access the CP server. TCP/IP based communication is used between the CP server and the VCS clusters.

About preferred fencing

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

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

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

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

See "Enabling or disabling the preferred fencing policy" on page 162.

Chapter 2

System requirements

This chapter includes the following topics:

Important preinstallation information for VCS

Before you install VCS, make sure that you have reviewed the following information:

- The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit the following URL:
  http://entsupport.symantec.com/docs/330441
  Before installing or upgrading VCS, review the current compatibility list to confirm the compatibility of your hardware and software.
- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:
  http://www.symantec.com/docs/TECH144835
- You can install VCS on clusters of up to 32 systems.

VCS is capable of supporting clusters with up to 64 nodes. Symantec has tested and qualified VCS configurations of up to 32 nodes at the time of the release. For more updates on this support, see the Late-Breaking News TechNote. Every system where you want to install VCS must meet the hardware and the software requirements.

Hardware requirements for VCS

Table 2-1 lists the hardware requirements for a VCS cluster.

Table 2-1 Hardware requirements for a VCS cluster

Item	Description
VCS nodes	From 1 to 32 HP (Itanium or PA-RISC) systems running HP-UX 11i v3. **Note:** VCS is capable of supporting clusters with up to 64 nodes. Symantec has tested and qualified VCS configurations of up to 32 nodes at the time of the release. For more updates on this support, see the Late-Breaking News TechNote. See "Important preinstallation information for VCS" on page 33.
DVD drive	One drive in a system that can communicate to all the nodes in the cluster.
Disks	Typical VCS configurations require that shared disks support the applications that migrate between systems in the cluster. The VCS I/O fencing feature requires that all data and coordinator disks support SCSI-3 Persistent Reservations (PR). **Note:** On HP-UX 11i v3, you must use only DMP disk devices for I/O fencing. See "About planning to configure I/O fencing" on page 98.

Table 2-1 Hardware requirements for a VCS cluster *(continued)*

Item	Description
Disk space	To run VCS, LLT, GAB, the Web Console, and the Java Console, each VCS node requires the following file system space: ■ 620 MB in /var If you do not have enough free space in /var, then use the `installvcs` command with `tmppath` option. Make sure that the specified tmppath file system has the required free space. ■ 350 MB in /opt ■ 20 MB in /usr ■ 2 MB in / **Note:** VCS may require more temporary disk space during installation than the specified disk space.
Network Interface Cards (NICs)	In addition to the built-in public NIC, VCS requires at least one more NIC per system. Symantec recommends two additional NICs. You can also configure aggregated interfaces. Symantec recommends that you turn off the spanning tree on the LLT switches, and set port-fast on.
Fibre Channel or SCSI host bus adapters	Typical VCS configuration requires at least one SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.
RAM	Each VCS node requires at least 1024 megabytes.

Required disk space for VCS

Confirm that your system has enough free disk space to install VCS.

Table 2-2 shows the approximate disk space usage by directory for the Veritas Cluster Server depots.

Table 2-2 Disk space requirements and totals

Depots	/	/opt	/usr	/var	Totals
Required	3 MB	241 MB	8 MB	1 MB	250 MB
Optional	1 MB	51 MB	0 MB	7 MB	58 MB
Required and optional total	4 MB	292 MB	8 MB	8 MB	308 MB

Note: If you do not have enough free space in /var, then use the `installvcs` command with `tmppath` option. Make sure that the specified tmppath file system has the required free space.

Supported HP-UX operating systems

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

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

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

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

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

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

Supported software for VCS

VCS supports the following volume managers and file systems:

- Logical Volume Manager (LVM)
- HP File System (HFS)
- Veritas Storage Foundation (SF): Veritas Volume Manager (VxVM) with Veritas File System (VxFS)

  VCS 5.1 SP1 supports the following versions of SF:

  - SF 5.1 SP1
    - VxVM 5.1 SP1 with VxFS 5.1 SP1
  - SF 5.0.1
    - VxVM 5.0.1 with VxFS 5.0.1

Note: VCS supports the previous version of SF and the next version of SF to facilitate product upgrades.

I/O fencing requirements

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

- Coordinator disks
  See "Coordinator disk requirements for I/O fencing" on page 37.
- CP servers
  See "CP server requirements" on page 37.

To configure disk-based fencing or to configure server-based fencing with at least one coordinator disk, make sure a version of Veritas Volume Manager (VxVM) that supports SCSI-3 persistent reservations (SCSI-3 PR) is installed on the VCS cluster.

See the *Veritas Storage Foundation and High Availability Installation Guide*.

If you have installed VCS in a virtual environment that is not SCSI-3 PR compliant, review the requirements to configure non-SCSI3 server-based fencing.

See "Non-SCSI3 I/O fencing requirements" on page 40.

Coordinator disk requirements for I/O fencing

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

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

CP server requirements

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

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

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

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

See the *Veritas Storage Foundation High Availability Installation Guide*.

See "Hardware requirements for VCS" on page 34.

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

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

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

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

Table 2-3 CP server hardware requirements

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

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

Table 2-4 CP server supported operating systems and versions

CP server	Operating system and version

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

Following are the CP server networking requirements and recommendations:

- Symantec recommends that network access from the application clusters to the CP servers should be made highly-available and redundant. The network connections require either a secure LAN or VPN.
- The CP server uses the TCP/IP protocol to connect to and communicate with the application clusters by these network paths. The CP server listens for messages from the application clusters using TCP port 14250. This is the default port that can be changed during a CP server configuration.
- The CP server supports either Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with the application clusters. If the CP server is configured to use an IPv6 virtual IP address, then the application clusters should also be on the IPv6 network where the CP server is being hosted.
- When placing the CP servers within a specific network configuration, you must take into consideration the number of hops from the different application cluster nodes to the CP servers. As a best practice, Symantec recommends that the number of hops from the different application cluster nodes to the CP servers should be equal. This ensures that if an event occurs that results in an I/O fencing scenario, there is no bias in the race due to the number of hops between the nodes.

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

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

For information about establishing secure communications between the application cluster and CP server, see the *Veritas Cluster Server Administrator's Guide*.

Non-SCSI3 I/O fencing requirements

Supported virtual environment for non-SCSI3 fencing:

- HP-UX Integrity Virtual Machines (IVM) Server 4.0 and 4.1

Make sure that you also meet the following requirements to configure non-SCSI3 fencing in the virtual environments that do not support SCSI-3 PR:

- VCS must be configured with Cluster attribute UseFence set to SCSI3
- All coordination points must be CP servers

Number of nodes supported

VCS is capable of supporting cluster configurations with up to 64 nodes. Symantec has tested and qualified configurations of up to 32 nodes on IA-64 (Itanium) at the time of the release.

For more updates on this support, see the Late-Breaking News TechNote on the Symantec Technical Support website:

http://www.symantec.com/docs/TECH144835

Chapter 3

Planning to install VCS

This chapter includes the following topics:

VCS installation methods

Table 3-1 lists the different methods you can choose to install and configure VCS:

Table 3-1 VCS installation methods

Method	Description
Interactive installation using the script-based installer	You can use one of the following script-based installers: ■ Veritas product installer Use to install and configure multiple Veritas products. ■ installvcs program Use to install and configure just VCS. The script-based installer asks you a series of questions and installs and configures VCS based on the information you provide.
Interactive installation using the web-based installer	You can use a web-interface to install and configure VCS.

Table 3-1 VCS installation methods *(continued)*

Method	Description
Automated installation using the VCS response files	At the end of each successful simulated or actual installation and configuration, the installer creates response files. You can use these response files to perform multiple installations to set up a large VCS cluster.
Manual installation using the HP-UX commands and utilities	You can install VCS using the operating system swinstall command and then manually configure VCS.

About the VCS installation program

You can access the installvcs program from the command line or through the Veritas product installer.

The VCS installation program is interactive and manages the following tasks:

- Licensing VCS
- Installing VCS depots on multiple cluster systems
- Configuring VCS, by creating several detailed configuration files on each system
- Starting VCS processes

You can choose to configure different optional features, such as the following:

- SNMP and SMTP notification
- The Symantec Product Authentication Services feature
- The wide area Global Cluster feature
- Cluster Virtual IP address

Review the highlights of the information for which installvcs program prompts you as you proceed to configure.

See "About preparing to install VCS" on page 59.

The uninstallvcs program, a companion to installvcs program, uninstalls VCS depots.

See "Preparing to uninstall VCS" on page 313.

Features of the script-based installer

The script-based installer supports installing, configuring, upgrading, and uninstalling VCS. In addition, the script-based installer also provides command options to perform the following tasks:

- Check the systems for VCS installation requirements.
  See "Performing automated preinstallation check" on page 70.
- Upgrade VCS if a previous version of VCS currently runs on a cluster.
  See "Upgrading VCS using the script-based installer" on page 258.
- Start or stop VCS processes
  See "Starting and stopping processes for the Veritas products " on page 436.
- Enable or disable a cluster to run in secure mode using Symantec Product Authentication Service (VxAT)
  See the *Veritas Cluster Server Administrator's Guide*.
- Configure I/O fencing for the clusters to prevent data corruption
  See "Setting up disk-based I/O fencing using installvcs program" on page 143.
  See "Setting up server-based I/O fencing using installvcs program" on page 150.
  See "Setting up non-SCSI3 server-based I/O fencing using installvcs program" on page 162.
- Create a single-node cluster
  See "Creating a single-node cluster using the installer program" on page 412.
- Add a node to an existing cluster
  See "Adding nodes using the VCS installer" on page 331.
- Perform automated installations using the values that are stored in a configuration file.
  See "Installing VCS using response files" on page 181.
  See "Configuring VCS using response files" on page 187.
  See "Upgrading VCS using response files" on page 277.

Interacting with the installvcs program

As you run the program, you are prompted to answer yes or no questions. A set of responses that resemble **[y, n, q, ?] (y)** typically follow these questions. The response within parentheses is the default, which you can select by pressing the Enter key. Enter the **?** character to get help to answer the prompt. Enter **q** to quit the installation.

Installation of VCS depots takes place only after you have confirmed the information. However, you must remove the partially installed VCS files before you run the installvcs program again.

See "Preparing to uninstall VCS" on page 313.

During the installation, the installer prompts you to type information. The installer expects your responses to be within a certain range or in a specific format. The installer provides examples. If you are prompted to enter an item from a list, enter your selection exactly as it is shown in the list.

The installer also prompts you to answer a series of questions that are related to a configuration activity. For such questions, you can enter the **b** character to return to the first prompt in the series. When the installer displays a set of information items you have entered, you are prompted to confirm it. If you answer **n**, the program lets you reenter all of the information for the set.

You can install the VCS Java Console on a single system, which is not required to be part of the cluster. Note that the installvcs program does not install the VCS Java Console.

See "Installing the Java Console" on page 293.

About the Web-based installer

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

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

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

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

The location of the Veritas XPortal Server configuration file is `/var/opt/webinstaller/xprtlwid.conf`.

See "Before using the Veritas Web-based installer" on page 167.

See "Starting the Veritas Web-based installer" on page 168.

Features not supported with Web-based installer

In this release, the following features that can be performed using the script installer are not available in the Web-based installer:

- Configuring server-based I/O fencing
- Configuring non-SCSI3 I/O fencing in virtual environments where SCSI3 is not supported

About response files

The installer generates a "response file" after performing an installer task such as installation, configuration, uninstallation, or upgrade. These response files contain the details that you provided to the installer questions in the form of values for the response file variables. The response file also contains descriptions and explanations of the variables and their values.

You can also create a response file using the `-makeresponsefile` option of the installer.

The installer displays the location of the response file at the end of each successful installer task. The installer saves the response file in the default location for the install-related log files: /opt/VRTS/install/logs. If you provided a different log path using the `-logpath` option, the installer saves the response file in the path that you specified.

The format of the response file name is:
/opt/VRTS/install/logs/*installscript-YYYYMMDDHHSSxxx*
/*installscript-YYYYMMDDHHSSxxx*.response, where:

- *installscript* may be, for example: installer, webinstaller, installvcs program, or uninstallvcs program
- *YYYYMMDDHHSS* is the current date when the *installscript* is run and *xxx* are three random letters that the script generates for an installation instance

For example:
/opt/VRTS/install/logs/installer-200910101010ldS/installer-200910101010ldS.response

You can customize the response file as required to perform unattended installations using the `-responsefile` option of the installer. This method of automated installations is useful in the following cases:

- To perform multiple installations to set up a large VCS cluster.
See "Installing VCS using response files" on page 181.
- To upgrade VCS on multiple systems in a large VCS cluster.
See "Upgrading VCS using response files" on page 277.
- To uninstall VCS from multiple systems in a large VCS cluster.
See "Uninstalling VCS using response files" on page 321.

Syntax in the response file

The syntax of the Perl statements that are included in the response file variables varies. It can depend on whether the variables require scalar or list values.

For example, in the case of a string value:

```
$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"];
```

Typical VCS cluster setup models

VCS clusters support different failover configurations, storage configurations, and cluster topologies.

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

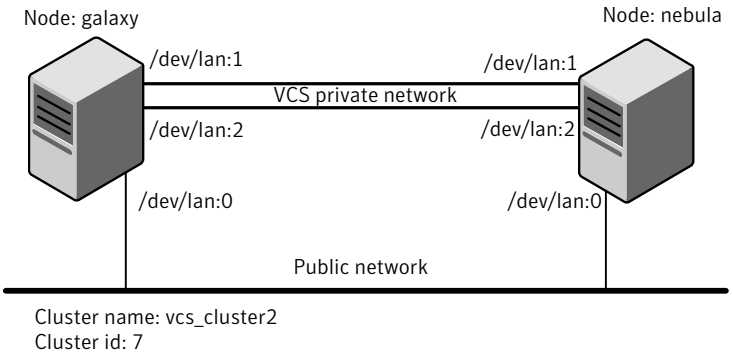
Some of the typical VCS setup models are as follows:

- Basic VCS cluster with two nodes
  See "Typical configuration of two-node VCS cluster" on page 48.
- VCS clusters in secure mode using Symantec Product Authentication Service (AT)
  See "Typical configuration of VCS clusters in secure mode" on page 49.
- VCS clusters centrally managed using Veritas Operations Manager (VOM)
  See "Typical configuration of VOM-managed VCS clusters" on page 50.
- VCS clusters with I/O fencing for data protection
  See "Typical VCS cluster configuration with disk-based I/O fencing" on page 101.
  See "Typical VCS cluster configuration with server-based I/O fencing" on page 102.
- VCS clusters such as global clusters, replicated data clusters, or campus clusters for disaster recovery
  See the *Veritas Cluster Server Administrator's Guide* for disaster recovery cluster configuration models.

Typical configuration of two-node VCS cluster

Figure 3-1 illustrates a simple VCS cluster setup with two nodes.

Figure 3-1 Typical two-node VCS cluster



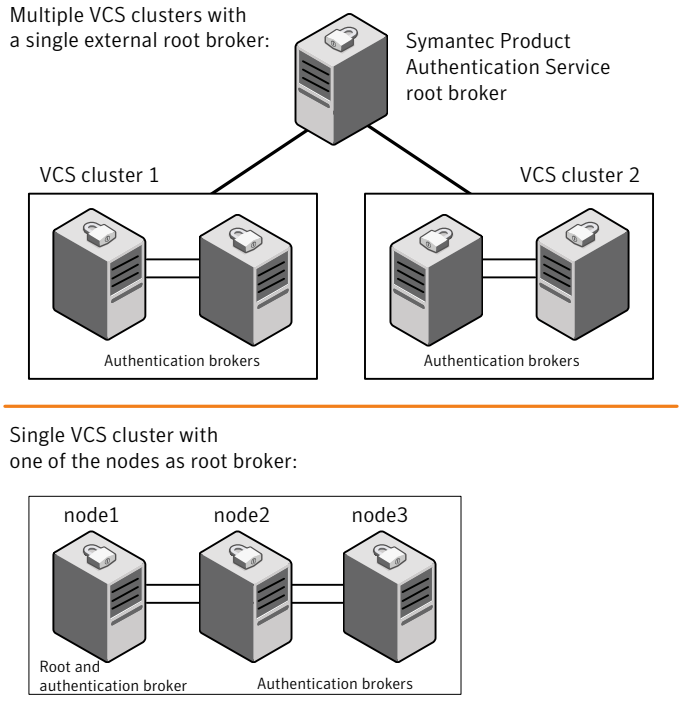
Typical configuration of VCS clusters in secure mode

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

See "About Symantec Product Authentication Service (AT)" on page 26.

Figure 3-2 illustrates typical configuration of VCS clusters in secure mode. You can use one of the cluster nodes as AT root broker or you can use a stable system outside the cluster as AT root broker.

Figure 3-2 Typical configuration of VCS clusters in secure mode



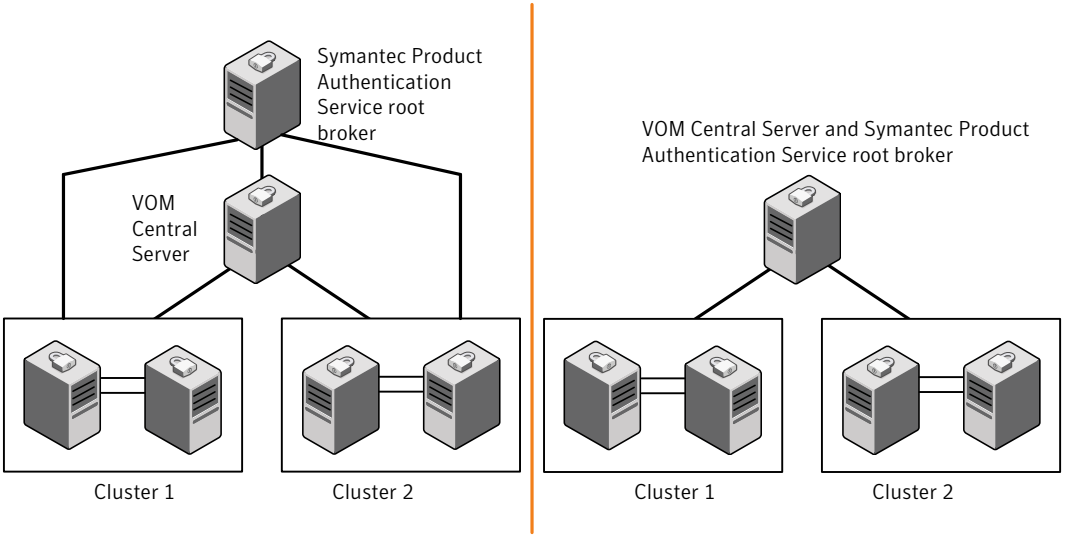
Typical configuration of VOM-managed VCS clusters

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

See "Veritas Operations Manager" on page 27.

Figure 3-3 illustrates a typical setup of VCS clusters that are centrally managed using Veritas Operations Manager. You can install Symantec Product Authentication Service root broker on the same system as that of VOM Central Server or on a different system.

Figure 3-3 Typical configuration of VOM-managed clusters



Chapter 4

Licensing VCS

This chapter includes the following topics:

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

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

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 216.
  See the `vxkeyless(1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
  See "Installing Veritas product license keys" on page 55.
  See the `vxlicinst(1m)` manual page.

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

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

Obtaining VCS license keys

If you decide to not use the keyless licensing, you must obtain and install a license key for VCS.

See "About Veritas product licensing" on page 53.

This product includes a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased. A single key lets you install the product on the number and type of systems for which you purchased the

license. A key may enable the operation of more products than are specified on the certificate. However, you are legally limited to the number of product licenses purchased. The product installation procedure describes how to activate the key.

To register and receive a software license key, go to the Symantec Licensing Portal at the following location:

https://licensing.symantec.com

Make sure you have your Software Product License document. You need information in this document to retrieve and manage license keys for your Symantec product. After you receive the license key, you can install the product.

Click the Help link at this site to access the *License Portal User Guide* and FAQ.

The VRTSvlic depot enables product licensing. For information about the commands that you can use after the installing VRTSvlic:

See "Installing Veritas product license keys" on page 55.

You can only install the Symantec software products for which you have purchased a license. The enclosed software discs might include other products for which you have not purchased a license.

Installing Veritas product license keys

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin

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

Section 2

Preinstallation tasks

Chapter 5

Preparing to install VCS

This chapter includes the following topics:

About preparing to install VCS

Before you perform the preinstallation tasks, make sure you reviewed the installation requirements, set up the basic hardware, and planned your VCS setup.

See "Important preinstallation information for VCS" on page 33.

Performing preinstallation tasks

Table 5-1 lists the tasks you must perform before proceeding to install VCS.

Table 5-1 Preinstallation tasks

Task	Reference
Obtain license keys if you do not want to use keyless licensing.	See "Obtaining VCS license keys" on page 54.
Set up the private network.	See "Setting up the private network" on page 60.
Enable communication between systems.	See "Setting up inter-system communication" on page 431.

Table 5-1 Preinstallation tasks *(continued)*

Task	Reference
Set up ssh on cluster systems.	See "Setting up ssh on cluster systems" on page 431.
Set up shared storage for I/O fencing (optional)	See "Setting up shared storage" on page 63.
Set the PATH and the MANPATH variables.	See "Setting the PATH variable" on page 67. See "Setting the MANPATH variable" on page 68.
Review basic instructions to optimize LLT media speeds.	See "Optimizing LLT media speed settings on private NICs" on page 68.
Review guidelines to help you set the LLT interconnects.	See "Guidelines for setting the media speed of the LLT interconnects" on page 68.
Mount the product disc	See "Mounting the product disc" on page 69.
Verify the systems before installation	See "Performing automated preinstallation check" on page 70.

Setting up the private network

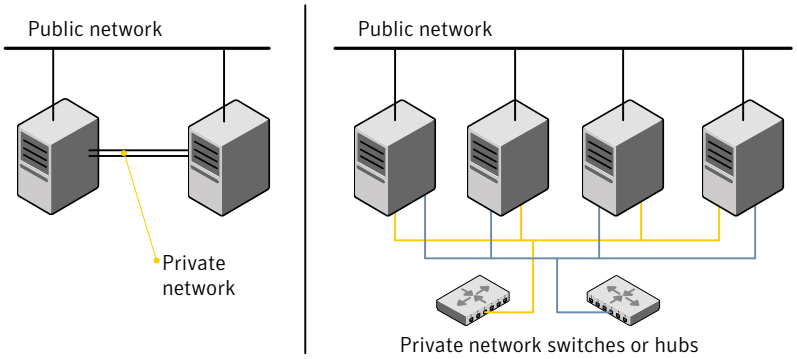
VCS requires you to set up a private network between the systems that form a cluster. You can use either NICs or aggregated interfaces to set up private network.

You can use network switches instead of hubs.

Refer to the *Veritas Cluster Server Administrator's Guide* to review VCS performance considerations.

Figure 5-1 shows two private networks for use with VCS.

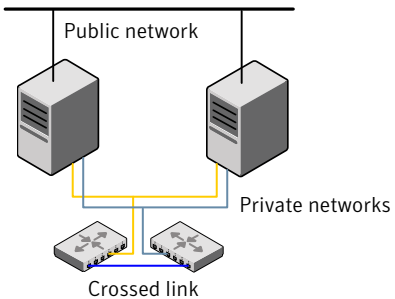
Figure 5-1 Private network setups: two-node and four-node clusters



Symantec recommends configuring two independent networks between the cluster nodes with a network switch for each network. You can also interconnect multiple layer 2 switches for advanced failure protection. Such connections for LLT are called cross-links.

Figure 5-2 shows a private network configuration with crossed links between the network switches.

Figure 5-2 Private network setup with crossed links



To set up the private network

1 Install the required network interface cards (NICs).

Create aggregated interfaces if you want to use these to set up private network.

2 Connect the VCS private NICs on each system.

3 Use crossover Ethernet cables, switches, or independent hubs for each VCS communication network. Note that the crossover Ethernet cables are supported only on two systems.

Ensure that you meet the following requirements:

- The power to the switches or hubs must come from separate sources.
- On each system, you must use two independent network cards to provide redundancy.
- If a network interface is part of an aggregated interface, you must not configure the network interface under LLT. However, you can configure the aggregated interface under LLT.
- When you configure Ethernet switches for LLT private interconnect, disable the spanning tree algorithm on the ports used for the interconnect.

During the process of setting up heartbeat connections, consider a case where a failure removes all communications between the systems.

Note that a chance for data corruption exists under the following conditions:

- The systems still run, and
- The systems can access the shared storage.

4 Test the network connections. Temporarily assign network addresses and use `telnet` or `ping` to verify communications.

LLT uses its own protocol, and does not use TCP/IP. So, you must ensure that the private network connections are used only for LLT communication and not for TCP/IP traffic. To verify this requirement, unplumb and unconfigure any temporary IP addresses that are configured on the network interfaces.

The installer configures the private network in the cluster during configuration.

You can also manually configure LLT.

See "Configuring LLT manually" on page 219.

About configuring ssh or remsh using the Veritas installer

The installer can configure passwordless secure shell (ssh) or remote shell (remsh) communications among systems. The installer uses the ssh or remsh daemon that comes bundled with the operating system. During an installation, you choose the communication method that you want to use. You then provide the installer with the superuser passwords for the systems where you plan to install. Note that for security reasons, the installation program neither stores nor caches these passwords. The ssh or remsh communication among the systems is removed when the installation process completes, unless the installation abruptly terminates. If installation terminated abruptly, use the installation script's `-comcleanup` option to remove the ssh or remsh configuration from the systems.

In most installation, configuration, upgrade (where necessary), and uninstallation scenarios, the installer can configure ssh or remsh on the target systems. In the following scenarios, you need to set up ssh or remsh manually:

- When the root broker is outside of the cluster that you plan to configure.
- When you add new nodes to an existing cluster.
- When the nodes are in a sub-cluster during a phased upgrade.
- When you perform installer sessions using a response file.

See "Setting up inter-system communication" on page 431.

Setting up shared storage

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

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

See "About planning to configure I/O fencing" on page 98.

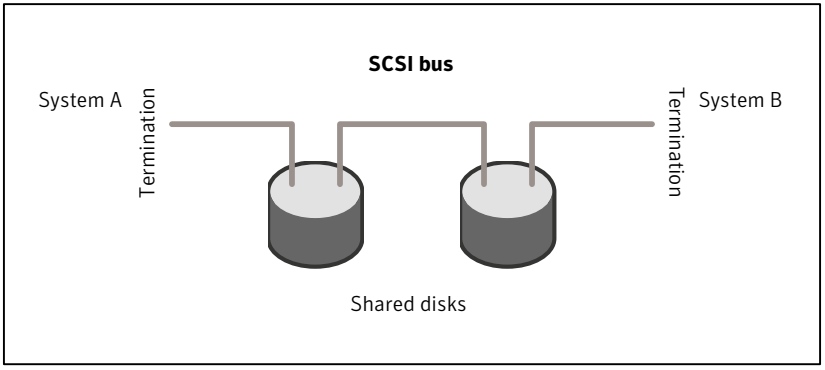
See also the *Veritas Cluster Server Administrator's Guide* for a description of I/O fencing.

Setting up shared storage: SCSI

Perform the following steps to set up shared storage.

Figure 5-3 shows how to cable systems for shared storage.

Figure 5-3 Cabling the shared storage



To set up shared storage

1. Shut down the systems in the cluster.
2. Install the required SCSI host bus adapters and set up the external shared SCSI storage devices.
3. Cable the external shared storage devices. With cables connected to shared storage between two systems, you must terminate the two ends of the SCSI bus on the systems. as shown in the figure.

   For more than two systems, disable SCSI termination on the systems that are not positioned at the ends of the SCSI chain.

Checking and changing SCSI Initiator IDs

The SCSI Initiator IDs for the host bus adapters (HBAs) on each of the systems that access the shared storage must be unique. So, you may have to change the HBA SCSI ID on one or more systems if these IDs are the same. Typically, the host bust adapters (HBAs) for the SCSI devices are shipped with a default SCSI ID of 7. Use the following procedure to check SCSI IDs and change them if necessary.

To check and change SCSI initiator IDs

1. For systems with PA architecture, turn on the power of the first system. During the boot process, the system delays for ten seconds, giving you the opportunity to stop the boot process and enter the boot menu:

   ```
   To discontinue, press any key within 10 seconds.
   ```

   Press any key. The boot process discontinues.

   ```
   Boot terminated.
   ```

2. When you see the boot Main Menu, display the Information Menu by entering:

   ```
   Main Menu: enter command or menu > in
   ```

3 From the Information Menu, enter "io" at the prompt for I/O interface information:

```
Information Menu: Enter command > io
```

The output shows information about the I/O interfaces and resembles:

```
Path       Bus     Slot    Vendor   Device
  Description      (dec)      #      #          Id           Id
  -----------      ----       ---    -----      ------     ------
  .
  .
  SCSI bus cntlr   0/3/0/0   24     10         0x1000     0xf
  .
```

4 Return to the Main Menu:

```
  Information Menu: Enter command > main
```

5 Go the Service Menu:

```
  Main Menu: enter command or menu > ser
```

6 Display the host bus adapter's SCSI ID:

```
  Service Menu: enter command or menu > scsi
```

The output displays information about the SCSI devices:

```
 Path (dec)        Initiator  ID    SCSI Rate    Auto Term
--------------   ------------       ---------    ---------
0/3/0/0          7                  Fast         Unknown
```

The output in this example shows the SCSI ID is 7, the preset default for the HBA as shipped.

- If you choose, you can leave the ID set at 7 and return to the Main Menu:

```
Service Menu: enter command or menu > main
```

- You can change the SCSI ID for the HBA. For example, to change the SCSI ID from 7 to 6, you would enter:

```
Service Menu: Enter command > SCSI init 0/3/0/0 6
FAST
```

- To verity the change, enter "SCSI" at the prompt:

```
                Service Menu: Enter command > SCSI

              Path (dec)    Initiator ID   SCSI Rate   Auto

   Term
          --------------   ------------ ---------
              0/3/0/0      6             Fast         Unknown
```

7 Return to the Main Menu:

```
    Service Menu: enter command or menu > main
```

8 At the Main Menu, enter the command to boot the system. Answer "n" when you are prompted to interact with IPL:

```
Menu: Enter command or menu > boot
Interact with IPL (Y, N, or Cancel)?> n

Booting...
```

Setting up shared storage: Fibre Channel

Perform the following steps to set up Fibre Channel.

To set up Fibre Channel shared storage

1 Shut down the cluster systems that must share the devices.

2 Install the required Fibre Channel host bus adapters on each system.

3 Cable the shared devices.

4 Reboot each system.

5 Verify that each system can see all shared devices. Use the command:

```
# ioscan -fnC disk
```

Where "disk" is the class of devices to be shared. For example, from a system galaxy type:

```
galaxy# ioscan -fnC disk
Class  I  H/W Path     Driver S/W State   H/W Type  Description
===========================================================
.
.
disk      4  0/4/0/0.1.16.255.13.4.0  sdisk  CLAIMED     DEVICE
SEAGATE ST318304 CLAR18
                /dev/dsk/c4t4d0   /dev/rdsk/c4t4d0
disk      5  0/4/0/0.1.16.255.13.5.0  sdisk  CLAIMED     DEVICE
SEAGATE ST318304 CLAR18
                  /dev/dsk/c4t5d0   /dev/rdsk/c4t5d0
.
.
```

And on another system, nebula, enter:

```
nebula# ioscan -fnC disk
Class  I  H/W Path     Driver S/W State   H/W Type  Description
===========================================================
.
.
disk      4  0/4/0/0.1.16.255.13.4.0  sdisk  CLAIMED     DEVICE
SEAGATE ST318304 CLAR18
                  /dev/dsk/c4t4d0   /dev/rdsk/c4t4d0
disk      5  0/4/0/0.1.16.255.13.5.0  sdisk  CLAIMED     DEVICE
   SEAGATE ST318304 CLAR18
                  /dev/dsk/c4t5d0   /dev/rdsk/c4t5d0
.
.
```

Setting the PATH variable

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

If you have any custom scripts located in /opt/VRTSvcs/bin directory, make sure to add the /opt/VRTSvcs/bin directory to your PATH environment variable.

To set the PATH variable

- Do one of the following:
  - For the Bourne Shell (sh or ksh), type:

    ```
    $ PATH=/opt/VRTS/bin:$PATH; export PATH
    ```

  - For the C Shell (csh or tcsh), type:

    ```
    $ setenv PATH :/opt/VRTS/bin:$PATH
    ```

Setting the MANPATH variable

Set the MANPATH variable to view the manual pages.

To set the MANPATH variable

- Do one of the following:
  - For the Bourne Shell (sh or ksh), type:

    ```
    $ MANPATH=/opt/VRTS/man:$MANPATH; export MANPATH
    ```

  - For the C Shell (csh or tcsh), type:

    ```
    % setenv MANPATH /usr/share/man:/opt/VRTS/man
    ```

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.

Mounting the product disc

You must have superuser (root) privileges to load the VCS software.

To mount the product disc

1. Log in as superuser on a system where you want to install VCS.

   The system from which you install VCS need not be part of the cluster. The systems must be in the same subnet.
2. Insert the product disc in the appropriate drive on your local system.
3. Determine the block device file for the DVD drive:

   ```
   # ioscan -fnC disk
   ```

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

   ```
   # mkdir -p /dvdrom
   # mount /dev/rdsk/c0t0d0 /dvdrom
   ```
5. Verify that the disc is mounted:

   ```
   # mount
   ```

Performing automated preinstallation check

Before you begin the installation of VCS software, you can check the readiness of the systems where you plan to install VCS. The command to start the preinstallation check is:

```
installvcs -precheck system1 system2 ...
```

See "Symantec Operations Readiness Tools" on page 28.

You can use the Veritas Operation Services to assess your setup for VCS installation.

To check the systems

1. Navigate to the folder that contains the installvcs program.

   ```
   # cd /dvdrom/cluster_server
   ```

2. Start the preinstallation check:

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

   The program proceeds in a noninteractive mode to examine the systems for licenses, depots, disk space, and system-to-system communications.

3. Review the output as the program displays the results of the check and saves the results of the check in a log file.

   See "Command options for installvcs program" on page 369.

Reformatting VCS configuration files on a stopped cluster

When you manually edit VCS configuration files (for example, the main.cf or types.cf file) you can potentially create formatting issues that may cause the installer to interpret the cluster configuration information incorrectly.

If you have manually edited any of the configuration files, you need to perform one of the following before you run the installation program:

- On a running cluster, perform an `haconf -dump` command. This command saves the configuration files and ensures that they do not have formatting errors before you run the installer.
- On cluster that is not running, perform the `hacf -cftocmd` and then the `hacf -cmdtocf` commands to format the configuration files.

Note: Remember to make back up copies of the configuration files before you edit them.

You also need to use this procedure if you have manually changed the configuration files before you perform the following actions using the installer:

- Upgrade VCS
- Uninstall VCS

For more information about the main.cf and types.cf files, refer to the *Veritas Cluster Server Administrator's Guide*.

To display the configuration files in the correct format on a running cluster

- Run the following commands to display the configuration files in the correct format:

```
# haconf -dump
```

To display the configuration files in the correct format on a stopped cluster

- Run the following commands to display the configuration files in the correct format:

```
# hacf -cftocmd config

# hacf -cmdtocf config
```

Getting your VCS installation and configuration information ready

The VCS installer prompts you for some information during the installation and configuration process. Review the following information and make sure you have made the necessary decisions and you have the required information ready before you perform the installation and configuration.

Table 5-2 lists the information you need to install the VCS depots.

Table 5-2 Information to install the VCS depots

Information	Description and sample value	Your value
System names	The system names where you plan to install VCS Example: **galaxy**, **nebula**	

Table 5-2 Information to install the VCS depots *(continued)*

Information	Description and sample value	Your value
The required license keys	If you decide to use keyless licensing, you do not need to obtain license keys. However, you require to set up management server within 60 days to manage the cluster. See "About Veritas product licensing" on page 53. Depending on the type of installation, keys can include: ■ A valid site license key ■ A valid demo license key ■ A valid license key for VCS global clusters See "Obtaining VCS license keys" on page 54.	
Decide which depots to install	■ Minimum depots—provides basic VCS functionality. ■ Recommended depots—provides full functionality of VCS without advanced features. ■ All depots—provides advanced feature functionality of VCS. The default option is to install the recommended depots. See "Viewing the list of VCS depots" on page 214.	

Table 5-3 lists the information you need to configure VCS cluster name and ID.

Table 5-3 Information you need to configure VCS cluster name and ID

Information	Description and sample value	Your value
A name for the cluster	The cluster name must begin with a letter of the alphabet. The cluster name can contain only the characters "a" through "z", "A" through "Z", the numbers "0" through "9", the hyphen "-", and the underscore "_". Example: **vcs_cluster27**	
A unique ID number for the cluster	A number in the range of 0-65535. Within the site that contains the cluster, each cluster must have a unique ID. Example: **7**	

Table 5-4 lists the information you need to configure VCS private heartbeat links.

Table 5-4 Information you need to configure VCS private heartbeat links

Information	Description and sample value	Your value
Decide how you want to configure LLT	You can configure LLT over Ethernet or LLT over UDP. Symantec recommends that you configure heartbeat links that use LLT over Ethernet, unless hardware requirements force you to use LLT over UDP. If you want to configure LLT over UDP, make sure you meet the prerequisites. See "Using the UDP layer for LLT" on page 415.	
Decide which configuration mode you want to choose	Installer provides you with three options: ■ 1. Configure heartbeat links using LLT over Ethernet ■ 2. Configure heartbeat links using LLT over UDP ■ 3. Automatically detect configuration for LLT over Ethernet You must manually enter details for options 1 and 2, whereas the installer detects the details for option 3.	
For option 1: LLT over Ethernet	■ The device names of the NICs that the private networks use among systems A network interface card or an aggregated interface. Do not use the network interface card that is used for the public network, which is typically lan0. Example: **lan1**, **lan2** ■ Choose whether to use the same NICs on all systems. If you want to use different NICs, enter the details for each system.	
For option 2: LLT over UDP	For each system, you must have the following details: ■ The device names of the NICs that the private networks use among systems ■ IP address for each NIC ■ UDP port details for each NIC	

Table 5-5 lists the information you need to configure virtual IP address of the cluster (optional).

Table 5-5 Information you need to configure virtual IP address

Information	Description and sample value	Your value
The name of the public NIC for each node in the cluster	The device name for the NIC that provides public network access. A network interface card or an aggregated interface. Example: lan0	

Table 5-5 Information you need to configure virtual IP address *(continued)*

Information	Description and sample value	Your value
A virtual IP address of the NIC	You can enter either an IPv4 or an IPv6 address. This virtual IP address becomes a resource for use by the ClusterService group. The "Cluster Virtual IP address" can fail over to another cluster system. Example IPv4 address: 192.168.1.16 Example IPv6 address: 2001:454e:205a:110:203:baff:feee:10	
The netmask for the virtual IPv4 address	The subnet that you use with the virtual IPv4 address. Example: 255.255.240.0	
The prefix for the virtual IPv6 address	The prefix length for the virtual IPv6 address. Example: 64	
The NetworkHosts IP addresses	IP addresses that are used to check the adapter connections. Example: 192.168.1.17	

Table 5-6 lists the information you need to configure VCS clusters in secure mode (optional).

Table 5-6 Information you need to configure VCS clusters in secure mode (optional)

Information	Description and sample value	Your value
To decide the root broker system you want to use	You can use an external system or one of the nodes in the cluster to serve as root broker.	
To decide which configuration mode you want to choose	Configuration modes are automatic, semiautomatic, and manual. The automatic mode is the simplest to configure, whereas the other two modes require knowledge of the Symantec Product Authentication Service. If you want one of the nodes in the cluster to serve as root broker, you must choose automatic configuration mode. See "Preparing to configure the clusters in secure mode" on page 89.	

Table 5-6 Information you need to configure VCS clusters in secure mode (optional) *(continued)*

Information	Description and sample value	Your value
For automatic mode (default)	If you use an external root broker system: ■ The name of the root broker system Example: `east` See "About Symantec Product Authentication Service (AT)" on page 26. ■ Access to the root broker system without use of a password. If you use one of the nodes in the cluster as root broker system: ■ Decide which node in the cluster you want the installer to configure as root and authentication broker. ■ The installer configures all other nodes in the cluster as authentication brokers.	
For semiautomatic mode using encrypted files	The path for the encrypted files that you get from the root broker administrator. See "Creating encrypted files for the security infrastructure" on page 95.	
For manual mode without using encrypted files	■ The fully-qualified hostname (FQHN) of the root broker . (e.g. east.symantecexample.com) The given example puts a system in the (DNS) domain symantecexample.com with the unqualified hostname east, which is designated as the root broker. ■ The root broker's security domain (e.g. **root@east.symantecexample.com**) ■ The root broker's port (e.g. **2821**) ■ The path to the local root hash (e.g. **/var/tmp/privatedir/root_hash**) ■ The authentication broker's identity and password on each cluster node (e.g. **galaxy.symantecexample.com** and **nebula.symantecexample.com**)	

Table 5-7 lists the information you need to add VCS users.

Table 5-7 Information you need to add VCS users

Information	Description and sample value	Your value
User names	VCS usernames are restricted to 1024 characters. Example: **smith**	

Table 5-7 Information you need to add VCS users *(continued)*

Information	Description and sample value	Your value
User passwords	VCS passwords are restricted to 255 characters. Enter the password at the prompt.	
To decide user privileges	Users have three levels of privileges: A=Administrator, O=Operator, or G=Guest. Example: **A**	

Table 5-8 lists the information you need to configure SMTP email notification (optional).

Table 5-8 Information you need to configure SMTP email notification (optional)

Information	Description and sample value	Your value
The name of the public NIC for each node in the cluster	The device name for the NIC that provides public network access. A network interface card or an aggregated interface. Example: **lan0**	
The domain-based address of the SMTP server	The SMTP server sends notification emails about the events within the cluster. Example: **smtp.symantecexample.com**	
The email address of each SMTP recipient to be notified	Example: **john@symantecexample.com**	

Table 5-8 Information you need to configure SMTP email notification (optional) *(continued)*

Information	Description and sample value	Your value
To decide the minimum severity of events for SMTP email notification	Events have four levels of severity, and the severity levels are cumulative: ■ I=Information VCS sends notifications for important events that exhibit normal behavior. ■ W=Warning VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events. ■ E=Error VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events. ■ S=SevereError VCS sends notifications for a critical error that can lead to data loss or corruption. Notifications include both Severe Error, Error, Warning, and Information type of events. Example: **E**	

Table 5-9 lists the information you need to configure SNMP trap notification (optional).

Table 5-9 Information you need to configure SNMP trap notification (optional)

Information	Description and sample value	Your value
The name of the public NIC for each node in the cluster	The device name for the NIC that provides public network access. A network interface card or an aggregated interface. Example: **lan0**	
The port number for the SNMP trap daemon	The default port number is 162.	
The system name for each SNMP console	Example: **saturn**	

Table 5-9 Information you need to configure SNMP trap notification (optional) *(continued)*

Information	Description and sample value	Your value
To decide the minimum severity of events for SNMP trap notification	Events have four levels of severity, and the severity levels are cumulative: ■ I=Information VCS sends notifications for important events that exhibit normal behavior. ■ W=Warning VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events. ■ E=Error VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events. ■ S=SevereError VCS sends notifications for a critical error that can lead to data loss or corruption. Notifications include both Severe Error, Error, Warning, and Information type of events. Example: **E**	

Table 5-10 lists the information you need to configure global clusters (optional).

Table 5-10 Information you need to configure global clusters (optional)

Information	Description and sample value	Your value
The name of the public NIC	You can use the same NIC that you used to configure the virtual IP of the cluster. Otherwise, specify appropriate values for the NIC. A network interface card or an aggregated interface. Example: **lan0**	
The virtual IP address of the NIC	You can enter either an IPv4 or an IPv6 address. You can use the same virtual IP address that you configured earlier for the cluster. Otherwise, specify appropriate values for the virtual IP address. Example IPv4 address: **192.168.1.16** Example IPv6 address: **2001:454e:205a:110:203:baff:feee:10**	

Table 5-10 Information you need to configure global clusters (optional) *(continued)*

Information	Description and sample value	Your value
The netmask for the virtual IPv4 address	You can use the same netmask that you used to configure the virtual IP of the cluster. Otherwise, specify appropriate values for the netmask. Example: **255.255.240.0**	
The prefix for the virtual IPv6 address	The prefix length for the virtual IPv6 address. Example: **64**	
The NetworkHosts IP addresses	You can use the same NetworkHosts IP address that you used to configure the virtual IP of the cluster. Otherwise, specify appropriate values for the NetworkHosts IP address when you are prompted. Example: **192.168.1.15**	

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

See "About planning to configure I/O fencing" on page 98.

Section 3

Installation using the script-based installer

Chapter 6

Installing VCS

This chapter includes the following topics:

Installing VCS using the installer

Perform the following steps to install VCS.

To install VCS

1. Confirm that you are logged in as the superuser and you mounted the product disc.

   See "Mounting the product disc" on page 69.

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

   Veritas product installer

   Perform the following steps to start the product installer:

   1. Start the installer.

      ```
      # ./installer
      ```

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

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

   3. From the displayed list of products to install, choose: Veritas Cluster Server.

installvcs program Perform the following steps to start the product installer:

1 Navigate to the folder that contains the installvcs program.

```
# cd dvd_mount/cluster_server
```

where *dist* is rhel5, sles10, or sles11 and *arch* is x86_64.

2 Start the installvcs program.

```
# ./installvcs
```

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

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

```
Do you agree with the terms of the End User License Agreement
as specified in the cluster_server/EULA/<lang>/EULA_VCS_Ux_5.1SP1.pdf
file present on media? [y,n,q,?] y
```

4 Choose the VCS depots that you want to install.

See "Veritas Cluster Server installation depots" on page 365.

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

1	Installs only the minimal required VCS depots that provides basic functionality of the product.
2	Installs the recommended VCS depots that provides complete functionality of the product. This option does not install the optional VCS depots. Note that this option is the default.
3	Installs all the VCS depots. You must choose this option to configure any optional VCS feature.
4	Displays the VCS depots for each option.

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

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

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

For a single-node VCS installation, enter one name for the system.

See "Creating a single-node cluster using the installer program" on page 412.

The installer does the following for the systems:

- Checks that the local system that runs the installer can communicate with remote systems.
  If the installer finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
  If the default communication method ssh fails, the installer attempts to use remsh.
- Makes sure the systems use one of the supported operating systems.
- Makes sure that the systems have the required operating system patches.
  If the installer reports that any of the patches are not available, install the patches on the system before proceeding with the VCS installation.
- Checks for product licenses.
- Checks whether a previous version of VCS is installed.
  If a previous version of VCS is installed , the installer provides an option to upgrade to VCS 5.1SP1.
  See "About upgrading to VCS 5.1SP1" on page 251.
- Checks for the required file system space and makes sure that any processes that are running do not conflict with the installation.
  If requirements for installation are not met, the installer stops and indicates the actions that you must perform to proceed with the process.
- Checks whether any of the depots already exists on a system.
  If the current version of any depot exists, the installer removes the depot from the installation list for the system. If a previous version of any depot exists, the installer replaces the depot with the current version.

6 Review the list of depots that the installer would install on each node.

The installer installs the VCS depots on the systems galaxy and nebula.

7 Select the license type.

```
  1) Enter a valid license key
  2) Enable keyless licensing and complete system licensing later

How would you like to license the systems? [1-2,q] (2)
```

Based on what license type you want to use, enter one of the following:

1 You must have a valid license key. Enter the license key at the prompt:

```
Enter a VCS license key: [b,q,?]
XXXX-XXXX-XXXX-XXXX-XXXX
```

If you plan to configure global clusters, enter the corresponding license keys when the installer prompts for additional licenses.

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

2 The keyless license option enables you to install VCS without entering a key. However, to ensure compliance, keyless licensing requires that you manage the systems with a management server.

For more information, go to the following website:

http://go.symantec.com/sfhakeyless

Note that this option is the default.

The installer registers the license and completes the installation process.

8 To install the Global Cluster Option, enter y at the prompt.

9 To configure VCS, enter y at the prompt. You can also configure VCS later.

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

See "Overview of tasks to configure VCS using the script-based installer" on page 121.

10 Enter y at the prompt to send the installation information to Symantec.

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

The installer provides an option to collect data about the installation process each time you complete an installation, upgrade, configuration, or uninstall of the product. The installer transfers the contents of the install log files to an internal Symantec site. The information is used only to gather metrics about how you use the installer. No personal customer data is collected, and no information will be shared by any other parties. Information gathered may include the product and the version installed or upgraded, how many systems were installed, and the time spent in any section of the install process.

11 After the installation, note the location of the installation log files, the summary file, and the response file for future reference.

The files provide the useful information that can assist you with the configuration and can also assist future configurations.

summary file	Lists the depots that are installed on each system.
log file	Details the entire installation.
response file	Contains the installation information that can be used to perform unattended or automated installations on other systems. See "Installing VCS using response files" on page 181.

Chapter 7

Preparing to configure VCS

This chapter includes the following topics:

Preparing to configure the clusters in secure mode

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

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

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

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

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

  - To use an external root broker, identify an existing root broker system in your enterprise or install and configure root broker on a stable system.
    See "Installing the root broker for the security infrastructure" on page 93.
  - To use one of the cluster nodes as root broker, the installer does not require you to do any preparatory tasks.
    When you configure the cluster in secure mode using the script-based installer, choose the automatic mode and choose one of the nodes for the installer to configure as root broker.

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

- For external root broker, an authentication broker (AB) account for each node in the cluster is set up on the root broker system.
  See "Creating authentication broker accounts on root broker system" on page 94.
- The system clocks of the external root broker and authentication brokers must be in sync.

The script-based installer provides the following configuration modes:

Automatic mode	The external root broker system must allow remsh or ssh passwordless login to use this mode.
Semi-automatic mode	This mode requires encrypted files (BLOB files) from the AT administrator to configure a cluster in secure mode. The nodes in the cluster must allow remsh or ssh passwordless login. See "Setting up inter-system communication" on page 431.
Manual mode	This mode requires root_hash file and the root broker information from the AT administrator to configure a cluster in secure mode. The nodes in the cluster must allow remsh or ssh passwordless login. See "Setting up inter-system communication" on page 431.

Figure 7-1 depicts the flow of configuring VCS cluster in secure mode.

Figure 7-1 Workflow to configure VCS cluster in secure mode

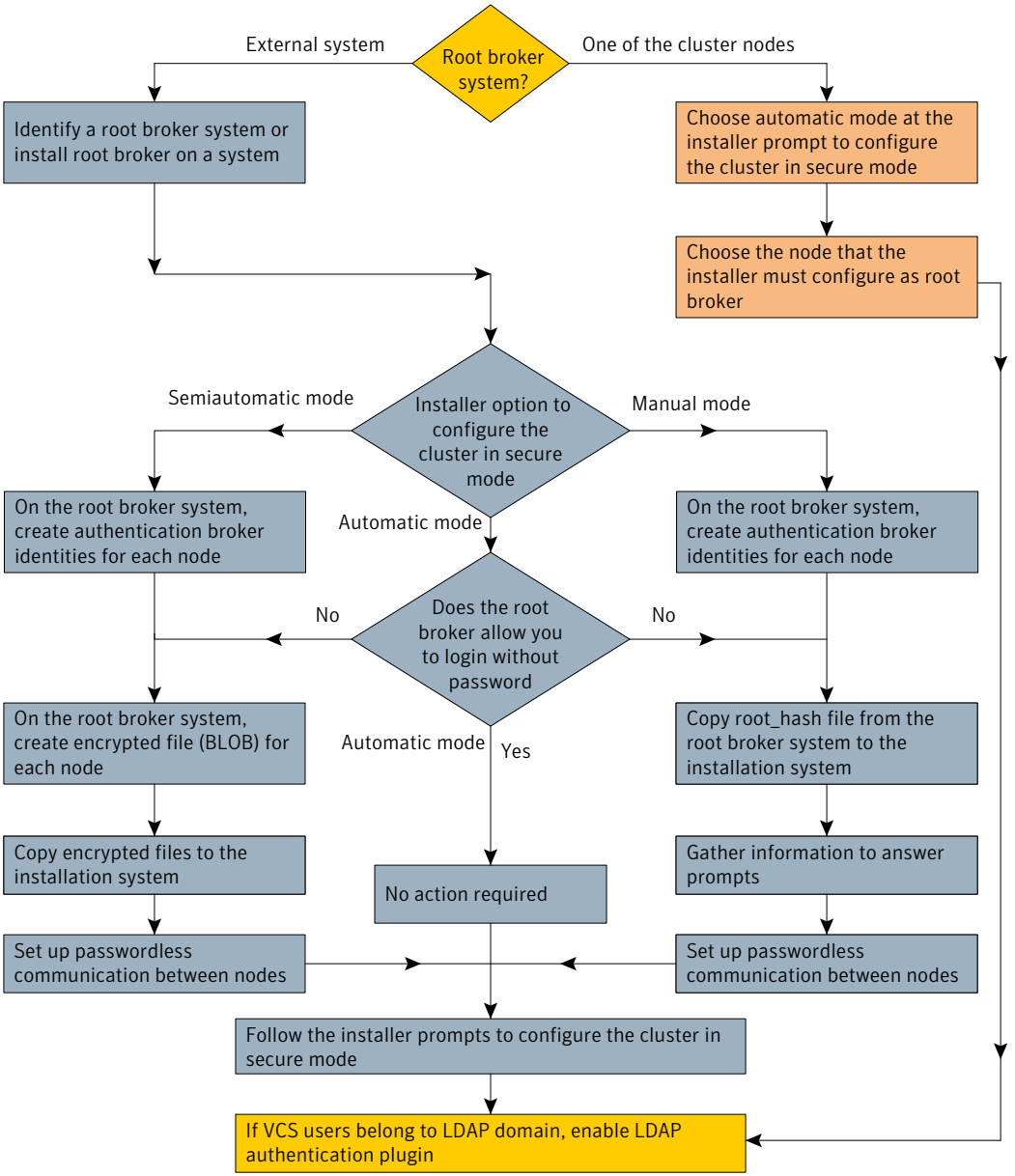


Table 7-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform. These preparatory tasks apply only when you use an external root broker system for the cluster.

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

Tasks	Who performs this task
Decide one of the following configuration modes to set up a cluster in secure mode: ■ Automatic mode ■ Semi-automatic mode ■ Manual mode	VCS administrator
Install the root broker on a stable system in the enterprise. See "Installing the root broker for the security infrastructure" on page 93.	AT administrator
To use the semi-automatic mode or the manual mode, on the root broker system, create authentication broker accounts for each node in the cluster. See "Creating authentication broker accounts on root broker system" on page 94. The AT administrator requires the following information from the VCS administrator: ■ Node names that are designated to serve as authentication brokers ■ Password for each authentication broker	AT administrator
To use the semi-automatic mode, create the encrypted files (BLOB files) for each node and provide the files to the VCS administrator. See "Creating encrypted files for the security infrastructure" on page 95. The AT administrator requires the following additional information from the VCS administrator: ■ Administrator password for each authentication broker Typically, the password is the same for all nodes.	AT administrator
To use the manual mode, provide the root_hash file (/opt/VRTSat/bin/root_hash) from the root broker system to the VCS administrator.	AT administrator
Copy the files that are required to configure a cluster in secure mode to the system from where you plan to install and configure VCS. See "Preparing the installation system for the security infrastructure" on page 97.	VCS administrator

Installing the root broker for the security infrastructure

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

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

See Symantec Product Authentication Service documentation for more information.

See "About Symantec Product Authentication Service (AT)" on page 26.

To install the root broker

1. Mount the product disc and start the installer.

   ```
   # ./installer
   ```

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

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

7. Review the output as the installer does the following:
   - Checks to make sure that AT supports the operating system
   - Checks if the depots are already on the system.

   The installer lists the depots that the program is about to install on the system. Press Enter to continue.
8. Review the output as the installer installs the root broker on the system.
9. After the installation, configure the root broker.

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

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

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

All AT processes that are currently running must be stopped

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

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

Creating authentication broker accounts on root broker system

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

To create authentication broker accounts on root broker system

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

```
venus> # vssat showalltrustedcreds
```

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

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

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

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

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

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

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

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

  Proceed to step 3.

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

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

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

Creating encrypted files for the security infrastructure

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

To create encrypted files

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

hash	The value of the root hash string, which consists of 40 characters. Execute the following command to find this value: `venus> # vssat showbrokerhash`
root_domain	The value for the domain name of the root broker system. Execute the following command to find this value: `venus> # vssat showalltrustedcreds`

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

identity	The value for the authentication broker identity, which you provided to create authentication broker principal on the root broker system. This is the value for the **--prplname** option of the `addprpl` command. See "Creating authentication broker accounts on root broker system" on page 94.
password	The value for the authentication broker password, which you provided to create authentication broker principal on the root broker system. This is the value for the **--password** option of the `addprpl` command. See "Creating authentication broker accounts on root broker system" on page 94.

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

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

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

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

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

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

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

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

For example:

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

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

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

Preparing the installation system for the security infrastructure

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

To prepare the installation system for the security infrastructure

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

Automatic mode	Do the following: ■ Gather the root broker system name from the AT administrator. ■ During VCS configuration, choose the configuration option 1 when the installvcs program prompts.
Semi-automatic mode	Do the following: ■ Copy the encrypted files (BLOB files) to the system from where you plan to install VCS. Note the path of these files that you copied to the installation system. ■ During VCS configuration, choose the configuration option 2 when the installvcs program prompts.

Manual mode	Do the following: ■ Copy the root_hash file that you fetched to the system from where you plan to install VCS. Note the path of the root hash file that you copied to the installation system. ■ Gather the root broker information such as name, fully qualified domain name, domain, and port from the AT administrator. ■ Note the principal name and password information for each authentication broker that you provided to the AT administrator to create the authentication broker accounts. ■ During VCS configuration, choose the configuration option 3 when the installvcs program prompts.

About planning to configure I/O fencing

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

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

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

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

If you have installed VCS in a virtual environment that is not SCSI-3 PR compliant, you can configure non-SCSI3 server-based fencing.

See Figure 7-3 on page 100.

Figure 7-2 illustrates a high-level flowchart to configure I/O fencing for the VCS cluster.

Figure 7-2 Workflow to configure I/O fencing

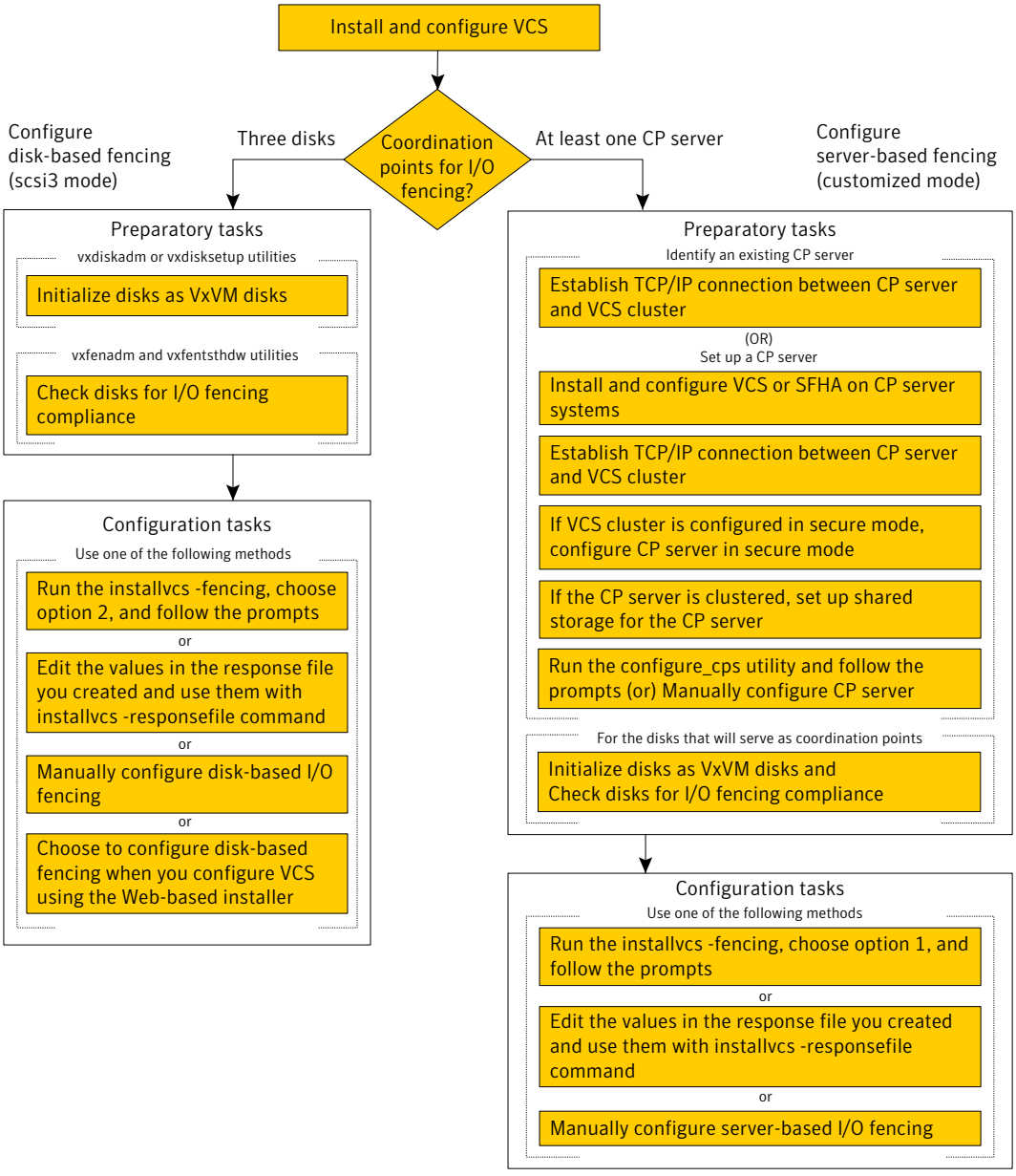
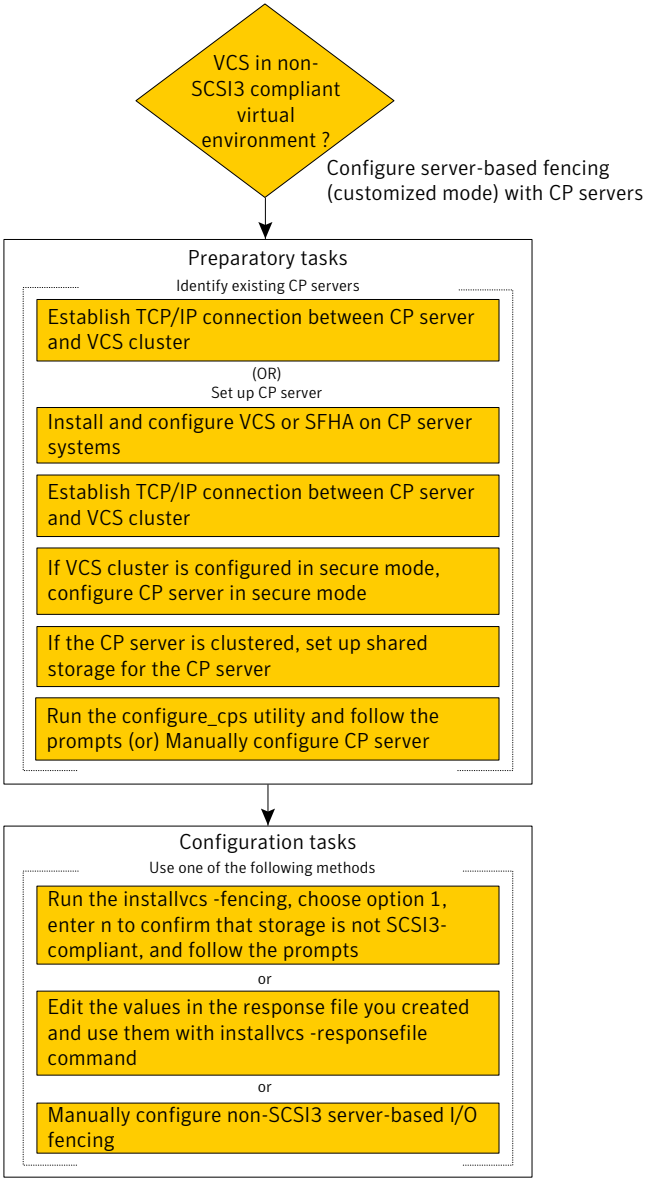


Figure 7-3 illustrates a high-level flowchart to configure non-SCSI3 server-based I/O fencing for the VCS cluster in virtual environments that do not support SCSI-3 PR.

Figure 7-3 Workflow to configure non-SCSI3 server-based I/O fencing



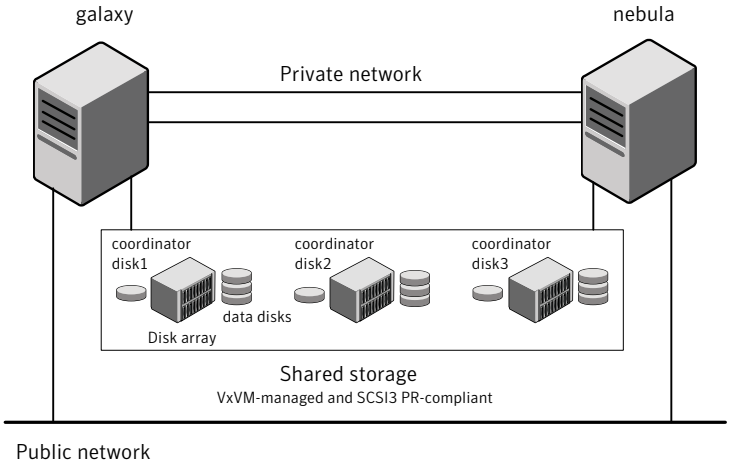
After you perform the preparatory tasks, you can use any of the following methods to configure I/O fencing:

Using the installvcs program	See "Setting up disk-based I/O fencing using installvcs program" on page 143. See "Setting up server-based I/O fencing using installvcs program" on page 150. See "Setting up non-SCSI3 server-based I/O fencing using installvcs program" on page 162.
Using the Web-based installer **Note:** The Web-based installer supports only the disk-based fencing configuration.	See "Configuring VCS using the Web-based installer" on page 173.
Using response files	See "Response file variables to configure disk-based I/O fencing" on page 200. See "Response file variables to configure server-based I/O fencing" on page 202. See "Response file variables to configure server-based I/O fencing" on page 202. See "Configuring I/O fencing using response files" on page 199.
Manually editing configuration files	See "Setting up disk-based I/O fencing manually" on page 227. See "Setting up server-based I/O fencing manually" on page 232. See "Setting up non-SCSI3 fencing in virtual environments manually" on page 244.

Typical VCS cluster configuration with disk-based I/O fencing

Figure 7-4 displays a typical VCS configuration with two nodes and shared storage. The configuration uses three coordinator disks for I/O fencing.

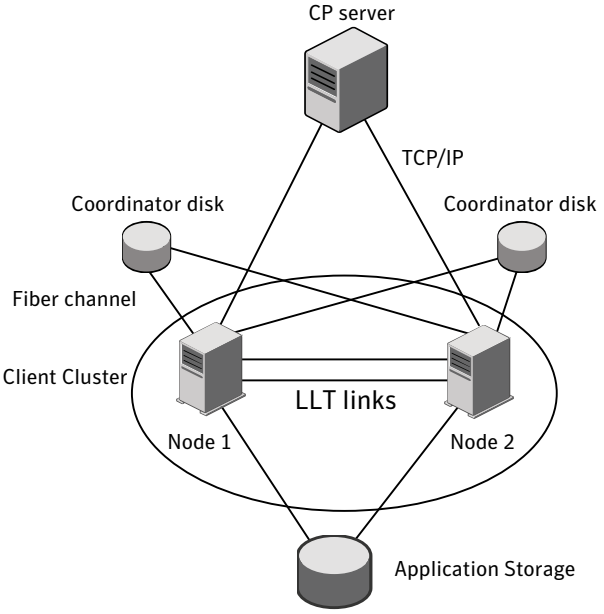
Figure 7-4 Typical VCS cluster configuration with disk-based I/O fencing



Typical VCS cluster configuration with server-based I/O fencing

Figure 7-5 displays a configuration using a VCS cluster (with two nodes), a single CP server, and two coordinator disks. The nodes within the VCS cluster are connected to and communicate with each other using LLT links.

Figure 7-5 CP server, VCS cluster, and coordinator disks



Recommended CP server configurations

Following are the recommended CP server configurations:

- Multiple application clusters use three CP servers as their coordination points.
  See Figure 7-6 on page 104.
- Multiple application clusters use a single CP server and multiple pairs of coordinator disks (two) as their coordination points.
  See Figure 7-7 on page 105.
- Multiple application clusters use a single CP server as their coordination point
  This single coordination point fencing configuration must use a highly available CP server that is configured on an SFHA cluster as its coordination point.
  See Figure 7-8 on page 105.

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

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

Figure 7-6 displays a configuration using three CP servers that are connected to multiple application clusters.

Figure 7-6 Three CP servers connecting to multiple application clusters

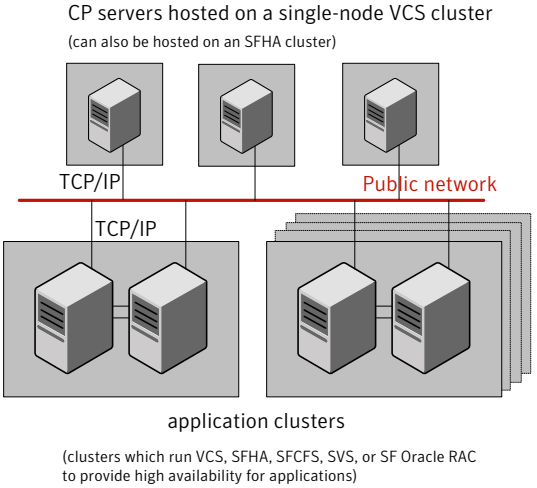


Figure 7-7 displays a configuration using a single CP server that is connected to multiple application clusters with each application cluster also using two coordinator disks.

Figure 7-7 Single CP server with two coordinator disks for each application cluster

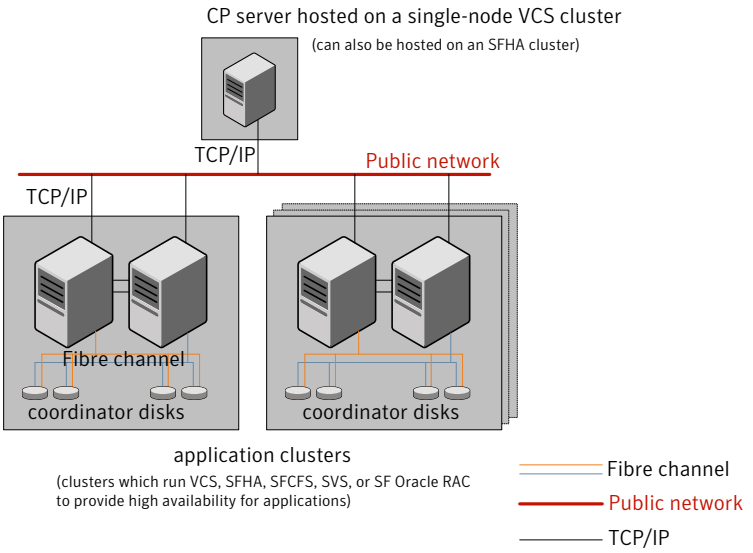
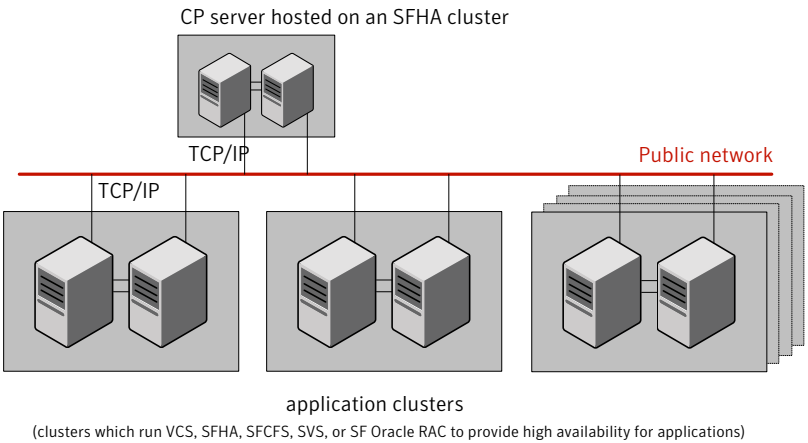


Figure 7-8 displays a configuration using a single CP server that is connected to multiple application clusters.

Figure 7-8 Single CP server connecting to multiple application clusters



See "Configuration diagrams for setting up server-based I/O fencing" on page 443.

Setting up the CP server

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

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

Task	Reference
Plan your CP server setup	See "Planning your CP server setup" on page 106.
Install the CP server	See "Installing the CP server using the installer" on page 107.
Configure the CP server cluster in secure mode	See "Configuring the CP server cluster in secure mode" on page 108.
Set up shared storage for the CP server database	See "Setting up shared storage for the CP server database" on page 109.
Configure the CP server	See " Configuring the CP server using the configuration utility" on page 110. See "Configuring the CP server manually" on page 118.
Verify the CP server configuration	See "Verifying the CP server configuration" on page 120.

Planning your CP server setup

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

To plan your CP server setup

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

   Symantec recommends hosting the CP server on an SFHA cluster.

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

   - You must configure fencing in enabled mode during the SFHA configuration.
   - You must set up shared storage for the CP server database during your CP server setup.

- Decide whether you want to configure server-based fencing for the VCS cluster (application cluster) with a single CP server as coordination point or with at least three coordination points.
  Symantec recommends using at least three coordination points.

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

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

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

  See "CP server requirements" on page 37.

5 Have the following information handy for CP server configuration:

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

Installing the CP server using the installer

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

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

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

CP server setup uses a single system

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

Meet the following requirements for CP server:

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

Proceed to configure the CP server.

See " Configuring the CP server using the configuration utility" on page 110.

See "Configuring the CP server manually" on page 118.

CP server setup uses multiple systems

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

Meet the following requirements for CP server:

- During installation, make sure to select all depots for installation. The VRTScps depot is installed only if you select to install all depots.
- During configuration, set up the cluster in secure mode if you want secure communication between the CP server and the VCS cluster (application cluster).
  See "Preparing to configure the clusters in secure mode" on page 89.
- During configuration, configure disk-based fencing (scsi3 mode).

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

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

Configuring the CP server cluster in secure mode

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

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

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

To configure the CP server cluster in secure mode

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

  ```
  # installvcs -security
  ```

  See "Preparing to configure the clusters in secure mode" on page 89.

Setting up shared storage for the CP server database

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

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

To set up shared storage for the CP server database

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

   For example:

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

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

   For example:

   ```
   # vxdg import cps_dg
   ```

3 Create a mirrored volume over the disk group.

For example:

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

4 Create a file system over the volume.

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

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

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

Configuring the CP server using the configuration utility

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

Perform one of the following procedures:

For CP servers on single-node VCS cluster:	See "To configure the CP server on a single-node VCS cluster" on page 110.
For CP servers on an SFHA cluster:	See "To configure the CP server on an SFHA cluster" on page 114.

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

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

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

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

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

The configuration utility then runs the following preconfiguration checks:

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

4 Enter the name of the CP server.

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

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

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

You can also use IPv6 address.

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

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

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

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

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

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

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

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

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

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

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

9 Verify and confirm the CP server configuration information.

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

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

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

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

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

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

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

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

12 Enter networkhosts information for the NIC resource.

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

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

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

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

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

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

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

For example:

```
# hagrp -state CPSSG

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

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

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

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

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

See "Sample configuration files for CP server" on page 405.

To configure the CP server on an SFHA cluster

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

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

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

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

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

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

The configuration utility then runs the following preconfiguration checks:

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

5 Enter the name of the CP server.

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

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

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

You can also use IPv6 address.

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

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

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

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

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

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

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

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

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

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

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

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

10 Verify and confirm the CP server configuration information.

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

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

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

The following output is for one node:

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

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

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

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

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

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

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

14 Enter networkhosts information for the NIC resource.

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

15 Enter the netmask for the virtual IP address.

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

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

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

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

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

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

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

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

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

For example:

```
# hagrp -state CPSSG

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

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

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

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

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

See "Sample configuration files for CP server" on page 405.

Configuring the CP server manually

Perform the following steps to manually configure the CP server.

To manually configure the CP server

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

```
# hastop -local
```

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

See "Sample configuration files for CP server" on page 405.

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

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

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

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

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

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

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

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

5 Start VCS on all the cluster nodes.

```
# hastart
```

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

```
# hagrp -state CPSSG
```

Output similar to the following appears:

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

Verifying the CP server configuration

Perform the following steps to verify the CP server configuration.

To verify the CP server configuration

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

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

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

Chapter 8

Configuring VCS

This chapter includes the following topics:

Overview of tasks to configure VCS using the script-based installer

Table 8-1 lists the tasks that are involved in configuring VCS using the script-based installer.

Table 8-1 Tasks to configure VCS using the script-based installer

Task	Reference
Start the software configuration	See "Starting the software configuration" on page 122.
Specify the systems where you want to configure VCS	See "Specifying systems for configuration" on page 123.
Configure the basic cluster	See "Configuring the cluster name and ID" on page 124. See "Configuring private heartbeat links" on page 124.
Configure virtual IP address of the cluster (optional)	See "Configuring the virtual IP of the cluster" on page 127.
Configure the cluster in secure mode (optional)	See "Configuring the cluster in secure mode" on page 129.
Add VCS users (required if you did not configure the cluster in secure mode)	See "Adding VCS users" on page 133.
Configure SMTP email notification (optional)	See "Configuring SMTP email notification" on page 133.
Configure SNMP email notification (optional)	See "Configuring SNMP trap notification" on page 135.
Configure global clusters (optional) **Note:** You must have enabled Global Cluster Option when you installed VCS.	See "Configuring global clusters" on page 137.
Complete the software configuration	See "Completing the VCS configuration" on page 138.

Starting the software configuration

You can configure VCS using the Veritas product installer or the installvcs program.

Note: If you want to reconfigure VCS, before you start the installer you must stop all the resources that are under VCS control using the `hastop` command or the `hagrp -offline` command.

To configure VCS using the product installer

1. Confirm that you are logged in as the superuser and that you have mounted the product disc.
2. Start the installer.

   ```
   # ./installer
   ```

   The installer starts the product installation program with a copyright message and specifies the directory where the logs are created.
3. From the opening Selection Menu, choose: `C` for "Configure an Installed Product."
4. From the displayed list of products to configure, choose the corresponding number for:

   Veritas Cluster Server

   Storage Foundation and High Availability

   Storage Foundation for Cluster File System

To configure VCS using the installvcs program

1. Confirm that you are logged in as the superuser.
2. Start the installvcs program.

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

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

Specifying systems for configuration

The installer prompts for the system names on which you want to configure VCS. The installer performs an initial check on the systems that you specify.

To specify system names for configuration

1. Enter the names of the systems where you want to configure VCS.

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

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

   The installer does the following tasks:

- Checks that the local node running the installer can communicate with remote nodes
  If the installer finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
- Makes sure that the systems are running with the supported operating system
- Checks whether VCS is installed
- Exits if VCS 5.1SP1 is not installed

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

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

See "About planning to configure I/O fencing" on page 98.

Configuring the cluster name and ID

Enter the cluster information when the installer prompts you.

To configure the cluster

1 Review the configuration instructions that the installer presents.

2 Enter the unique cluster name and cluster ID.

```
Enter the unique cluster name: [q,?] clus1
Enter a unique Cluster ID number between 0-65535: [b,q,?] 7
```

Configuring private heartbeat links

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

See "Using the UDP layer for LLT" on page 415.

The following procedure helps you configure LLT over Ethernet.

To configure private heartbeat links

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

- Option 1: LLT over Ethernet (answer installer questions)
  Enter the heartbeat link details at the installer prompt to configure LLT over Ethernet.
  Skip to step 2.
- Option 2: LLT over UDP (answer installer questions)
  Make sure that each NIC you want to use as heartbeat link has an IP address configured. Enter the heartbeat link details at the installer prompt to configure LLT over UDP. If you had not already configured IP addresses to the NICs, the installer provides you an option to detect the IP address for a given NIC.
  Skip to step 3.
- Option 3: LLT over Ethernet (allow installer to detect)
  Allow the installer to automatically detect the heartbeat link details to configure LLT over Ethernet. The installer tries to detect all connected links between all systems.
  Skip to step 5.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 Verify and confirm the information that the installer summarizes.

Configuring the virtual IP of the cluster

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

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

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

To configure the virtual IP of the cluster

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

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

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

Do one of the following:

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

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

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

Do one of the following:

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

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

5 Enter the virtual IP address for the cluster.

You can enter either an IPv4 address or an IPv6 address.

For IPv4:

- Enter the virtual IP address.

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

- Confirm the default netmask or enter another one:

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

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

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

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

        NIC: lan0
        IP: 192.168.1.16
        Netmask: 255.255.240.0

        NetworkHosts: 192.168.1.17

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

For IPv6

- Enter the virtual IP address.

```
Enter the Virtual IP address for the Cluster:
[b,q,?] 2001:454e:205a:110:203:baff:feee:10
```

- Enter the prefix for the virtual IPv6 address you provided. For example:

```
Enter the Prefix for IP
2001:454e:205a:110:203:baff:feee:10: [b,q,?] 64
```

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

```
Enter the NetworkHosts IP addresses, separated
by spaces: [b,q,?] 2001:db8::1 2001:db8::2
```

- Verify and confirm the Cluster Virtual IP information.

```
Cluster Virtual IP verification:

      NIC: lan0
      IP: 2001:454e:205a:110:203:baff:feee:10
      Prefix: 64

      NetworkHosts: 2001:db8::1 2001:db8::2

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

Configuring the cluster in secure mode

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

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

See "Preparing to configure the clusters in secure mode" on page 89.

To configure the cluster in secure mode

1 Choose whether to configure VCS to use Symantec Product Authentication Service.

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

- If you want to configure the cluster in secure mode, make sure you meet the prerequisites and enter **y**.
- If you do not want to configure the cluster in secure mode, enter **n**.
  You must add VCS users when the configuration program prompts.
  See "Adding VCS users" on page 133.

2 Select one of the options to enable security.

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

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

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

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

Option 1. Automatic configuration

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

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

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

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

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

Option 2. Semiautomatic configuration

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

Option 3. Manual configuration

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

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

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

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

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

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

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

Adding VCS users

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

To add VCS users

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

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

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

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

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

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

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

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

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

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

Configuring SMTP email notification

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

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

To configure SMTP email notification

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

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

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

See "Configuring SNMP trap notification" on page 135.

3. Provide information to configure SMTP notification.

Provide the following information:

- Enter the NIC information.

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

- Enter the SMTP server's host name.

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

- Enter the email address of each recipient.

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

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

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

4. Add more SMTP recipients, if necessary.

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

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

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

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

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

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

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

5 Verify and confirm the SMTP notification information.

```
NIC: lan0

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

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

Configuring SNMP trap notification

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

Note that you can also configure the notification after installation.

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

To configure the SNMP trap notification

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

2 Specify whether you want to configure the SNMP notification.

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

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

See "Configuring global clusters" on page 137.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

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

- Enter the SNMP trap daemon port.

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

- Enter the SNMP console system name.

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

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

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

4 Add more SNMP consoles, if necessary.

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

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

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

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

5 Verify and confirm the SNMP notification information.

```
NIC: lan0

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

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

Configuring global clusters

If you had installed a valid HA/DR license, the installer provides you an option to configure this cluster as global cluster. If not, the installer proceeds to configure VCS based on the configuration details you provided. You can also run the gcoconfig utility in each cluster later to update the VCS configuration file for global cluster.

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

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

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

To configure the global cluster option

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

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

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

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

3 Provide information to configure this cluster as global cluster.

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

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

You can also enter an IPv6 address as a virtual IP address.

4 Verify and confirm the configuration of the global cluster. For example:

For IPv4:

```
Global Cluster Option configuration verification:

      NIC: lan0
      IP: 192.168.1.16
      Netmask: 255.255.240.0

      NetworkHosts: 192.168.1.17

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

For IPv6

```
Global Cluster Option configuration verification:

      NIC: lan0
      IP: 2001:454e:205a:110:203:baff:feee:10
      Prefix: 64

      NetworkHosts: 2001:db8::1 2001:db8::2

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

Completing the VCS configuration

After you enter the VCS configuration information, the installer prompts to stop the VCS processes to complete the configuration process. The installer continues to create configuration files and copies them to each system. The installer also configures a cluster UUID value for the cluster at the end of the configuration. After the installer successfully configures VCS, it restarts VCS and its related processes.

If you chose to configure the cluster in secure mode, the installer then does the following before it starts VCS in secure mode:

- Depending on the security mode you chose to set up Authentication Service, the installer does one of the following:
  - Creates the security principal
  - Executes the encrypted file to create security principal on each node in the cluster
- Creates the VxSS service group
- Creates the Authentication Server credentials on each node in the cluster
- Creates the Web credentials for VCS users
- Sets up trust with the root broker

To complete the VCS configuration

1 If prompted, press Enter at the following prompt.

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

2 Review the output as the installer stops various processes and performs the configuration. The installer then restarts VCS and its related processes.

3 Enter y at the prompt to send the installation information to Symantec.

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

4 After the installer configures VCS successfully, note the location of summary, log, and response files that installer creates.

The files provide the useful information that can assist you with the configuration and can also assist future configurations.

summary file	Describes the cluster and its configured resources.
log file	Details the entire configuration.
response file	Contains the configuration information that can be used to perform secure or unattended installations on other systems. See "Configuring VCS using response files" on page 187.

Verifying and updating licenses on the system

After you install VCS, you can verify the licensing information using the vxlicrep program. You can replace the demo licenses with a permanent license.

See "Checking licensing information on the system" on page 140.

See "Updating product licenses using vxlicinst" on page 140.

Checking licensing information on the system

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

To check licensing information

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

```
# vxlicrep
```

2 Review the following output to determine the following information:

- The license key
- The type of license
- The product for which it applies
- Its expiration date, if any. Demo keys have expiration dates. Permanent keys and site keys do not have expiration dates.

```
License Key                    = xxx-xxx-xxx-xxx-xxx
Product Name                   = Veritas Cluster Server
Serial Number                  = xxxxx
License Type                   = PERMANENT
OEM ID                         = xxxxx

Features :=
Platform                       = HP-UX
Version                        = 5.1
Tier                           = 0
Reserved                       = 0
Mode                           = VCS
```

Updating product licenses using vxlicinst

You can use the `vxlicinst` command to add the VCS license key on each node. If you have VCS already installed and configured and you use a demo license, you can replace the demo license.

See "Replacing a VCS demo license with a permanent license" on page 141.

To update product licenses

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

```
# vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

Replacing a VCS demo license with a permanent license

When a VCS demo key license expires, you can replace it with a permanent license using the `vxlicinst(1)` program.

To replace a demo key

1. Make sure you have permissions to log in as root on each of the nodes in the cluster.
2. Shut down VCS on all nodes in the cluster:

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

   This command does not shut down any running applications.

3. Enter the permanent license key using the following command on each node:

```
# vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

4. Make sure demo licenses are replaced on all cluster nodes before starting VCS.

```
# vxlicrep
```

5. Start VCS on each node:

```
# hastart
```

Chapter 9

Configuring VCS clusters for data integrity

This chapter includes the following topics:

Setting up disk-based I/O fencing using installvcs program

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

Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

To initialize disks as VxVM disks

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

```
# ioscan -nfC disk
# insf -e
```

Warning: The HP-UX man page for the `insf` command instructs you to run the command in single-user mode only. You can run `insf -e` in multiuser mode only when no other user accesses any of the device files. This command can change the mode, owner, or group of an existing special (device) file, or unlink and recreate a file. The special files that are currently open may be left in an indeterminate state.

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

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

  ```
  vxdisksetup -i device_name
  ```

  The example specifies the CDS format:

  ```
  # vxdisksetup -i c2t13d0
  ```

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

Configuring disk-based I/O fencing using installvcs program

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

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

1 Start the installvcs program with `-fencing` option.

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

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

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

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

The program checks that the local node running the script can communicate with remote nodes and checks whether VCS 5.1 SP1 is configured properly.

3 Review the I/O fencing configuration options that the program presents. Type **2** to configure disk-based I/O fencing.

```
Select the fencing mechanism to be configured in this
Application Cluster [1-3,b,q] 2
```

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

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

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

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

- To use an existing disk group, enter the number corresponding to the disk group at the prompt.
  The program verifies whether the disk group you chose has an odd number of disks and that the disk group has a minimum of three disks.
- To create a new disk group, perform the following steps:
  - Enter the number corresponding to the **Create a new disk group** option.
    The program lists the available disks that are in the CDS disk format in the cluster and asks you to choose an odd number of disks with at least three disks to be used as coordinator disks.

Symantec recommends that you use three disks as coordination points for disk-based I/O fencing.

- Enter the numbers corresponding to the disks that you want to use as coordinator disks.
- Enter the disk group name.

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

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

See "Checking shared disks for I/O fencing" on page 147.

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

The program also does the following:

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

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

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

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

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

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

See "Configuring Coordination Point agent to monitor coordination points" on page 241.

Checking shared disks for I/O fencing

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

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

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

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

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

- Verifying the Array Support Library (ASL)
  See "Verifying Array Support Library (ASL)" on page 147.
- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 148.
- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 149.

Verifying Array Support Library (ASL)

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

To verify Array Support Library (ASL)

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

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

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

```
# vxddladm listsupport all
```

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

```
# vxdisk scandisks
```

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

Verifying that the nodes have access to the same disk

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

To verify that the nodes have access to the same disk

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

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

```
vxfenadm -i diskpath
```

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

For example, an EMC disk is accessible by the /dev/vx/rdmp/c1t1d0 path on node A and the /dev/vx/rdmp/c2t1d0 path on node B.

From node A, enter:

```
vxfenadm -i /dev/vx/rdmp/c1t1d0

Vendor id : EMC
Product id : SYMMETRIX
```

```
Revision : 5567
Serial Number : 42031000a
```

The same serial number information should appear when you enter the equivalent command on node B using the /dev/vx/rdmp/c2t1d0 path.

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

```
# vxfenadm -i /dev/vx/rdmp/c3t1d0

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

Testing the disks using vxfentsthdw utility

This procedure uses the /dev/vx/rdmp/c1t1d0 disk in the steps.

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

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

```
The disk /dev/vx/rdmp/c1t1d0 is ready to be configured for I/O Fencing on
node galaxy
```

For more information on how to replace coordinator disks, refer to the *Veritas Cluster Server Administrator's Guide*.

To test the disks using vxfentsthdw utility

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

See "Setting up inter-system communication" on page 431.

2 From one node, start the utility.

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

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

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

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

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

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

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

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

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

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

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

ALL tests on the disk /dev/vx/rdmp/c1t1d0 have PASSED
The disk is now ready to be configured for I/O Fencing on node
galaxy
```

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

Setting up server-based I/O fencing using installvcs program

If VCS cluster is configured to run in secure mode, then verify that the configuration is correct before you configure CP server-based I/O fencing.

See "Verifying the security configuration on the VCS cluster to use CP server coordination point" on page 151.

See “Configuring server-based I/O fencing using the installvcs program” on page 153.

Verifying the security configuration on the VCS cluster to use CP server coordination point

After configuring security using the `installvcs -security` command, follow the procedure below on each VCS cluster node to confirm that security is correctly configured.

To verify the security configuration on VCS cluster to use CP server coordination point

1 Run the following command:

```
# /opt/VRTScps/bin/cpsat listpd -t local
```

The following is an example of the command output:

```
Domain(s) Found 1

**************************

Domain Name HA_SERVICES@galaxy.symantec.com

Expiry Interval 0

**************************
```

2 There should be a domain name entry with the following format in the command output:

HA_SERVICES@*hostname.domainname*

or

HA_SERVICES@*hostname*

3 There should not be duplicate entries for HA_SERVICES domain.

The following is an example of an incorrect configuration:

```
showdomains

Domain(s) Found :       3

**************************************

Domain Name:    HA_SERVICES@galaxy.symantec.com

Domain Type:    vx

**************************************

Domain Name:    broker@galaxy.symantec.com

Domain Type:    vx

**************************************

Domain Name:    HA_SERVICES@galaxy

Domain Type:    vx

**************************************
```

Proceed to reconfigure security in case duplicate entries appear as shown in the above example.

Configuring server-based I/O fencing using the installvcs program

You can configure server-based I/O fencing for the VCS cluster using the installvcs program.

With server-based fencing, you can have the coordination points in your configuration as follows:

- Combination of CP servers and SCSI-3 compliant coordinator disks
- CP servers only
  Symantec also supports server-based fencing with a single highly available CP server that acts as a single coordination point.

See "About planning to configure I/O fencing" on page 98.

See "Recommended CP server configurations" on page 103.

This section covers the following example procedures:

Mix of CP servers and coordinator disks	See "To configure server-based fencing for the VCS cluster (one CP server and two coordinator disks)" on page 154.
Single CP server	See "To configure server-based fencing for the VCS cluster (single CP server)" on page 159.

To configure server-based fencing for the VCS cluster (one CP server and two coordinator disks)

1. Depending on the server-based configuration model in your setup, make sure of the following:
   - CP servers are configured and are reachable from the VCS cluster. The VCS cluster is also referred to as the application cluster or the client cluster.
     See "Setting up the CP server" on page 106.
   - The coordination disks are verified for SCSI3-PR compliance.
     See "Checking shared disks for I/O fencing" on page 147.
2. Start the installvcs program with `-fencing` option.

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

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

   Note the location of log files which you can access in the event of any problem with the configuration process.
3. Confirm that you want to proceed with the I/O fencing configuration at the prompt.

   The program checks that the local node running the script can communicate with remote nodes and checks whether VCS 5.1 SP1 is configured properly.
4. Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

   ```
   Select the fencing mechanism to be configured in this
   Application Cluster [1-3,b,q] 1
   ```
5. Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

   ```
   Does your storage environment support SCSI3 PR? [y,n,q] (y)
   ```

6 Provide the following details about the coordination points at the installer prompt:

- Enter the total number of coordination points including both servers and disks. This number should be at least 3.

```
Enter the total number of co-ordination points including both
CP servers and disks: [b] (3)
```

- Enter the total number of coordinator disks among the coordination points.

```
Enter the total number of disks among these:
[b] (0) 2
```

7 Provide the following CP server details at the installer prompt:

- Enter the virtual IP addresses or host names of the virtual IP address for each of the CP servers. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address/fully qualified host name
for the Co-ordination Point Server #1:
[b] 10.209.80.197
```

- Enter the port that the CP server would be listening on.

```
Enter the port in the range [49152, 65535] which the
Co-ordination Point Server 10.209.80.197
would be listening on or simply accept the default port suggested:
[b] (14250)
```

8 Provide the following coordinator disks-related details at the installer prompt:

- Enter the I/O fencing disk policy for the coordinator disks.

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

- Choose the coordinator disks from the list of available disks that the installer displays. Ensure that the disk you choose is available from all the VCS (application cluster) nodes.
  The number of times that the installer asks you to choose the disks depends on the information that you provided in step 6. For example, if you had chosen to configure two coordinator disks, the installer asks you to choose the first disk and then the second disk:

```
Select disk number 1 for co-ordination point

1) c1t1d0
2) c2t1d0
3) c3t1d0

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

- If you have not already checked the disks for SCSI-3 PR compliance in step 1, check the disks now.
  The installer displays a message that recommends you to verify the disks in another window and then return to this configuration procedure.
  Press Enter to continue, and confirm your disk selection at the installer prompt.
- Enter a disk group name for the coordinator disks or accept the default.

```
Enter the disk group name for coordinating disk(s):
[b] (vxfencoorddg)
```

9 Verify and confirm the coordination points information for the fencing configuration.

For example:

```
Total number of coordination points being used: 3
CP Server (Port):
    1. 10.209.80.197 (14250)
SCSI-3 disks:
    1. c1t1d0
    2. c2t1d0
Disk Group name for the disks in customized fencing: vxfencoorddg
Disk mechanism used for customized fencing: raw
```

The installer initializes the disks and the disk group and deports the disk group on the VCS (application cluster) node.

10 If the CP server is configured for security, the installer sets up secure communication between the CP server and the VCS (application cluster):

- Make sure that the security configuration in the application cluster and the CP server is the same. If CP server is configured for security, ensure that the application cluster also runs in secure mode.
- If the CP server is configured for security, perform the following steps:

- Review the output as the installer verifies if the VCS (application cluster) nodes have already established trust with an AT root broker.
- If the VCS (application cluster) nodes and the CP server use different AT root brokers, enter y at the installer prompt and provide the following information:
  - Hostname for the authentication broker for any one of the CP servers
  - Port number where the authentication broker for the CP server is listening for establishing trust
  - Hostname for the authentication broker for any one of the VCS (application cluster) nodes
  - Port number where the authentication broker for the VCS (application cluster) is listening for establishing trust

  After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

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

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

12 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

```
Updating client cluster information on CP Server 10.210.80.199

Adding the client cluster to the CP Server 10.210.80.199 .................. Done

Registering client node galaxy with CP Server 10.210.80.199.............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Registering client node nebula with CP Server 10.210.80.199 ............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Updating /etc/vxfenmode file on galaxy ................................. Done
Updating /etc/vxfenmode file on nebula ......... ........................ Done
```

See "About I/O fencing configuration files" on page 403.

13 Configure the CP agent on the VCS (application cluster).

```
Do you want to configure CP Agent on the client cluster? [y,n,q]
(y)

Enter a non-existing name for the service group for CP Agent:
[b] (vxfen)

Adding CP Agent via galaxy ........................ Done
```

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

15 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

To configure server-based fencing for the VCS cluster (single CP server)

1. Make sure that the CP server is configured and is reachable from the VCS cluster. The VCS cluster is also referred to as the application cluster or the client cluster.

   See "Setting up the CP server" on page 106.

2. Start the installvcs program with `-fencing` option.

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

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

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

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

   The program checks that the local node running the script can communicate with remote nodes and checks whether VCS 5.1 SP1 is configured properly.

4. Review the I/O fencing configuration options that the program presents. Type **1** to configure server-based I/O fencing.

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

5. Make sure that the storage supports SCSI3-PR, and answer y at the following prompt.

   ```
   Does your storage environment support SCSI3 PR? [y,n,q] (y)
   ```

6. Enter the total number of coordination points as **1**.

   ```
   Enter the total number of co-ordination points including both
   CP servers and disks: [b] (3) 1
   ```

   Read the installer warning carefully before you proceed with the configuration.

7. Provide the following CP server details at the installer prompt:

   - Enter the virtual IP address or the host name of the virtual IP address for the CP server. The installer assumes these values to be identical as viewed from all the application cluster nodes.

```
Enter the Virtual IP address/fully qualified host name
for the Co-ordination Point Server #1:
[b] 10.209.80.197
```

- Enter the port that the CP server would be listening on.

```
Enter the port in the range [49152, 65535] which the
Co-ordination Point Server 10.209.80.197
would be listening on or simply accept the default port suggested:
[b] (14250)
```

8 Verify and confirm the coordination points information for the fencing configuration.

For example:

```
Total number of coordination points being used: 1
CP Server (Port):
    1. 10.209.80.197 (14250)
```

9 If the CP server is configured for security, the installer sets up secure communication between the CP server and the VCS (application cluster):

- Make sure that the security configuration in the application cluster and the CP server is the same. If CP server is configured for security, ensure that the application cluster also runs in secure mode.
- If the CP server is configured for security, perform the following steps:
  - Review the output as the installer verifies if the VCS (application cluster) nodes have already established trust with an AT root broker.
  - If the VCS (application cluster) nodes and the CP server use different AT root brokers, enter y at the installer prompt and provide the following information:
    - Hostname for the authentication broker for any one of the CP servers
    - Port number where the authentication broker for the CP server is listening for establishing trust
    - Hostname for the authentication broker for any one of the VCS (application cluster) nodes
    - Port number where the authentication broker for the VCS (application cluster) is listening for establishing trust

After the installer establishes trust between the authentication brokers of the CP servers and the application cluster nodes, press Enter to continue.

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

```
CPS Admin utility location: /opt/VRTScps/bin/cpsadm
Cluster ID: 2122
Cluster Name: clus1
UUID for the above cluster: {ae5e589a-1dd1-11b2-dd44-00144f79240c}
```

11 Review the output as the installer updates the application cluster information on each of the CP servers to ensure connectivity between them. The installer then populates the `/etc/vxfenmode` file with the appropriate details in each of the application cluster nodes.

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

```
Updating client cluster information on CP Server 10.210.80.199

Adding the client cluster to the CP Server 10.210.80.199 .................. Done

Registering client node galaxy with CP Server 10.210.80.199.............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Registering client node nebula with CP Server 10.210.80.199 ............. Done
Adding CPClient user for communicating to CP Server 10.210.80.199 ......... Done
Adding cluster clus1 to the CPClient user on CP Server 10.210.80.199 ... Done

Updating /etc/vxfenmode file on galaxy ................................. Done
Updating /etc/vxfenmode file on nebula ......... ....................... Done
```

See "About I/O fencing configuration files" on page 403.

12 Configure the CP agent on the VCS (application cluster).

```
Do you want to configure CP Agent on the client cluster? [y,n,q]
(y)

Enter a non-existing name for the service group for CP Agent:
[b] (vxfen)

Adding CP Agent via galaxy ....................... Done
```

13 Review the output as the installer stops and restarts VCS with the fencing processes on each application cluster node, and completes the I/O fencing configuration.

14 Note the location of the configuration log files, summary files, and response files that the installer displays for later use.

Setting up non-SCSI3 server-based I/O fencing using installvcs program

If VCS cluster is configured to run in secure mode, then verify that the configuration is correct before you configure non-SCSI3 server-based I/O fencing.

See "Verifying the security configuration on the VCS cluster to use CP server coordination point" on page 151.

Enabling or disabling the preferred fencing policy

You can enable or disable the preferred fencing feature for your I/O fencing configuration.

You can enable preferred fencing to use system-based race policy or group-based race policy. If you disable preferred fencing, the I/O fencing configuration uses the default count-based race policy.

See "About preferred fencing" on page 31.

To enable preferred fencing for the I/O fencing configuration

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

```
# vxfenadm -d
```

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

```
# haclus -value UseFence
```

3 To enable system-based race policy, perform the following steps:

- Make the VCS configuration writable.

  ```
  # haconf -makerw
  ```

- Set the value of the cluster-level attribute PreferredFencingPolicy as System.

```
# haclus -modify PreferredFencingPolicy System
```

- Set the value of the system-level attribute FencingWeight for each node in the cluster.
  For example, in a two-node cluster, where you want to assign galaxy five times more weight compared to nebula, run the following commands:

  ```
  # hasys -modify galaxy FencingWeight 50
  # hasys -modify nebula FencingWeight 10
  ```

- Save the VCS configuration.

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

4 To enable group-based race policy, perform the following steps:

- Make the VCS configuration writable.

  ```
  # haconf -makerw
  ```

- Set the value of the cluster-level attribute PreferredFencingPolicy as Group.

  ```
  # haclus -modify PreferredFencingPolicy Group
  ```

- Set the value of the group-level attribute Priority for each service group. For example, run the following command:

  ```
  # hagrp -modify service_group Priority 1
  ```

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

- Save the VCS configuration.

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

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

```
# vxfenconfig -a
```

To disable preferred fencing for the I/O fencing configuration

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

```
# vxfenadm -d
```

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

```
# haclus -value UseFence
```

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

```
# haconf -makerw
# haclus -modify PreferredFencingPolicy Disabled
# haconf -dump -makero
```

Section 4

Installation using the Web-based installer

Chapter 10

Installing VCS

This chapter includes the following topics:

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

Table 10-1 Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Veritas products.	Must be a supported platform for VCS 5.1SP1.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.

Table 10-1 Web-based installer requirements *(continued)*

System	Function	Requirements
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: ■ Internet Explorer 6, 7, and 8 ■ Firefox 3.x

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

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

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

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

2 On the administrative server, start the Web browser.

3 Navigate to the URL that the script displayed.

4 The browser may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

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

Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.

To obtain a security exception

1 Click **Or you can add an exception** link.

2 Click **Add Exception** button.

3 Click **Get Certificate** button.

4 Uncheck **Permanently Store this exception checkbox (recommended)**.

5 Click **Confirm Security Exception** button.

6 Enter root in User Name field and root password of the web server in the Password field.

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

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

To perform a pre-installation check

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 168.

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

3 Select the product from the **Product** drop-down list, and click **Next**.

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

5 The installer performs the precheck and displays the results.

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

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

Installing VCS with the Web-based installer

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

To install VCS using the Web-based installer

1 Perform preliminary steps. See "Performing a pre-installation check with the Veritas Web-based installer" on page 169.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 168.

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

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

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

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

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

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

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

10 After the installation completes, you must choose your licensing method.

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

- Keyless licensing

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

  For more information, go to the following website:

  http://go.symantec.com/sfhakeyless

  Complete the following information:

  - Choose whether you want to enable Global Cluster option.

  Click **Register**.

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

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

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

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

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

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

Click **Finish**.

Chapter 11

Configuring VCS

This chapter includes the following topics:

Configuring VCS using the Web-based installer

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

Note: If you want to reconfigure VCS, before you start the installer you must stop all the resources that are under VCS control using the `hastop` command or the `hagrp -offline` command.

See "Getting your VCS installation and configuration information ready" on page 71.

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

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

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

To configure VCS on a cluster

1 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 168.

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

Task	Configure a Product
Product	Veritas Cluster Server

Click **Next**.

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

Example: **galaxy nebula**

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

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

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

To configure disk-based I/O fencing, click **Yes**.

If you want to configure server-based I/O fencing, or if you decide to configure I/O fencing later, click **No**. You can either use the `installvcs -fencing` command or manually configure.

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

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

Click **Next**.

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

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

Click **Next**.

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

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

If you want to perform this task later, click **No**. You can use the `installvcs -security` command. Go to step 9.

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

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

Click **Next**.

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

Virtual IP	■ Select the **Configure Virtual IP** check box. ■ If each system uses a separate NIC, select the **Configure NICs for every system separately** check box. ■ Select the interface on which you want to configure the virtual IP. ■ Enter a virtual IP address and value for the netmask. Enter the value for the networkhosts. You can use an IPv4 or an IPv6 address.
VCS Users	■ Reset the password for the Admin user, if necessary. ■ Click **Add** to add a new user. Specify the user name, password, and user privileges for this user.

SMTP

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

SNMP

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

GCO

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

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

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

Click **Next**.

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

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

If you did not choose to configure I/O fencing in step 4, then skip to step 14. Go to step 12 to configure fencing.

12 On the Select Fencing Type page, specify the following information:

Configure disk based fencing	Choose the **Configure disk based fencing** option.
Select a Disk Group	Select the **Create a new disk group** option or select one of the disk groups from the list. ■ If you selected one of the disk groups that is listed, the default fencing mechanism for the disk group is dmp. Go to step 14. ■ If you selected the **Create a new disk group** option, make sure you have SCSI-3 PR enabled disks, and click **Yes** in the confirmation dialog box. Click **Next**. Go to step 13.

13 On the Create New DG page, specify the following information:

New Disk Group Name	Enter a name for the new coordinator disk group you want to create.
Select Disks	Select at least three disks to create the coordinator disk group. If you want to select more than three disks, make sure to select an odd number of disks.
Fencing Mechanism	The default fencing mechanism for the disk group is dmp.

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

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

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

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

Section 5

Installation using response files

Chapter 12

Performing automated VCS installation

This chapter includes the following topics:

Installing VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS installation on one cluster to install VCS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To install VCS using response files

1. Make sure the systems where you want to install VCS meet the installation requirements.

   See "Important preinstallation information for VCS" on page 33.

2. Make sure the preinstallation tasks are completed.

   See "Performing preinstallation tasks" on page 59.

3. Copy the response file to one of the cluster systems where you want to install VCS.

   See "Sample response file for installing VCS" on page 184.

4. Edit the values of the response file variables as necessary.

   See "Response file variables to install VCS" on page 182.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installation from the system to which you copied the response file. For example:

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

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

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

Response file variables to install VCS

Table 12-1 lists the response file variables that you can define to install VCS.

Table 12-1 Response file variables specific to installing VCS

Variable	List or Scalar	Description
CFG{opt}{install}	Scalar	Installs VCS depots. (Required)
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 installed. Required
CFG{prod}	Scalar	Defines the product to be installed. The value is VCS51 for VCS. (Required)

Table 12-1 Response file variables specific to installing VCS *(continued)*

Variable	List or Scalar	Description
CFG{opt}{installallpkgs} or CFG{opt}{installrecpkgs} or CFG{opt}{installminpkgs}	Scalar	Instructs the installer to install VCS depots based on the variable that has the value set to 1: ■ installallpkgs: Installs all depots ■ installrecpkgs: Installs recommended depots ■ installminpkgs: Installs minimum depots **Note:** The installer requires only one of these variable values to be set to 1. (Required)
CFG{opt}{rsh}	Scalar	Defines that *remsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{gco}	Scalar	Defines that the installer must enable the global cluster option. You must set this variable value to 1 if you want to configure global clusters. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{patchpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. (Optional)

Table 12-1 Response file variables specific to installing VCS *(continued)*

Variable	List or Scalar	Description
CFG{opt}{pkgpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)
CFG{opt}{vxkeyless}	Scalar	Installs the product with keyless license if the value is set to 1. If the value is set to 0, you must define the CFG{keys}{system} variable with the license keys. (Optional)
CFG{keys} {system}	Scalar	List of keys to be registered on the system if the variable $CFG{opt}{vxkeyless} is set to 0. (Optional)

Sample response file for installing VCS

Review the response file variables and their definitions.

See "Response file variables to install VCS" on page 182.

```
#
# Configuration Values:
#
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{prod}="VCS51";
$CFG{systems}=[ qw(galaxy nebula) ];
1;
```

Chapter 13

Performing automated VCS configuration

This chapter includes the following topics:

Configuring VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS configuration on one cluster to configure VCS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To configure VCS using response files

1. Make sure the VCS depots are installed on the systems where you want to configure VCS.
2. Copy the response file to one of the cluster systems where you want to configure VCS.

   See "Sample response file for configuring VCS" on page 197.

3 Edit the values of the response file variables as necessary.

To configure optional features, you must define appropriate values for all the response file variables that are related to the optional feature.

See "Response file variables to configure VCS" on page 188.

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

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

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

Response file variables to configure VCS

Table 13-1 lists the response file variables that you can define to configure VCS.

Table 13-1 Response file variables specific to configuring VCS

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the depots are already installed. (Required)
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 VCS51 for VCS. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)

Table 13-1 Response file variables specific to configuring VCS *(continued)*

Variable	List or Scalar	Description
CFG{opt}{rsh}	Scalar	Defines that *remsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is `/opt/VRTS/install/logs`. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)
$CFG{uploadlogs}	Scalar	Defines Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (the csgnic, csgvip, and csgnetmask variables) must be defined if any are defined. The same is true for the SMTP notification (the smtpserver, smtprecp, and smtprsev variables), the SNMP trap notification (the snmpport, snmpcons, and snmpcsev variables), and the Global Cluster Option (the gconic, gcovip, and gconetmask variables).

Table 13-2 lists the response file variables that specify the required information to configure a basic VCS cluster.

Table 13-2 Response file variables specific to configuring a basic VCS cluster

Variable	List or Scalar	Description
CFG{vcs_clusterid}	Scalar	An integer between 0 and 65535 that uniquely identifies the cluster. (Required)
CFG{vcs_clustername}	Scalar	Defines the name of the cluster. (Required)
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)
$CFG{fencingenabled}	Scalar	In a VCS configuration, defines if fencing is enabled. Valid values are 0 or 1. (Required)

Table 13-3 lists the response file variables that specify the required information to configure LLT over Ethernet.

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

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 13-3 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 13-4 lists the response file variables that specify the required information to configure LLT over UDP.

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

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 13-4 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)
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 13-5 lists the response file variables that specify the required information to configure virtual IP for VCS cluster.

Table 13-5 Response file variables specific to configuring virtual IP for VCS cluster

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 13-6 lists the response file variables that specify the required information to configure the VCS cluster in secure mode.

Table 13-6 Response file variables specific to configuring VCS cluster in secure mode

Variable	List or Scalar	Description
CFG{at_rootdomain}	Scalar	Defines the name of the system where the root broker is installed. (Optional)
CFG{at_rootbroker}	Scalar	Defines the root broker's name.
CFG{vcs_securitymenuopt}	Scalar	Specifies the menu option to choose to configure the cluster in secure mode. ■ 1—Automatic ■ 2—Semi-automatic ■ 3—Manual (Optional)

Table 13-6 Response file variables specific to configuring VCS cluster in secure mode *(continued)*

Variable	List or Scalar	Description
CFG{vcs_vssdefport}	Scalar	Specifies the default port address of the root broker. (Optional)
CFG{vcs_roothashpath}	Scalar	Specifies the path of the root hash file. (Optional)
CFG{vcs_ab_prplname} {system}	Scalar	Specifies the authentication broker's principal name on system. (Optional)
CFG{vcs_ab_password} {system}	Scalar	Specifies the authentication broker's password on system. (Optional)
CFG{vcs_blobpath} {system}	Scalar	Specifies the path of the encrypted BLOB file for system. (Optional)

Table 13-7 lists the response file variables that specify the required information to configure VCS users.

Table 13-7 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 13-7 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 13-8 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

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

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, and SevereError) that listed SMTP recipients are to receive. Note that the ordering of severity levels must match that of the addresses of SMTP recipients. (Optional)

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

Table 13-9 Response file variables specific to configuring VCS notifications using SNMP

Variable	List or Scalar	Description
CFG{vcs_snmpport}	Scalar	Defines the SNMP trap daemon port (default=162). (Optional)
CFG{vcs_snmpcons}	List	List of SNMP console system names. (Optional)
CFG{vcs_snmpcsev}	List	Defines the minimum severity level of messages (Information, Warning, Error, and SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names. (Optional)

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

Table 13-10 Response file variables specific to configuring VCS global clusters

Variable	List or Scalar	Description
CFG{vcs_gconic} {system}	Scalar	Defines the NIC for the Virtual IP that the Global Cluster Option uses. You can enter 'all' as a system value if the same NIC is used on all systems. (Optional)
CFG{vcs_gcovip}	Scalar	Defines the virtual IP address to that the Global Cluster Option uses. (Optional)
CFG{vcs_gconetmask}	Scalar	Defines the Netmask of the virtual IP address that the Global Cluster Option uses. (Optional)

Sample response file for configuring VCS

Review the response file variables and their definitions.

See "Response file variables to configure VCS" on page 188.

```
#
# Configuration Values:
#
our %CFG;

$CFG{at_rootdomain}="root\@east.symantecexample.com";
$CFG{rootbroker}="east.symantecexample.com";
$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{opt}{ha}=1;
$CFG{prod}="VCS51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_allowcomms}=1;
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="clus1";
$CFG{vcs_csgnetmask}="255.255.255.0";
$CFG{vcs_csgnic}{all}="lan0";
$CFG{vcs_csgvip}="10.10.12.1";
$CFG{vcs_gconetmask}="255.255.255.0";
$CFG{vcs_gcovip}="10.10.12.1";
$CFG{vcs_lltlink1}{galaxy}="lan1";
$CFG{vcs_lltlink1}{nebula}="lan1";
$CFG{vcs_lltlink2}{galaxy}="lan2";
$CFG{vcs_lltlink2}{nebula}="lan2";

$CFG{vcs_networkhosts}="10.10.12.2

$CFG{vcs_securitymenuopt}=1;
$CFG{vcs_smtprecp}=[ qw(earnie@symantecexample.com) ];
$CFG{vcs_smtprsev}=[ qw(SevereError) ];
$CFG{vcs_smtpserver}="smtp.symantecexample.com";
$CFG{vcs_snmpcons}=[ qw(neptune) ];
$CFG{vcs_snmpcsev}=[ qw(SevereError) ];
$CFG{vcs_snmpport}=162;
1;
```

Chapter 14

Performing automated I/O fencing configuration for VCS

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 VCS.

To configure I/O fencing using response files

1. Make sure that VCS is configured.
2. Based on whether you want to configure disk-based or server-based I/O fencing, make sure you have completed the preparatory tasks.

   See "About planning to configure I/O fencing" on page 98.

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 201.

See "Sample response file for configuring server-based I/O fencing" on page 204.

4 Edit the values of the response file variables as necessary.

See "Response file variables to configure disk-based I/O fencing" on page 200.

See "Response file variables to configure server-based I/O fencing" on page 202.

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

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

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

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

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

Table 14-1 Response file variables specific to configuring disk-based I/O fencing

Variable	List or Scalar	Description
CFG{opt}{fencing}	Scalar	Performs the I/O fencing configuration. (Required)
CFG{vxfen_config_fencing_option}	Scalar	Specifies the I/O fencing configuration mode. ■ 1—Coordination Point Server-based I/O fencing ■ 2—Coordinator disk-based I/O fencing ■ 3—Disabled mode (Required)

Table 14-1 Response file variables specific to configuring disk-based I/O fencing *(continued)*

Variable	List or Scalar	Description
CFG {vxfen_config _fencing_mechanism}	Scalar	Specifies the I/O fencing mechanism. This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the vxfen_config _fencing_mechanism variable and either the vxfen_config_fencing_dg variable or the vxfen_config _fencing_newdg_disks variable. (Optional)
CFG{vxfen_config_fencing_dg}	Scalar	Specifies the disk group for I/O fencing. (Optional) **Note:** You must define the vxfen_config_fencing_dg variable to use an existing disk group. If you want to create a new disk group, you must use both the vxfen_config_fencing_dg variable and the vxfen_config_fencing_newdg_disks variable.
CFG{vxfen_config _fencing_newdg_disks}	List	Specifies the disks to use to create a new disk group for I/O fencing. (Optional) **Note:** You must define the vxfen_config_fencing_dg variable to use an existing disk group. If you want to create a new disk group, you must use both the vxfen_config_fencing_dg variable and the vxfen_config_fencing_newdg_disks variable.

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 200.

```
#
# Configuration Values:
#
our %CFG;

$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="VCS51";

$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_dg}="fendg";
$CFG{vxfen_config_fencing_mechanism}="dmp";
$CFG{vxfen_config_fencing_newdg_disks}=
 [ qw(c1t1d0 c2t1d0 c3t1d0) ];
$CFG{vxfen_config_fencing_option}=2;
```

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

You can use a CP server response file to configure server-based customized I/O fencing. The installer uses the CP server response file for the following types of I/O fencing configurations:

- Client cluster fencing (server-based I/O fencing configuration itself)
  The installer configures server-based customized I/O fencing on the VCS cluster without prompting for user input.
- Disk-based fencing with the disk group already created
  The installer configures fencing in disk-based mode on the VCS cluster without prompting for user input.
  Disk-based fencing configuration is one in which SCSI-3 disks are used as the only coordination points.
  Disk-based fencing with the disk group already created means that the disk group consisting of the coordinating disks already exists on the VCS cluster nodes.
- Disk-based fencing with the disk group to be created
  The installer creates the disk group and configures fencing properly on all the nodes in the VCS cluster without user intervention.

Disk-based fencing with the disk group to be created means that the disk group does not exist yet, but will be created with the disks mentioned as coordination point.

Table 14-2 lists the fields in the response file that are relevant for server-based customized I/O fencing.

Table 14-2 CP server response file definitions

Response file field	Definition
fencing_cpc_config_cpagent	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.
fencing_cpc_cpagentgrp	Name of the service group which will have the Coordination Point agent resource as part of it. **Note:** This field is obsolete if the `fencing_cpc_config_cpagent` field is given a value of '0'.
fencing_cpc_cps	Virtual IP address or Virtual hostname of the CP servers.
fencing_cpc_reusedg	This response file field indicates whether to reuse an existing DG name for the fencing configuration in customized fencing (CP server and coordinator disks). Enter either a "1" or "0". Entering a "1" indicates reuse, and entering a "0" indicates do not reuse. When reusing an existing DG name for the mixed mode fencing configuration. you need to manually add a line of text , such as "$CFG{fencing_cpc_reusedg}=0" or "$CFG{fencing_cpc_reusedg}=1" before proceeding with a silent installation.
fencing_cpc_dgname	The name of the disk group to be used in the customized fencing, where at least one disk is being used.

Table 14-2 CP server response file definitions *(continued)*

Response file field	Definition
fencing_cpc_diffab	This response field indicates whether the CP servers and VCS clusters use different root brokers. Entering a "1" indicates that they are using different root brokers. Entering a "0" indicates that they are not using different root brokers.
fencing_cpc_disks	The disks being used as coordination points if any.
fencing_cpc_ncps	Total number of coordination points being used, including both CP servers and disks.
fencing_cpc_ndisks	The number of disks being used.
fencing_cpc_ports	The port of the CP server that is denoted by *cps* .
fencing_cpc_ccab	The name of the authentication broker (AB) for any one of the VCS cluster nodes.
fencing_cpc_cpsabport	The port at which the authentication broker (AB) mentioned above listens for authentication..
fencing_cpc_ccabport	The port at which the authentication broker (AB) mentioned above listens for authentication.
fencing_cpc_mechanism	The disk mechanism that is used by customized fencing. The value for this field is either "raw" or "dmp"
fencing_cpc_cpsab	The name of the authentication broker (AB) for any one of the CP servers.
fencing_cpc_security	This field indicates whether security is enabled or not Entering a "1" indicates that security is enabled. Entering a "0" indicates that security has not been enabled.

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

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

```
$CFG{fencing_cpc_config_cpagent}=0;
$CFG{fencing_cpc_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cpc_dgname}="vxfencoorddg";
$CFG{fencing_cpc_diffab}=0;
$CFG{fencing_cpc_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_cpc_mechanism}="raw";
$CFG{fencing_cpc_ncps}=3;
$CFG{fencing_cpc_ndisks}=2;
$CFG{fencing_cpc_ports}{"10.200.117.145"}=14250;
$CFG{fencing_cpc_reusedg}=1;
$CFG{fencing_cpc_security}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="VCS51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_option}=1;
```

Response file variables to configure non-SCSI3 server-based I/O fencing

Table 14-3 lists the fields in the response file that are relevant for non-SCSI3 server-based customized I/O fencing.

See "About I/O fencing for VCS in virtual machines that do not support SCSI-3 PR" on page 29.

Table 14-3 Non-SCSI3 server-based I/O fencing response file definitions

Response file field	Definition
CFG{non_scsi3_fencing}	Defines whether to configure non-SCSI3 server-based I/O fencing. Valid values are 1 or 0. Enter 1 to configure non-SCSI3 server-based I/O fencing.

Table 14-3 Non-SCSI3 server-based I/O fencing response file definitions *(continued)*

Response file field	Definition
CFG {fencing_cpc_config_cpagent}	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.
CFG {fencing_cpc_cpagentgrp}	Name of the service group which will have the Coordination Point agent resource as part of it. **Note:** This field is obsolete if the `fencing_cpc_config_cpagent` field is given a value of '0'.
CFG {fencing_cpc_cps}	Virtual IP address or Virtual hostname of the CP servers.
CFG {fencing_cpc_diffab}	This response field indicates whether the CP servers and VCS clusters use different root brokers. Entering a "1" indicates that they are using different root brokers. Entering a "0" indicates that they are not using different root brokers.
CFG {fencing_cpc_ncps}	Total number of coordination points (CP servers only) being used.
CFG {fencing_cpc_ports}	The port of the CP server that is denoted by *cps* .
CFG {fencing_cpc_ccab}	The name of the authentication broker (AB) for any one of the VCS cluster nodes.
CFG {fencing_cpc_cpsabport}	The port at which the authentication broker (AB) mentioned above listens for authentication..
CFG {fencing_cpc_ccabport}	The port at which the authentication broker (AB) mentioned above listens for authentication.
CFG {fencing_cpc_cpsab}	The name of the authentication broker (AB) for any one of the CP servers.

Table 14-3 Non-SCSI3 server-based I/O fencing response file definitions *(continued)*

Response file field	Definition
CFG {fencing_cpc_security}	This field indicates whether security is enabled or not Entering a "1" indicates that security is enabled. Entering a "0" indicates that security has not been enabled.

Sample response file for configuring non-SCSI3 server-based I/O fencing

The following is a sample response file used for non-SCSI3 server-based I/O fencing :

```
$CFG{fencing_cpc_config_cpagent}=0;
$CFG{fencing_cpc_cps}=[ qw(10.198.89.251 10.198.89.252 10.198.89.253) ];
$CFG{fencing_cpc_ncps}=3;
$CFG{fencing_cpc_ndisks}=0;
$CFG{fencing_cpc_ports}{"10.198.89.251"}=14250;
$CFG{fencing_cpc_ports}{"10.198.89.252"}=14250;
$CFG{fencing_cpc_ports}{"10.198.89.253"}=14250;
$CFG{fencing_cpc_security}=1;
$CFG{non_scsi3_fencing}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="VCS51";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{vxfen_config_fencing_option}=1;
```

Section 6

Manual installation

Chapter 15

Performing preinstallation tasks

This chapter includes the following topics:

Preparing for a manual installation

Before you start installation, log in as the superuser. Mount the disc, copy the files to a temporary location locally for your convenience. Each operating system occupies an entire disc. Each disc has an identical directory structure.

To prepare for installation

1. Log in as the superuser.
2. Mount the appropriate disc.

   See "Mounting the product disc" on page 69.
3. Copy the files to a temporary location on the system.

   ```
   # cp -r depot/* /tmp/install
   ```

Requirements for installing VCS

Review requirements before you install.

See "Important preinstallation information for VCS" on page 33.

Chapter 16

Manually installing VCS

This chapter includes the following topics:

About VCS manual installation

You can manually install and configure VCS instead of using the installvcs program.

A manual installation takes a lot of time, patience, and care. Symantec recommends that you use the installvcs program instead of the manual installation when possible.

Installing VCS software manually

Table 16-1 lists the tasks that you must perform when you manually install and configure VCS 5.1SP1.

Table 16-1 Manual installation tasks for VCS 5.1SP1

Task	Reference
Install VCS software manually on each node in the cluster.	See "Installing VCS depots for a manual installation" on page 215.
Add a license key.	See "Adding a license key for a manual installation" on page 216.
Copy the installation guide to each node.	See "Copying the installation guide to each node" on page 217.

Table 16-1 Manual installation tasks for VCS 5.1SP1 *(continued)*

Task	Reference
Configure LLT and GAB.	■ See "Configuring LLT manually" on page 219. ■ See "Configuring GAB manually" on page 222.
Configure VCS.	See "Configuring VCS manually" on page 223.
Start LLT, GAB, and VCS services.	See "Starting LLT, GAB, and VCS after manual configuration" on page 225.
Modify the VCS configuration.	See "Modifying the VCS configuration" on page 226.
Replace demo license with a permanent license.	See "Replacing a VCS demo license with a permanent license for manual installations" on page 217.

Viewing the list of VCS depots

During the VCS installation, the installer prompts you with an option to choose the VCS depots to install. You can view the list of depots that each of these options would install using the installer command-line option.

Manual installation or upgrade of the product requires you to install the depots in a specified order. For example, you must install some depots before other depots because of various product dependencies. The following installer command options list the depots in the order in which you must install these depots.

Table 16-2 describes the VCS depot installation options and the corresponding command to view the list of depots.

Table 16-2 Installer command options to view VCS depots

Option	Description	Command option to view the list of depots
1	Installs only the minimal required VCS depots that provide basic functionality of the product.	`installvcs -minpkgs`
2	Installs the recommended VCS depots that provide complete functionality of the product. This option does not install the optional VCS depots.	`installvcs -recpkgs`
3	Installs all the VCS depots. You must choose this option to configure any optional VCS feature.	`installvcs -allpkgs`

To view the list of VCS depots

1 Navigate to the directory where you can start the installvcs program.

```
# cd cluster_server
```

2 Run the following command to view the list of depots. Based on what depots you want to install, enter the appropriate command option:

```
# ./installvcs -minpkgs
```

Or

```
# ./installvcs -recpkgs
```

Or

```
# ./installvcs -allpkgs
```

Installing VCS depots for a manual installation

All depots are installed into the /opt directory.

You can create lists of the depots to install.

See "Viewing the list of VCS depots" on page 214.

If you copied these files to /tmp/install, navigate to the directory and perform the following on each system:

To install VCS depots on a node

- Install the required depots in the order shown:

```
# swinstall -s `pwd` VRTSvlic
# swinstall -s `pwd` VRTSperl
# swinstall -s `pwd` VRTSspt
# swinstall -s `pwd` VRTSat
# swinstall -s `pwd` VRTSllt
# swinstall -s `pwd` VRTSgab
# swinstall -s `pwd` VRTSvxfen
# swinstall -s `pwd` VRTSamf
# swinstall -s `pwd` VRTSvcs
# swinstall -s `pwd` VRTScps
# swinstall -s `pwd` VRTSvcsag
# swinstall -s `pwd` VRTSvcsea
```

See "Veritas Cluster Server installation depots" on page 365.

Adding a license key for a manual installation

You can either add the VCS license keys or use keyless licensing for VCS.

See "Setting or changing the product level for keyless licensing" on page 216.

After you have installed all depots on each cluster node, use the `vxlicinst` command to add the VCS license key on each system:

```
# vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

Setting or changing the product level for keyless licensing

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

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

http://go.symantec.com/vom

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

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

To set or change the product level

1 View the current setting for the product level.

```
# vxkeyless -v display
```

2 View the possible settings for the product level.

```
# vxkeyless displayall
```

3 Set the desired product level.

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

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

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

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

To clear the product license level

1 View the current setting for the product license level.

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

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

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

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

Checking licensing information on the system for a manual installation

Use the `vxlicrep` utility to display information about all Veritas licenses on a system. For example, enter:

```
# vxlicrep
```

From the output, you can determine the following:

- The license key
- The type of license
- The product for which it applies
- Its expiration date, if one exists
  Demo keys have expiration dates, while permanent keys and site keys do not.

Replacing a VCS demo license with a permanent license for manual installations

When a VCS demo key license expires, you can replace it with a permanent license using the `vxlicinst` program.

See "Checking licensing information on the system" on page 140.

Copying the installation guide to each node

After you install VCS, Symantec recommends that you copy the PDF version of this guide from the installation disc

(cluster_server/docs/vcs_install_*version_platform*.pdf) to the directory /opt/VRTS/docs on each node to make it available for reference.

Where version is the release version and platform is the name of the operating system.

Chapter 17

Manually configuring VCS

This chapter includes the following topics:

Configuring LLT manually

VCS uses the Low Latency Transport (LLT) protocol for all cluster communications as a high-performance, low-latency replacement for the IP stack. LLT has two major functions.

It handles the following tasks:

- Traffic distribution
- Heartbeat traffic

To configure LLT, perform the following steps on each node in the cluster:

- Set up the file /etc/llthosts.
  See "Setting up /etc/llthosts for a manual installation" on page 220.
- Set up the file /etc/llttab.
  See "Setting up /etc/llttab for a manual installation" on page 220.
- Edit the following file on each node in the cluster to change the values of the LLT_START and the LLT_STOP environment variables to 1:
  /etc/rc.config.d/lltconf

Setting up /etc/llthosts for a manual installation

The file llthosts(4) is a database. It contains one entry per system that links the LLT system ID (in the first column) with the LLT host name. You must ensure that contents of this file are identical on all the nodes in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.

Use vi or another editor, to create the file /etc/llthosts that contains the entries that resemble:

```
0 galaxy
1 nebula
```

Setting up /etc/lltab for a manual installation

The /etc/lltab file must specify the system's ID number (or its node name), its cluster ID, and the network links that correspond to the system. In addition, the file can contain other directives. Refer also to the sample lltab file in /opt/VRTSllt.

See "About LLT directives in /etc/lltab file" on page 221.

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

```
set-node galaxy
set-cluster 2
link lan1 /dev/lan:1 - ether - -
link lan2 /dev/lan:2 - ether - -
```

The first line must identify the system where the file exists. In the example, the value for `set-node` can be: galaxy or 0. The next two lines, beginning with the link command, identify the two private network cards that the LLT protocol uses. The order of directives must be the same as in the sample lltab file in /opt/VRTSllt.

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

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

```
set-node galaxy
set-cluster 2
link lan1 /dev/lan:1 - ether - -
link lan2 /dev/lan:2 - ether - -
link-lowpri lan3 /dev/lan:3 - ether - -
```

About LLT directives in /etc/llttab file

Table 17-1 lists the LLT directives in /etc/llttab file.

Table 17-1 LLT directives

Directive	Description
`set-node`	Assigns the system ID or symbolic name. The system ID number must be unique for each system in the cluster, and must be in the range 0-31. The symbolic name corresponds to the system ID, which is in /etc/llthosts file. Note that LLT fails to operate if any systems share the same ID.
`link`	Attaches LLT to a network interface. At least one link is required, and up to eight are supported. LLT distributes network traffic evenly across all available network connections unless you mark the link as low-priority using the link-lowpri directive or you configured LLT to use destination-based load balancing. The first argument to link is a user-defined tag shown in the `lltstat(1M)` output to identify the link. It may also be used in `lltab` to set optional static MAC addresses. The second argument to link is the device name of the network interface. Its format is device_name:device_instance_number. The remaining four arguments to link are defaults; these arguments should be modified only in advanced configurations. There should be one link directive for each network interface. LLT uses an unregistered Ethernet SAP of 0xCAFE. If the SAP is unacceptable, refer to the `lltab(4)` manual page for information on how to customize SAP. Note that IP addresses do not need to be assigned to the network device; LLT does not use IP addresses.
`set-cluster`	Assigns a unique cluster number. Use this directive when more than one cluster is configured on the same physical network connection. LLT uses a default cluster number of zero.

Table 17-1 LLT directives *(continued)*

Directive	Description
`link-lowpri`	Use this directive in place of `link` for public network interfaces. This directive prevents VCS communication on the public network until the network is the last link, and reduces the rate of heartbeat broadcasts. If you use private NICs with different speed, use "link-lowpri" directive in place of "link" for all links with lower speed. Use the "link" directive only for the private NIC with higher speed to enhance LLT performance. LLT uses low-priority network links for VCS communication only when other links fail.

For more information about the LLT directives, refer to the `lltab`(4) manual page.

Additional considerations for LLT for a manual installation

You must attach each network interface that is configured for LLT to a separate and distinct physical network.

Configuring GAB manually

VCS uses the Group Membership Services/Atomic Broadcast (GAB) protocol for cluster membership and reliable cluster communications. GAB has two major functions.

It handles the following tasks:

- Cluster membership
- Cluster communications

To configure GAB

1 Set up an /etc/gabtab configuration file on each node in the cluster using vi or another editor. The following example shows an /etc/gabtab file:

```
/sbin/gabconfig -c -nN
```

Where the `-c` option configures the driver for use. The `-n`N option specifies that the cluster is not formed until at least N systems are ready to form the cluster. Symantec recommends that you set N to be the total number of systems in the cluster.

Warning: Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` can lead to a split-brain condition.

2 Edit the following file on each node in the cluster to change the values of the GAB_START and the GAB_STOP environment variables to 1:

/etc/rc.config.d/gabconf

Configuring VCS manually

VCS configuration requires the types.cf and main.cf files on each system in the cluster. Both of the files are in the /etc/VRTSvcs/conf/config directory.

main.cf file — The main.cf configuration file requires the following minimum essential elements:

- An "include" statement that specifies the file, types.cf, which defines the VCS bundled agent resources.
- The name of the cluster.
- The name of the systems that make up the cluster.

types.cf file — Note that the "include" statement in main.cf refers to the types.cf file. This text file describes the VCS bundled agent resources. During new installations, the types.cf file is automatically copied in to the /etc/VRTSvcs/conf/config directory.

When you manually install VCS, the file /etc/VRTSvcs/conf/config/main.cf contains only the line:

```
include "types.cf"
```

For a full description of the main.cf file, and how to edit and verify it, refer to the *Veritas Cluster Server Administrator's Guide*.

To configure VCS manually

1 Log on as superuser, and move to the directory that contains the configuration file:

```
# cd /etc/VRTSvcs/conf/config
```

2 Use vi or another text editor to edit the main.cf file, defining your cluster name and system names. Refer to the following example.

An example main.cf for a two-node cluster:

```
include "types.cf"
cluster VCSCluster2 ( )
system galaxy ( )
system nebula ( )
```

An example main.cf for a single-node cluster:

```
include "types.cf"
cluster VCSCluster1 ( )
system sn1
```

3 Save and close the main.cf file.

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

/etc/rc.config.d/vcsconf

Configuring the cluster UUID when creating a cluster manually

You need to configure the cluster UUID when you manually create a cluster.

To configure the cluster UUID when you create a cluster manually

- On one node in the cluster, perform the following command to populate the cluster UUID on each node in the cluster.

```
# /opt/VRTSvcs/bin/uuidconfig.pl -clus -configure nodeA
        nodeB ... nodeN
```

Where *nodeA*, *nodeB*, through *nodeN* are the names of the cluster nodes.

Starting LLT, GAB, and VCS after manual configuration

After you have configured LLT, GAB, and VCS, use the following procedures to start LLT, GAB, and VCS.

To start LLT

1 On each node, run the following command to start LLT:

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

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

```
Loading LLT Driver...
Starting LLT...
Starting LLT done.
```

2 On each node, run the following command to verify that LLT is running:

```
# /sbin/lltconfig
LLT is running
```

To start GAB

1 On each node, run the following command to start GAB:

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

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

```
GAB: Starting
GAB: Starting Done
```

2 On each node, run the following command to verify that GAB is running:

```
# /sbin/gabconfig -a
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
```

To start VCS

- On each node, type:

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

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

```
VCS:10619:'HAD' starting on: galaxy
VCS:10620:Waiting for local cluster configuration status
VCS:10625:Local cluster configuration valid
VCS:11034:registering for cluster membership
VCS:11035:Waiting for cluster membership
VCS:10077:received new cluster membership
VCS:10082:System (galaxy) is in Regular Membership -
       Membership:0x1
VCS:10073:building from local configuration
VCS:10066:entering RUNNING state
```

See "Verifying the cluster" on page 304.

Modifying the VCS configuration

After the successful installation of VCS, you can modify the configuration of VCS using several methods. You can dynamically modify the configuration from the command line, Veritas Operations Manager, or the Cluster Manager (Java Console). For information on management tools, refer to the *Veritas Cluster Server Administrator's Guide*.

You can also edit the main.cf file directly. For information on the structure of the main.cf file, refer to the *Veritas Cluster Server Administrator's Guide*.

Configuring the ClusterService group

When you have installed VCS, and verified that LLT, GAB, and VCS work, you can create a service group to include the optional features. These features include the VCS notification components, and the Global Cluster option. If you manually added VCS to your cluster systems, you must manually create the ClusterService group. You can refer to the configuration examples of a system with a ClusterService group.

See "Sample main.cf file for VCS clusters" on page 398.

Chapter 18

Manually configuring the clusters for data integrity

This chapter includes the following topics:

- Setting up disk-based I/O fencing manually
- Setting up server-based I/O fencing manually
- Setting up non-SCSI3 fencing in virtual environments manually

Setting up disk-based I/O fencing manually

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

Table 18-1 Tasks to set up I/O fencing manually

Task	Reference
Initializing disks as VxVM disks	See "Initializing disks as VxVM disks" on page 143.
Identifying disks to use as coordinator disks	See "Identifying disks to use as coordinator disks" on page 228.
Checking shared disks for I/O fencing	See "Checking shared disks for I/O fencing" on page 147.
Setting up coordinator disk groups	See "Setting up coordinator disk groups" on page 228.
Creating I/O fencing configuration files	See "Creating I/O fencing configuration files" on page 229.

Table 18-1 Tasks to set up I/O fencing manually *(continued)*

Task	Reference
Modifying VCS configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 230.
Configuring Coordination Point agent to monitor coordination points	See "Configuring Coordination Point agent to monitor coordination points" on page 241.
Verifying I/O fencing configuration	See "Verifying I/O fencing configuration" on page 232.

Identifying disks to use as coordinator disks

Make sure you initialized disks as VxVM disks.

See "Initializing disks as VxVM disks" on page 143.

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 147.

Setting up coordinator disk groups

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

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

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

The following example procedure assumes that the disks have the device names c1t1d0, c2t1d0, and c3t1d0.

To create the vxfencoorddg disk group

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

```
# vxdg init vxfencoorddg c1t1d0 c2t1d0 c3t1d0
```

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

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

3 Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

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

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

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

```
# vxdg deport vxfencoorddg
```

Creating I/O fencing configuration files

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

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

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

1 On each nodes, type:

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

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

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

2 Update the /etc/vxfenmode file to specify to use the SCSI-3 dmp disk policy. On all cluster nodes, type:

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

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

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

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

/etc/rc.config.d/vxfenconf

Modifying VCS configuration to use I/O fencing

After you add coordination points and configure I/O fencing, add the UseFence = SCSI3 cluster attribute to the VCS configuration file /etc/VRTSvcs/conf/config/main.cf. If you reset this attribute to UseFence = None, VCS does not make use of I/O fencing abilities while failing over service groups. However, I/O fencing needs to be disabled separately.

To modify VCS configuration to enable I/O fencing

1 Save the existing configuration:

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

2 Stop VCS on all nodes:

```
# hastop -all
```

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

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

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

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

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

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

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

6 Save and close the file.

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

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

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

For example, on each remaining node, enter:

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

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

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

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

- Start VCS.

  ```
  # /opt/VRTS/bin/hastart
  ```

Verifying I/O fencing configuration

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

To verify I/O fencing configuration

1 On one of the nodes, type:

```
# vxfenadm -d
```

Output similar to the following appears if the SCSI3 disk policy is dmp:

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

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

   * 0 (galaxy)
   1 (nebula)

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

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

```
# vxfenconfig -l
```

Setting up server-based I/O fencing manually

Tasks that are involved in setting up server-based I/O fencing manually include:

Table 18-2 Tasks to set up server-based I/O fencing manually

Action	Description
Preparing the CP servers for use by the VCS cluster	See "Preparing the CP servers manually for use by the VCS cluster" on page 233.
Modifying I/O fencing configuration files to configure server-based I/O fencing	See "Configuring server-based fencing on the VCS cluster manually" on page 237.

Table 18-2 Tasks to set up server-based I/O fencing manually *(continued)*

Action	Description
Modifying VCS configuration to use I/O fencing	See "Modifying VCS configuration to use I/O fencing" on page 230.
Configuring Coordination Point agent to monitor coordination points	See "Configuring Coordination Point agent to monitor coordination points" on page 241.
Verifying the server-based I/O fencing configuration	See "Verifying server-based I/O fencing configuration" on page 243.

Preparing the CP servers manually for use by the VCS cluster

Use this procedure to manually prepare the CP server for use by the VCS cluster or clusters.

Table 18-3 displays the sample values used in this procedure.

Table 18-3 Sample values in procedure

CP server configuration component	Sample name
CP server	mycps1.symantecexample.com
Node #1 - VCS cluster	galaxy
Node #2 - VCS cluster	nebula
Cluster name	clus1
Cluster UUID	{f0735332-1dd1-11b2}

To manually configure CP servers for use by the VCS cluster

1 Determine the cluster name and uuid on the VCS cluster.

For example, issue the following commands on one of the VCS cluster nodes (galaxy):

```
# grep cluster /etc/VRTSvcs/conf/config/main.cf

cluster clus1

# cat /etc/vx/.uuids/clusuuid

{f0735332-1dd1-11b2}
```

2 Use the `cpsadm` command to check whether the VCS cluster and nodes are present in the CP server.

For example:

```
# cpsadm -s mycps1.symantecexample.com -a list_nodes

ClusName  UUID                 Hostname(Node ID) Registered
clus1  {f0735332-1dd1-11b2} galaxy(0)         0
clus1  {f0735332-1dd1-11b2} nebula(1)         0
```

If the output does not show the cluster and nodes, then add them as described in the next step.

For detailed information about the `cpsadm` command, see the *Veritas Cluster Server Administrator's Guide*.

3 Add the VCS cluster and nodes to each CP server.

For example, issue the following command on the CP server (mycps1.symantecexample.com) to add the cluster:

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

Cluster clus1 added successfully
```

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

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

Node 0 (galaxy) successfully added
```

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

```
# cpsadm -s mycps1.symantecexample.com -a add_node\
 -c clus1 -u {f0735332-1dd1-11b2} -h nebula -n1

Node 1 (nebula) successfully added
```

4 If security is to be enabled, check whether the _HA_VCS_ users are created in the CP server.

If the output below does not show the users, then add them as described in the next step.

```
# cpsadm -s mycps1.symantecexample.com -a list_users

Username/Domain Type  Cluster Name / UUID         Role

_HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com/vx
                      clus1/{f0735332-1dd1-11b2} Operator

_HA_VCS_nebula@HA_SERVICES@nebula.symantec.com/vx
                      clus1/{f0735332-1dd1-11b2} Operator
```

If security is to be disabled, then add the user name "cpsclient@hostname" to the server instead of the _HA_VCS_ users (for example, cpsclient@galaxy).

The CP server can only run in either secure mode or non-secure mode, both connections are not accepted at the same time.

5 Add the users to the CP server.

First, determine the user@domain to be added on the VCS cluster (application cluster).

The user for fencing should be of the form _HA_VCS_*short-hostname* and domain name is that of HA_SERVICES user in the output of command:

```
# /opt/VRTScps/bin/cpsat listpd -t local
```

Next, issue the following commands on the CP server (mycps1.symantecexample.com):

```
# cpsadm -s mycps1.symantecexample.com -a add_user -e\
 _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com\
 -f cps_operator -g vx

User _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com
successfully added

# cpsadm -s mycps1.symantecexample.com -a add_user -e\
 _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com\
 -f cps_operator -g vx

User _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com
successfully added
```

6 Authorize the CP server user to administer the VCS cluster. You must perform this task for the CP server users corresponding to each node in the VCS cluster.

For example, issue the following command on the CP server (mycps1.symantecexample.com) for VCS cluster clus1 with two nodes galaxy and nebula:

```
# cpsadm -s mycps1.symantecexample.com -a\
add_clus_to_user -c clus1\
 -u {f0735332-1dd1-11b2}\
 -e _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com\
 -f cps_operator -g vx

Cluster successfully added to user
 _HA_VCS_galaxy@HA_SERVICES@galaxy.symantec.com privileges.

# cpsadm -s mycps1.symantecexample.com -a\
add_clus_to_user -c clus1\
 -u {f0735332-1dd1-11b2}\
 -e _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com\
 -f cps_operator -g vx

Cluster successfully added to user
 _HA_VCS_nebula@HA_SERVICES@nebula.symantec.com privileges.
```

Configuring server-based fencing on the VCS cluster manually

The configuration process for the client or VCS cluster to use CP server as a coordination point requires editing the `/etc/vxfenmode` file.

You need to edit this file to specify the following information for your configuration:

- Fencing mode
- Fencing mechanism
- Fencing disk policy (if applicable to your I/O fencing configuration)
- Appropriate value for the security configuration
- CP server or CP servers
- Coordinator disk group (if applicable to your I/O fencing configuration)

Note: Whenever coordinator disks are used as coordination points in your I/O fencing configuration, you must create a disk group (vxfendg). You must specify this disk group in the `/etc/vxfenmode` file.

See "Setting up coordinator disk groups" on page 228.

The customized fencing framework also generates the `/etc/vxfentab` file which has security setting and the coordination points (all the CP servers and disks from disk group specified in `/etc/vxfenmode` file).

To configure server-based fencing on the VCS cluster manually

1. Use a text editor to edit the following file on each node in the cluster:

   `/etc/rc.config.d/vxfenconf`

   You must change the values of the VXFEN_START and the VXFEN_STOP environment variables to 1.

2. Use a text editor to edit the `/etc/vxfenmode` file values to meet your configuration specifications.

   If your server-based fencing configuration uses a single highly available CP server as its only coordination point, make sure to add the `single_cp=1` entry in the `/etc/vxfenmode` file.

   The following sample file output displays what the `/etc/vxfenmode` file contains:

   See "Sample vxfenmode file output" on page 238.

3. After editing the `/etc/vxfenmode` file, run the vxfen init script to start fencing.

   For example:

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

Sample vxfenmode file output

The following sample file output displays

```
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
```

```
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps      - use a coordination point server with optional script
#            controlled scsi3 disks
#
vxfen_mechanism=cps

#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks. This field is
# required only if customized coordinator disks are being used.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
scsi3_disk_policy=dmp

# security when enabled uses secure communication to the cp server
# using VxAT (Veritas Authentication Service)
# available options:
# 0 - don't use Veritas Authentication Service for cp server
#   communication
# 1  - use Veritas Authentication Service for cp server
#   communication
security=1

#
# Specify 3 or more odd number of coordination points in this file,
# one in each row. They can be all-CP servers, all-SCSI-3 compliant
# coordinator disks, or a combination of CP servers and SCSI-3
# compliant coordinator disks. Please ensure that the CP server
# coordination points are numbered sequentially and in the same
# order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
#  cps<number>=<Virtual IP/ Virtual hostname of cp server> in
# square brackets ([]), followed by ":" and CPS port number.
```

```
#
# Examples:
# cps1=[192.168.0.23]:14250
# cps2=[mycps.company.com]:14250
#
# SCSI-3 compliant coordinator disks are specified as:
#
#  vxfendg=<coordinator disk group name>
# Example:
#  vxfendg=vxfencoorddg
#
# Examples of different configurations:
#  1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
```

Table 18-4 defines the vxfenmode parameters that must be edited.

Table 18-4 vxfenmode file parameters

vxfenmode File Parameter	Description
vxfen_mode	Fencing mode of operation. This parameter must be set to “customized”.
vxfen_mechanism	Fencing mechanism. This parameter defines the mechanism that is used for fencing. If one of the three coordination points is a CP server, then this parameter must be set to “cps”.
scsi3_disk_policy	Configure the vxfen module to use either DMP devices, "dmp" or the underlying raw character devices, "raw". **Note:** The configured disk policy is applied on all the nodes.

Table 18-4 vxfenmode file parameters *(continued)*

vxfenmode File Parameter	Description
security	Security parameter 1 indicates that Symantec Product Authentication Service is used for CP server communications. Security parameter 0 indicates that communication with the CP server is made in non-secure mode. The default security value is 1. **Note:** Symantec only supports a configuration where both the CP server and client sides have the same security setting. The security setting on both sides must be either enabled or disabled.
cps1, cps2, cps3, or vxfendg	Coordination point parameters. Enter either the Virtual IP address or FQHN (whichever is accessible) of the CP server. **Note:** Whenever coordinator disks are used in an I/O fencing configuration, a disk group has to be created (vxfendg) and specified in the /etc/vxfenmode file. Additionally, the customized fencing framework also generates the /etc/vxfentab file which specifies the security setting and the coordination points (all the CP servers and the disks from disk group specified in /etc/vxfenmode file).
single_cp	Value 1 for single_cp parameter indicates that the server-based fencing uses a single highly available CP server as its only coordination point. Value 0 for single_cp parameter indicates that the server-based fencing uses at least three coordination points.

Configuring Coordination Point agent to monitor coordination points

The following procedure describes how to manually configure the Coordination Point agent to monitor coordination points (CP server or SCSI-3 disks).

To configure Configuration Point agent to monitor coordination points

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

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

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

```
# hares -state coordpoint
```

The following is an example of the command and output:

```
# hares -state coordpoint

# Resource    Attribute   System   Value
coordpoint   State        galaxy   ONLINE
coordpoint   State        nebula   ONLINE
```

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

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

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

```
# haconf -makerw

# hatype -modify Coordpoint LogDbg 10

# haconf -dump -makero
```

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

/var/VRTSvcs/log/engine_A.log

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

Verifying server-based I/O fencing configuration

Follow the procedure described below to verify your server-based I/O fencing configuration.

To verify the server-based I/O fencing configuration

1 Verify that the I/O fencing configuration was successful by running the `vxfenadm` command.

For example, run the following command:

```
# vxfenadm -d
```

Note: For troubleshooting any server-based I/O fencing configuration issues, refer to the *Veritas Cluster Server Administrator's Guide*.

2 Verify that I/O fencing is using the specified coordination points by running the `vxfenconfig` command.

For example, run the following command:

```
# vxfenconfig -l
```

If the output displays `single_cp=1`, it indicates that the application cluster uses a CP server as the single coordination point for server-based fencing.

Setting up non-SCSI3 fencing in virtual environments manually

To manually set up I/O fencing in a non-SCSI-3 PR compliant setup

1 Configure I/O fencing in customized mode with only CP servers as coordination points.

See "Setting up server-based I/O fencing manually" on page 232.

2 Make sure that the VCS cluster is online and check that the fencing mode is customized.

```
# vxfenadm -d
```

3 Make sure that the cluster attribute UseFence is set to SCSI3.

```
# haclus -value UseFence
```

4 On each node, edit the /etc/vxenviron file as follows:

```
data_disk_fencing=off
```

5 Enter the following command to change the vxfen_min_delay parameter value:

```
# /usr/sbin/kctune vxfen_vxfnd_tmt=25
```

6 On each node, edit the /etc/vxfenmode file as follows:

```
loser_exit_delay=55
vxfen_script_timeout=25
```

Refer to the sample /etc/vxfenmode file.

7 On each node, set the value of the LLT sendhbcap timer parameter value as follows:

- Run the following command:

```
lltconfig -T sendhbcap:3000
```

- Add the following line to the /etc/llttab file so that the changes remain persistent after any reboot:

```
set-timer senhbcap:3000
```

8 On any one node, edit the VCS configuration file as follows:

- Make the VCS configuration file writable:

```
# haconf -makerw
```

- For each resource of the type DiskGroup, set the value of the MonitorReservation attribute to 0 and the value of the Reservation attribute to NONE.

```
# hares -modify <dg_resource> MonitorReservation 0

# hares -modify <dg_resource> Reservation "NONE"
```

- Run the following command to verify the value:

```
# hares -list Type=DiskGroup MonitorReservation!=0

# hares -list Type=DiskGroup Reservation!="NONE"
```

The command should not list any resources.

- Modify the default value of the Reservation attribute at type-level.

```
# haattr -default DiskGroup Reservation "NONE"
```

- Make the VCS configuration file read-only

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

9 Make sure that the UseFence attribute in the VCS configuration file main.cf is set to SCSI3.

10 To make these VxFEN changes take effect, stop and restart VxFEN and the dependent modules

- On each node, run the following command to stop VCS:

```
/sbin/init.d/vcs stop
```

- After VCS takes all services offline, run the following command to stop VxFEN:

```
/sbin/init.d/vxfen stop
```

- On each node, run the following commands to restart VxFEN and VCS:

```
# /sbin/init.d/vxfen start
# /sbin/init.d/vcs start
```

Sample /etc/vxfenmode file for non-SCSI3 fencing

```
================================
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3      - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled   - run the driver but don't do any actual fencing
#
vxfen_mode=customized

# vxfen_mechanism determines the mechanism for customized I/O
# fencing that should be used.
#
# available options:
# cps      - use a coordination point server with optional script
#            controlled scsi3 disks
#
vxfen_mechanism=cps
```

```
#
# scsi3_disk_policy determines the way in which I/O Fencing communicates wi
# the coordination disks. This field is required only if customized
# coordinator disks are being used.
#
# available options:
# dmp - use dynamic multipathing
# raw - connect to disks using the native interface
#
# scsi3_disk_policy=dmp

#
# Seconds for which the winning sub cluster waits to allow for the losing
# subcluster to panic & drain I/Os. Useful in the absence of SCSI3 based
# data disk fencing
loser_exit_delay=55

#
# Seconds for which vxfend process wait for a customized fencing
# script to complete. Only used with vxfen_mode=customized
vxfen_script_timeout=25

#
# security when enabled uses secure communication to the cp server
# using VxAT (Veritas Authentication Service)
# available options:
# 0 - don't use Veritas Authentication Service for cp server
#   communication
# 1  - use Veritas Authentication Service for cp server
#   communication
security=1

#
# Specify 3 or more odd number of coordination points in this file,
# one in each row. They can be all-CP servers, all-SCSI-3 compliant
# coordinator disks, or a combination of CP servers and SCSI-3 compliant
# coordinator disks. Please ensure that the CP server coordination points
# are numbered sequentially and in the same order on all the cluster nodes.
#
# Coordination Point Server(CPS) is specified as:
#
#  cps<number>=<Virtual IP/Virtual hostname of cp server> in square
```

```
# brackets ([]), followed by ":" and CPS port number.
#
# Examples:
#  cps1=[192.168.0.23]:14250
# cps2=[mycps.company.com]:14250
#
# SCSI-3 compliant coordinator disks are specified as:
#
#  vxfendg=<coordinator disk group name>
# Example:
#  vxfendg=vxfencoorddg
#
# Examples of different configurations:
#  1. All CP server coordination points
# cps1=
# cps2=
# cps3=
#
# 2. A combination of CP server and a disk group having two SCSI-3
# coordinator disks
# cps1=
# vxfendg=
# Note: The disk group specified in this case should have two disks
#
# 3. All SCSI-3 coordinator disks
# vxfendg=
# Note: The disk group specified in case should have three disks
#
cps1=[mycps1.company.com]:14250
cps2=[mycps2.company.com]:14250
cps3=[mycps3.company.com]:14250
================================
```

Section 7

Upgrading VCS

Chapter 19

Planning to upgrade VCS

This chapter includes the following topics:

About upgrading to VCS 5.1SP1

You can upgrade VCS using one of the following methods:

- Typical upgrade using Veritas product installer or the installvcs program
  See "Upgrading VCS using the script-based installer" on page 258.
- Typical upgrade Veritas Web installer
- Phased upgrade to reduce downtime
  See "Performing a phased upgrade" on page 261.
- Automated upgrade using response files
  See "Upgrading VCS using response files" on page 277.

You can upgrade VCS 5.1SP1 to Storage Foundation High Availability 5.1SP1 using Veritas product installer or response files.

See the *Veritas Storage Foundation and High Availability Installation Guide.*

VCS supported upgrade paths

Table 19-1 lists the supported upgrade paths.

Table 19-1 Supported upgrade paths

From	To
VCS 4.1 on HP-UX 11i v2	VCS 5.1SP1 on HP-UX 11i v3
VCS 5.0 on HP-UX 11i v2	VCS 5.1SP1 on HP-UX 11i v3
VCS 5.0 on HP-UX 11i v3	VCS 5.1SP1 on HP-UX 11i v3
VCS 5.0.1 on HP-UX 11i v3	VCS 5.1SP1 on HP-UX 11i v3

Note: If you are upgrading from VCS version 3.5, you need to first upgrade to version 4.1, and then upgrade to VCS 5.1 SP1.

Upgrading VCS in secure enterprise environments

In secure enterprise environments, ssh or remsh communication is not allowed between systems. In such cases, the installvcs program can upgrade VCS only on systems with which it can communicate (most often the local system only).

Warning: If you are running the cluster in secure mode, make sure to remove the file /tmp/disable_selfcont from the cluster before upgrading to VCS 5.1SP1.

To upgrade VCS in secure enterprise environments with no remsh or ssh communication

1 Run the installvcs program on each node to upgrade the cluster to VCS 5.1SP1.

On each node, the installvcs program updates the configuration, stops the cluster, and then upgrades VCS on the node. The program also generates a cluster UUID on the node. Each node may have a different cluster UUID at this point.

2 Start VCS on the first node.

```
# hastart
```

VCS comes up with the cluster UUID on this node. Run the following command to display the cluster UUID on the local node:

```
# /opt/VRTSvcs/bin/uuidconfig.pl -clus -display systemname
```

3 On each of the other nodes, do the following:

- Set the value of the VCS_HOST environment variable as the name of the first node.
- Display the value of the CID attribute that stores the cluster UUID:

```
# haclus -value CID
```

- Copy the output of the CID attribute to the file /etc/vx/.uuids/clusuuid.
- Clear the value of VCS_HOST.
- Start VCS.
  The node must successfully join the already running nodes in the cluster.
  See "Verifying LLT, GAB, and cluster operation" on page 300.

About phased upgrade

Perform a phased upgrade to minimize the downtime for the cluster. Depending on the situation, you can calculate the approximate downtime as follows:

You can fail over all your service groups to the nodes that are up.	Downtime equals the time that is taken to offline and online the service groups.
You have a service group that you cannot fail over to a node that runs during upgrade.	Downtime for that service group equals the time that is taken to perform an upgrade and restart the node.

Prerequisites for a phased upgrade

Before you start the upgrade, confirm that you have licenses for all the nodes that you plan to upgrade.

Planning for a phased upgrade

Plan the movement of the service groups from one node to another to minimize the downtime for any particular service group.

Some rough guidelines follow:

- Split the cluster into two subclusters of equal or near equal size.
- Split the cluster so that your high priority service groups remain online during the upgrade of the first subcluster.

Phased upgrade limitations

The following limitations primarily describe not to tamper with configurations or service groups during the phased upgrade:

- While you perform the upgrades, do not start any modules.
- When you start the installer, only select VCS.
- While you perform the upgrades, do not add or remove service groups from any of the nodes.
- Depending on your configuration, you may find that you cannot upgrade multiple nodes at the same time. You may only be able to upgrade one node at a time.
- For very large clusters, you might have to repeat these steps multiple times to upgrade your cluster.

Phased upgrade example

In this example, you have four nodes: node01, node02, node03, and node04. You also have four service groups: sg1, sg2, sg3, and sg4. For the purposes of this example, the cluster is split into two subclusters. The nodes node01 and node02 are in the first subcluster, which you first upgrade. The nodes node03 and node04 are in the second subcluster, which you upgrade last.

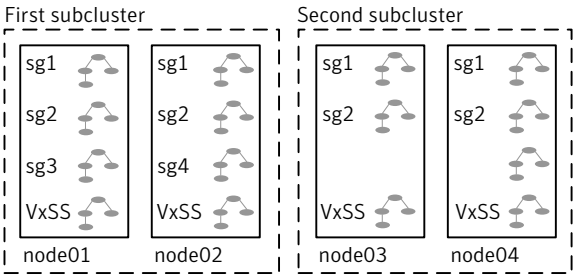
Each service group is running on the nodes as follows:

- sg1 and sg2 are parallel service groups and run on all the nodes.
- sg3 and sg4 are failover service groups. sg3 runs on node01 and sg4 runs on node02.
- VxSS service group runs on all nodes (secure mode is enabled)

In your system list, you have each service group that fails over to other nodes as follows:

- sg1 and sg2 are running on all the nodes.
- sg3 and sg4 can fail over to any of the nodes in the cluster.
- VxSS service group runs on all nodes

Figure 19-1 Example of phased upgrade set up



Phased upgrade example overview

This example's upgrade path follows:

- Move all the service groups from the first subcluster to the second subcluster.
- Upgrade the operating system on the first subcluster's nodes, if required.
- On the first subcluster, start the upgrade using the installation program.
- Get the second subcluster ready.
- Activate the first subcluster.
- Upgrade the operating system on the second subcluster's nodes, if required.
- On the second subcluster, start the upgrade using the installation program.
- Activate the second subcluster.

See "Performing a phased upgrade" on page 261.

Chapter 20

Performing a typical VCS upgrade using the installer

This chapter includes the following topics:

Before upgrading from 4.x using the script-based or Web-based installer

Before you upgrade VCS, perform the following steps if you are upgrading from VCS 4.x. You first need to remove deprecated resource types and modify changed values.

To prepare to upgrade to VCS 5.1SP1 from VCS 4.x

1. Remove deprecated resources and modify attributes. The installer program can erase obsolete types and resources can be erased from the system or you can manually remove them.

   See "Manually removing deprecated resource types and modifying attributes" on page 390.

2. Stop the application agents that are installed on the VxVM disk (for example the NBU agent).

   Perform the following steps to stop the application agents:

   - Take the resources offline on all systems that you want to upgrade.

     ```
     # hares -offline resname -sys sysname
     ```

- Stop the application agents that are installed on VxVM disk on all the systems.

  ```
  # haagent -stop agentname -sys sysname
  ```

- Ensure that the agent processes are not running.

  ```
  # ps -ef | grep agentname
  ```

  This command does not list any processes in the VxVM installation directory.

3 Make sure that LLT, GAB, and VCS are running on all of the nodes in the cluster. The installer program cannot proceed unless these processes are running.

```
# lltconfig
```

LLT is running

```
# gabconfig -a

=======================================================
Port a gen cc701 membership 01
Port h gen cc704 membership 01
```

Upgrading VCS using the script-based installer

You can use the product installer to upgrade VCS.

To upgrade VCS using the product installer

1 Log in as superuser and mount the product disc.

2 Start the installer.

```
# ./installer
```

The installer starts the product installation program with a copyright message. It then specifies where it creates the logs. Note the log's directory and name.

3 From the opening Selection Menu, choose: **G** for "Upgrade a Product."

4 Enter the names of the nodes that you want to upgrade. Use spaces to separate node names. Press the Enter key to proceed.

The installer runs some verification checks on the nodes.

5 When the verification checks are complete, the installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.

The installer lists the depots to upgrade.

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

The installer stops VCS processes, uninstalls depots, installs, upgrades, and configures VCS.

7 The installer lists the nodes that Symantec recommends you restart.

8 The installer asks if you would like to send the information about this installation to Symantec to help improve installation in the future. Enter your response.

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

9 If you want to upgrade CP server systems that use VCS or SFHA to VCS 5.1SP1, make sure that you upgraded all application clusters to version VCS 5.1SP1. Then, upgrade VCS or SFHA on the CP server systems.

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

If you are upgrading from 4.x, you may need to create new VCS accounts if you used native OS accounts.

See "Creating new VCS accounts if you used native operating system accounts" on page 391.

Upgrading VCS with the Veritas Web-based installer

This section describes how to upgrade VCS with the Veritas Web-based installer. The installer detects and upgrades the product that is currently installed on the specified system or systems. If you want to upgrade to a different product, you may need to perform additional steps.

To upgrade VCS

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 168.

3 On the Select a task and a product page, select **Upgrade a Product**.

The installer detects the product that is installed on the specified system.

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

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

6 Click **Next** to complete the upgrade.

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

7 After the upgrade, if the product is not configured, the web-based installer asks: "Do you want to configure this product?" If the product is already configured, it will not ask any questions.

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

9 If you want to upgrade VCS or SFHA 5.1 on the CP server systems to version VCS 5.1SP1, make sure that you upgraded all application clusters to version VCS 5.1SP1. Then, upgrade VCS or SFHA on the CP server systems. For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

If you are upgrading from 4.x, you may need to create new VCS accounts if you used native operating system accounts.

See "Creating new VCS accounts if you used native operating system accounts" on page 391.

Chapter 21

Performing a phased upgrade

This chapter includes the following topics:

Performing a phased upgrade

This section explains how to perform a phased upgrade of VCS on four nodes with four service groups. Note that in this scenario, VCS and the service groups cannot stay online on the second subcluster during the upgrade of the second subcluster and vice versa. Do not add, remove, or change resources or service groups on any nodes during the upgrade. These changes are likely to get lost after the upgrade. The following example illustrates the steps to perform a phased upgrade. The phased upgrade is on a secure cluster.

You can perform a phased upgrade from VCS 5.0.1 to VCS 5.1SP1.

See "About phased upgrade" on page 253.

See "Phased upgrade example" on page 254.

Moving the service groups to the second subcluster

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

To move service groups to the second subcluster

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

```
# hagrp -state
```

The output resembles the following:

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

2 Take the parallel service groups (sg1 and sg2) and the VXSS group offline from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (node01 and node02) to the nodes on the second subcluster (node03 and node04).

```
# hagrp -offline sg1 -sys node01
# hagrp -offline sg2 -sys node01
# hagrp -offline sg1 -sys node02
# hagrp -offline sg2 -sys node02
# hagrp -offline VxSS -sys node01
# hagrp -offline VxSS -sys node02
# hagrp -switch sg3 -to node03
# hagrp -switch sg4 -to node04
```

3 On the nodes in the first subcluster, stop all VxVM volumes (for each disk group) that VCS does not manage.

4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

5 Freeze the nodes in the first subcluster.

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

6 Dump the configuration and make it read-only.

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

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

```
# hagrp -state
```

Output resembles:

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

8 Perform this step on the nodes (node01 and node02) in the first subcluster if the cluster uses I/O Fencing. Use an editor of your choice and change the following:

- In the `/etc/vxfenmode` file, change the value of the vxfen_mode variable from scsi3 to disabled. You want the line in the `vxfenmode` file to resemble:

  ```
  vxfen_mode=disabled
  ```

- In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the UseFence attribute from SCSI3 to NONE. You want the line in the `main.cf` file to resemble:

  ```
  UseFence = NONE
  ```

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

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

Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required. Refer to the operating system's documentation for more information.

Upgrading the first subcluster

You now navigate to the installer program and start it.

To start the installer for the phased upgrade

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Make sure that you can ssh or remsh from the node where you launched the installer to the nodes in the second subcluster without requests for a password.
3. Navigate to the folder that contains installvcs.

   ```
   # cd /cluster_server
   ```

4. Start the installvcs program, specify the nodes in the first subcluster (node1 and node2).

   ```
   # ./installvcs node1 node2
   ```

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

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

   ```
   Do you agree with the terms of the End User License Agreement
   as specified in the cluster_server/EULA/<lang>/EULA_VCS_Ux_5.1SP1PR1.pdf
   file present on media? [y,n,q,?] y
   ```

6. Review the available installation options.

   See "Veritas Cluster Server installation depots" on page 365.

   1. Installs only the minimal required VCS depots that provides basic functionality of the product.
   2. Installs the recommended VCS depots that provide complete functionality of the product. This option does not install the optional VCS depots.

      Note that this option is the default.
   3. Installs all the VCS depots.

      You must choose this option to configure any optional VCS feature.
   4. Displays the VCS depots for each option.

      For this example, select 3 for all depots.

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

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

8 When you are prompted, reply **y** to continue with the upgrade.

```
Do you want to continue? [y,n,q] (y)
```

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

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

10 The installer ends for the first subcluster with the following output:

```
    Configuring VCS: 100%

    Estimated time remaining: 0:00

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

Veritas Cluster Server Configure completed successfully


You are performing phased upgrade (Phased 1) on the systems.
Follow  the steps in install guide to upgrade the remaining
systems.

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

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the Preparing the second subcluster procedure.

Preparing the second subcluster

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

To prepare to upgrade the second subcluster

1 Get the summary of the status of your resources.

```
# hastatus -summ
-- SYSTEM STATE
-- System               State                Frozen

A  node01               EXITED                1
A  node02               EXITED                1
A  node03               RUNNING               0
A  node04               RUNNING               0

-- GROUP STATE
-- Group           System  Probed     AutoDisabled    State

B  SG1             node01   Y          N               OFFLINE
B  SG1             node02   Y          N               OFFLINE
B  SG1             node03   Y          N               ONLINE
B  SG1             node04   Y          N               ONLINE
B  SG2             node01   Y          N               OFFLINE
B  SG2             node02   Y          N               OFFLINE
B  SG2             node03   Y          N               ONLINE
B  SG2             node04   Y          N               ONLINE
B  SG3             node01   Y          N               OFFLINE
B  SG3             node02   Y          N               OFFLINE
B  SG3             node03   Y          N               ONLINE
B  SG3             node04   Y          N               OFFLINE
B  SG4             node01   Y          N               OFFLINE
B  SG4             node02   Y          N               OFFLINE
B  SG4             node03   Y          N               OFFLINE
B  SG4             node04   Y          N               ONLINE
B  VxSS            node01   Y          N               OFFLINE
B  VxSS            node02   Y          N               OFFLINE
B  VxSS            node03   Y          N               ONLINE
B  VxSS            node04   Y          N               ONLINE
```

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

3 Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

4 Unfreeze the service groups.

```
# hagrp -unfreeze sg1 -persistent
# hagrp -unfreeze sg2 -persistent
# hagrp -unfreeze sg3 -persistent
# hagrp -unfreeze sg4 -persistent
# hagrp -unfreeze VxSS -persistent
```

5 Dump the configuration and make it read-only.

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

6 Take the service groups offline on node03 and node04.

```
# hagrp -offline sg1 -sys node03
# hagrp -offline sg1 -sys node04
# hagrp -offline sg2 -sys node03
# hagrp -offline sg2 -sys node04
# hagrp -offline sg3 -sys node03
# hagrp -offline sg4 -sys node04
# hagrp -offline VxSS -sys node03
# hagrp -offline VxSS -sys node04
```

7 Verify the state of the service groups.

```
# hagrp -state
#Group       Attribute    System     Value
SG1             State      node01    |OFFLINE|
SG1             State      node02    |OFFLINE|
SG1             State      node03    |OFFLINE|
SG1             State      node04    |OFFLINE|
SG2             State      node01    |OFFLINE|
SG2             State      node02    |OFFLINE|
SG2             State      node03    |OFFLINE|
SG2             State      node04    |OFFLINE|
SG3             State      node01    |OFFLINE|
SG3             State      node02    |OFFLINE|
SG3             State      node03    |OFFLINE|
SG3             State      node04    |OFFLINE|
VxSS            State      node01    |OFFLINE|
VxSS            State      node02    |OFFLINE|
VxSS            State      node03    |OFFLINE|
VxSS            State      node04    |OFFLINE|
```

8 Perform this step on node03 and node04 if the cluster uses I/O Fencing. Use an editor of your choice and change the following:

- In the `/etc/vxfenmode` file, change the value of the vxfen_mode variable from scsi3 to disabled. You want the line in the `vxfenmode` file to resemble:

  ```
  vxfen_mode=disabled
  ```

- In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the UseFence attribute from SCSI3 to NONE. You want the line in the `main.cf` file to resemble:

  ```
  UseFence = NONE
  ```

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

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

Activating the first subcluster

Get the first subcluster ready for the service groups.

Note: These steps fulfill part of the installer's output instructions, see Upgrading the first subcluster step 10.

To activate the first subcluster

1 Perform this step on node01 and node02 if the cluster uses I/O Fencing. Use an editor of your choice and revert the following to an enabled state before you reboot the first subcluster's nodes:

- In the `/etc/VRTSvcs/conf/config/main.cf` file, change the value of the UseFence attribute from NONE to SCSI3. You want the line in the `main.cf` file to resemble:

  ```
  UseFence = SCSI3
  ```

- In the `/etc/vxfenmode` file, change the value of the vxfen_mode variable from disabled to scsi3. You want the line in the `vxfenmode` file to resemble:

```
vxfen_mode=scsi3
```

2 Reboot the node01 and node02 in the first subcluster.

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

3 Seed node01 and node02 in the first subcluster.

```
# gabconfig -xc
```

4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

5 Unfreeze the nodes in the first subcluster.

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

6 Dump the configuration and make it read-only.

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

7 Bring the service groups online on node01 and node02.

```
# hagrp -online sg1 -sys node01
# hagrp -online sg1 -sys node02
# hagrp -online sg2 -sys node01
# hagrp -online sg2 -sys node02
# hagrp -online sg3 -sys node01
# hagrp -online sg4 -sys node02
# hagrp -online VxSS -sys node01
# hagrp -online VxSS -sys node02
```

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required. Refer to the operating system's documentation for more information.

Upgrading the second subcluster

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

To start the installer to upgrade the second subcluster

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Navigate to the folder that contains installvcs.

   ```
   # cd /cluster_server
   ```

3. Confirm that VCS is stopped on node03 and node04. Start the installvcs program, specify the nodes in the second subcluster (node3 and node4).

   ```
   # ./installvcs node3 node4
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs.
4. Enter **y** to agree to the End User License Agreement (EULA).

   ```
   Do you agree with the terms of the End User License Agreement
   as specified in the cluster_server/EULA/<lang>/EULA_VCS_Ux_5.1SP1PR1.pdf
   file present on media? [y,n,q,?] y
   ```

5. Review the available installation options.

   See "Veritas Cluster Server installation depots" on page 365.

   1. Installs only the minimal required VCS depots that provides basic functionality of the product.
   2. Installs the recommended VCS depots that provide complete functionality of the product. This option does not install the optional VCS depots.

      Note that this option is the default.
   3. Installs all the VCS depots.

      You must choose this option to configure any optional VCS feature.
   4. Displays the VCS depots for each option.

      For this example, select 3 for all depots.

      Select the depots to be installed on all systems? [1-4,q,?] (2) 3
6. The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.

7 When you are prompted, reply **y** to continue with the upgrade.

```
Do you want to continue? [y,n,q] (y)
```

8 When you are prompted, reply **y** to stop VCS processes.

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

9 Monitor the installer program answering questions as appropriate until the upgrade completes.

Finishing the phased upgrade

You now have to reboot the nodes in the second subcluster.

To finish the upgrade

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

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-remsh]
-clus -display node1 [node2 ...]
```

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

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

2 Perform this step on node03 and node04 if the cluster uses I/O Fencing. Use an editor of your choice and revert the following to an enabled state before you reboot the second subcluster's nodes:

- In the `/etc/vxfenmode` file, change the value of the vxfen_mode variable from disabled to scsi3. You want the line in the `vxfenmode` file to resemble:

  ```
  vxfen_mode=scsi3
  ```

3 Reboot the node03 and node04 in the second subcluster.

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

The nodes in the second subcluster join the nodes in the first subcluster.

4 Check to see if VCS and its components are up.

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   nxxxnn membership 0123
Port b gen   nxxxnn membership 0123
Port h gen   nxxxnn membership 0123
```

5 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```
# hastatus -sum

-- SYSTEM STATE
-- System          State           Frozen

A  node01          RUNNING         0
A  node02          RUNNING         0
A  node03          RUNNING         0
A  node04          RUNNING         0

-- GROUP STATE
-- Group    System    Probed   AutoDisabled   State

B  VxSS     node01    Y        N              ONLINE
B  VxSS     node02    Y        N              ONLINE
B  VxSS     node03    Y        N              ONLINE
B  VxSS     node04    Y        N              ONLINE
B  sg1      node01    Y        N              ONLINE
B  sg1      node02    Y        N              ONLINE
B  sg1      node03    Y        N              ONLINE
B  sg1      node04    Y        N              ONLINE
B  sg2      node01    Y        N              ONLINE
B  sg2      node02    Y        N              ONLINE
B  sg2      node03    Y        N              ONLINE
B  sg2      node04    Y        N              ONLINE
B  sg3      node01    Y        N              ONLINE
B  sg3      node02    Y        N              OFFLINE
B  sg3      node03    Y        N              OFFLINE
B  sg3      node04    Y        N              OFFLINE
B  sg4      node01    Y        N              OFFLINE
B  sg4      node02    Y        N              ONLINE
B  sg4      node03    Y        N              OFFLINE
B  sg4      node04    Y        N              OFFLINE
```

6 After the upgrade is complete, mount the VxFS file systems and start the VxVM volumes (for each disk group) that VCS does not manage.

In this example, you have performed a phased upgrade of VCS. The service groups were down when you took them offline on node03 and node04, to the time VCS brought them online on node01 or node02.

Note: If you want to upgrade CP server systems that use VCS or SFHA to 5.1 SP1, make sure that you upgraded all application clusters to version 5.1 SP1. Then, upgrade VCS or SFHA on the CP server systems. For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

Chapter 22

Performing an automated VCS upgrade using response files

This chapter includes the following topics:

Upgrading VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS upgrade on one cluster to upgrade VCS on other clusters. You can also create a response file using the `-makeresponsefile` option of the installer.

To perform automated VCS upgrade

1. Make sure the systems where you want to upgrade VCS meet the upgrade requirements.
2. Make sure the pre-upgrade tasks are completed.
3. Copy the response file to one of the cluster systems where you want to upgrade VCS.

   See "Sample response file for upgrading VCS" on page 280.
4. Edit the values of the response file variables as necessary.

   See "Response file variables to upgrade VCS" on page 278.

5 Mount the product disk, and navigate to the folder that contains the installation program.

6 Start the upgrade from the system to which you copied the response file. For example:

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

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

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

Response file variables to upgrade VCS

Table 22-1 lists the response file variables that you can define to upgrade VCS.

Table 22-1 Response file variables specific to upgrading VCS

Variable	List or Scalar	Description
CFG{opt}{upgrade}	Scalar	Upgrades VCS depots. (Required)
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{opt}{systems}	List	List of systems on which the product is to be upgraded. (Required)
CFG{prod}	Scalar	Defines the product to be upgraded. The value is VCS51 for VCS. (Required)
CFG{vcs_allowcomms}	Scalar	Indicates whether or not to start LLT and GAB when you set up a single-node cluster. The value can be 0 (do not start) or 1 (start). (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)

Table 22-1 Response file variables specific to upgrading VCS *(continued)*

Variable	List or Scalar	Description
CFG{opt}{patchpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. (Optional)
CFG{opt}{pkgpath}	Scalar	Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *remsh* must be used instead of ssh as the communication method between systems. (Optional)

Sample response file for upgrading VCS

Review the response file variables and their definitions.

See "Response file variables to upgrade VCS" on page 278.

```
#
# Configuration Values:
#
our %CFG;

$CFG{accepteula}=1;
$CFG{vcs_allowcomms}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="VCS51";
$CFG{systems}=[ qw( galaxy nebula) ];
1;
```

Section 8

Post-installation tasks

Chapter 23

Performing post-installation tasks

This chapter includes the following topics:

About enabling LDAP authentication for clusters that run in secure mode

Symantec Product Authentication Service (AT) supports LDAP (Lightweight Directory Access Protocol) user authentication through a plug-in for the authentication broker. AT supports all common LDAP distributions such as Sun Directory Server, Netscape, OpenLDAP, and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

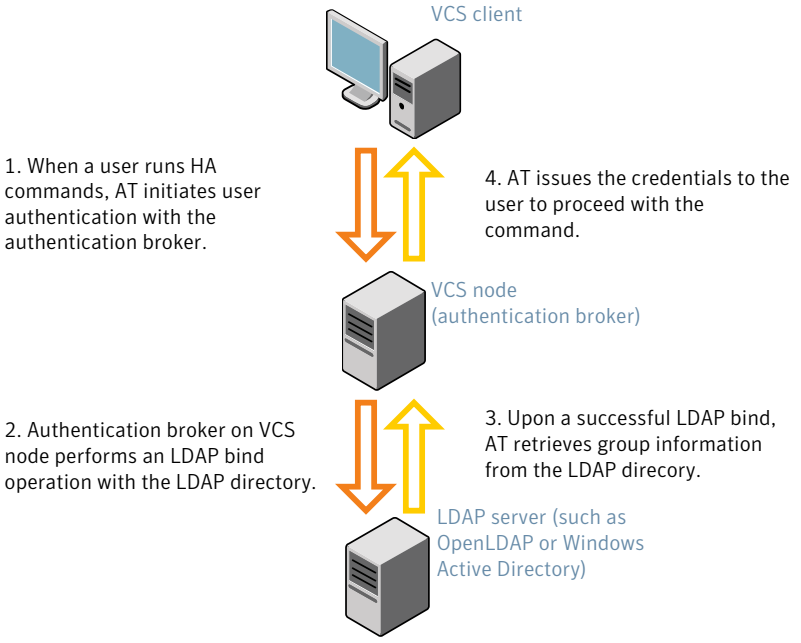
See "Enabling LDAP authentication for clusters that run in secure mode" on page 285.

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 23-1 depicts the VCS cluster communication with the LDAP servers when clusters run in secure mode.

Figure 23-1 Client communication with LDAP servers



See the *Symantec Product Authentication Service Administrator's Guide.*

The LDAP schema and syntax for LDAP commands (such as, ldapadd, ldapmodify, and ldapsearch) vary based on your LDAP implementation.

Before adding the LDAP domain in Symantec Product Authentication Service, note the following information about your LDAP environment:

- The type of LDAP schema used (the default is RFC 2307)
  - UserObjectClass (the default is posixAccount)
  - UserObject Attribute (the default is uid)
  - User Group Attribute (the default is gidNumber)
  - Group Object Class (the default is posixGroup)
  - GroupObject Attribute (the default is cn)
  - Group GID Attribute (the default is gidNumber)
  - Group Membership Attribute (the default is memberUid)
- URL to the LDAP Directory

- Distinguished name for the user container (for example, UserBaseDN=ou=people,dc=comp,dc=com)
- Distinguished name for the group container (for example, GroupBaseDN=ou=group,dc=comp,dc=com)

Enabling LDAP authentication for clusters that run in secure mode

The following procedure shows how to enable the plug-in module for LDAP authentication. This section provides examples for OpenLDAP and Windows Active Directory LDAP distributions.

Before you enable the LDAP authentication, complete the following steps:

- Make sure that the cluster runs in secure mode.

```
# haclus -value SecureClus
```

  The output must return the value as 1.

- Make sure that the AT version is 5.0.32.0 or later.

```
# /opt/VRTSat/bin/vssat showversion
vssat version: 5.0.32.0
```

See the `vssat.1m` and the `atldapconf.1m` manual pages.

To enable OpenLDAP authentication for clusters that run in secure mode

1 Add the LDAP domain to the AT configuration using the `vssat` command.

The following example adds the LDAP domain, MYENTERPRISE:

```
# /opt/VRTSat/bin/vssat addldapdomain \
--domainname "MYENTERPRISE.symantecdomain.com"\
--server_url "ldap://my_openldap_host.symantecexample.com"\
--user_base_dn "ou=people,dc=symantecdomain,dc=myenterprise,dc=com"\
--user_attribute "cn" --user_object_class "account"\
--user_gid_attribute "gidNumber"\
--group_base_dn "ou=group,dc=symantecdomain,dc=myenterprise,dc=com"\
--group_attribute "cn" --group_object_class "posixGroup"\
--group_gid_attribute "member"\
--admin_user "cn=manager,dc=symantecdomain,dc=myenterprise,dc=com"\
--admin_user_password "password" --auth_type "FLAT"
```

2 Verify that you can successfully authenticate an LDAP user on the VCS nodes.

You must have a valid LDAP user ID and password to run the command. In the following example, authentication is verified for the MYENTERPRISE domain for the LDAP user, vcsadmin1.

```
galaxy# /opt/VRTSat/bin/vssat authenticate
--domain ldap:MYENTERPRISE.symantecdomain.com
--prplname vcsadmin1 --broker galaxy:2821

Enter password for vcsadmin1: ##########

authenticate
----------------------
----------------------

Authenticated User vcsadmin1
----------------------
```

3 Add the LDAP user to the main.cf file.

```
# haconf makerw
# hauser -add "CN=vcsadmin1/CN=people/\
DC=symantecdomain/DC=myenterprise/\
DC=com@myenterprise.symantecdomain.com" -priv Administrator
# haconf -dump -makero
```

If you want to enable group-level authentication, you must run the following command:

```
# hauser -addpriv \
ldap_group@ldap_domain AdministratorGroup
```

4 Verify that the main.cf file has the following lines:

```
# cat /etc/VRTSvcs/conf/config/main.cf
...
...
cluster clus1 (
  SecureClus = 1
  Administrators = {
    "CN=vcsadmin1/CN=people/DC=symantecdomain/DC=myenterprise/
    DC=com@myenterprise.symantecdomain.com" }
  AdministratorGroups = {
    "CN=symantecusergroups/DC=symantecdomain/DC=myenterprise/
    DC=com@myenterprise.symantecdomain.com " }
  )
...
...
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=myenterprise.symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh or ksh), run the following commands:

```
# export VCS_DOMAIN=myenterprise.symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
galaxy     Attribute  RUNNING
nebula     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the VCS node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

To enable Windows Active Directory authentication for clusters that run in secure mode

1 Run the LDAP configuration tool atldapconf using the -d option. The -d option discovers and retrieves an LDAP properties file which is a prioritized attribute list.

```
# /opt/VRTSat/bin/atldapconf -d
-s domain_controller_name_or_ipaddress
-u domain_user -g domain_group
```

For example:

```
# /opt/VRTSat/bin/atldapconf -d -s 192.168.20.32 \
-u Administrator -g "Domain Admins"
Search User provided is invalid or Authentication is required to
proceed further.
Please provide authentication information for LDAP server.

Username/Common Name: symantecdomain\administrator
Password:

Attribute file created.
```

2 Run the LDAP configuration tool atldapconf using the -c option. The -c option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSat/bin/atldapconf -c -d windows_domain_name
```

For example:

```
# /opt/VRTSat/bin/atldapconf -c -d symantecdomain.com
Attribute list file not provided, using default AttributeList.txt.
CLI file name not provided, using default CLI.txt.

CLI for addldapdomain generated.
```

3 Run the LDAP configuration tool atldapconf using the -x option. The -x option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/VRTSat/bin/atldapconf -x
```

4 List the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSat/bin/vssat listldapdomains

Domain Name :          symantecdomain.com
Server URL :           ldap://192.168.20.32:389
SSL Enabled :          No
User Base DN :         CN=people,DC=symantecdomain,DC=com
User Object Class :    account
User Attribute :       cn
User GID Attribute :   gidNumber
Group Base DN :        CN=group,DC=symantecdomain,DC=com
Group Object Class :   group
Group Attribute :      cn
Group GID Attribute :  cn
Auth Type :            FLAT
Admin User :
Admin User Password :
Search Scope :         SUB
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh or ksh), run the following commands:

```
# export VCS_DOMAIN=symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
galaxy     Attribute  RUNNING
nebula     Attribute  RUNNING
```

Similarly, you can use the same LDAP user credentials to log on to the VCS node using the VCS Cluster Manager (Java Console).

7 To enable LDAP authentication on other nodes in the cluster, perform the procedure on each of the nodes in the cluster.

Accessing the VCS documentation

The software disc contains the documentation for VCS in Portable Document Format (PDF) in the cluster_server/docs directory. After you install VCS, Symantec recommends that you copy the PDF version of the documents to the /opt/VRTS/docs directory on each node to make it available for reference.

To access the VCS documentation

- Copy the PDF from the software disc (cluster_server/docs/) to the directory /opt/VRTS/docs.

Removing permissions for communication

Make sure you completed the installation of VCS and the verification of disk support for I/O fencing. If you used `remsh`, remove the temporary `remsh` access permissions that you set for the nodes and restore the connections to the public network.

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

Chapter 24

Installing or upgrading VCS components

This chapter includes the following topics:

Installing the Java Console

You can administer VCS using the VCS Java-based graphical user interface, Java Console. After VCS has been installed, install the Java Console on a Windows system or HP-UX system. Review the software requirements for Java Console.

The system from which you run the Java Console can be a system in the cluster or a remote workstation. A remote workstation enables each system in the cluster to be administered remotely.

Review the information about using the Java Console. For more information, refer to the *Veritas Cluster Server Administrator's Guide*.

Software requirements for the Java Console

Cluster Manager (Java Console) is supported on:

- HP-UX 11i v3 IA and PA - RISC
- Windows XP and Windows 2003

Note: Make sure that you are using an operating system version that supports JRE 1.5.

Hardware requirements for the Java Console

The minimum hardware requirements for the Java Console follow:

- Pentium II 300 megahertz
- 256 megabytes of RAM
- 800x600 display resolution
- 8-bit color depth of the monitor
- A graphics card that is capable of 2D images

Note: Symantec recommends using Pentium III, 400MHz, 256MB RAM, and 800x600 display resolution.

The version of the Java™ 2 Runtime Environment (JRE) requires 32 megabytes of RAM.

Symantec recommends using the following hardware:

- 48 megabytes of RAM
- 16-bit color mode
- The KDE and the KWM window managers that are used with displays set to local hosts

Installing the Java Console on HP-UX

Review the procedure to install the Java console. Before you begin with the procedure, ensure that you have the `gunzip` utility installed on your system.

To install Java console on HP-UX

1. Download the Java GUI utility from http://go.symantec.com/vcsm_download to a temporary directory.
2. Use SD-UX to install the VRTScscm depot. For example, from the disc:

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

   The `-s` option specifies the source.

Installing the Java Console on a Windows system

Review the procedure to install the Java console on a Windows system.

To install the Java Console on a Windows system

1. Download the Java GUI utility from http://go.symantec.com/vcsm_download to a temporary directory.
2. Extract the zipped file to a temporary folder.
3. From this extracted folder, double-click setup.exe.
4. The Veritas Cluster Manager Install Wizard guides you through the installation process.

Upgrading the Java Console

Use one of the following applicable procedures to upgrade Java Console.

To upgrade Java console on HP-UX

1. Log in as superuser on the node where you intend to install the depot.
2. Remove the GUI from the previous installation.
3. Install the VCS Java console.

   See "Installing the Java Console on HP-UX" on page 294.

To upgrade the Java Console on a Windows client

1. Stop Cluster Manager (Java Console) if it is running.
2. Remove Cluster Manager from the system.
   - From the Control Panel, double-click **Add/Remove Programs**
   - Select **Veritas Cluster Manager**.
   - Click **Add/Remove**.
   - Follow the uninstall wizard instructions.
3. Install the new Cluster Manager.

   See "Installing the Java Console on a Windows system" on page 295.

Installing VCS Simulator

You can administer VCS Simulator from the Java Console or from the command line. Review the software requirements for VCS Simulator.

Software requirements for VCS Simulator

VCS Simulator is supported on:

- Windows XP and Windows 2003

Note: Make sure that you are using an operating system version that supports JRE 1.5.

Installing VCS Simulator on Windows systems

This section describes the procedure to install VCS Simulator on Windows systems.

To install VCS Simulator on Windows systems

1. Download VCS Simulator from the following location to a temporary directory.

   http://www.symantec.com/business/cluster-server and click **Utilities**.
2. Extract the compressed files to another directory.
3. Navigate to the path of the Simulator installer file:

   \cluster_server\windows\VCSWindowsInstallers\Simulator
4. Double-click the installer file.
5. Read the information in the Welcome screen and click **Next**.
6. In the Destination Folders dialog box, click **Next** to accepted the suggested installation path or click **Change** to choose a different location.
7. In the Ready to Install the Program dialog box, click **Back** to make changes to your selections or click **Install** to proceed with the installation.
8. In the Installshield Wizard Completed dialog box, click **Finish**.

Reviewing the installation

VCS Simulator installs Cluster Manager (Java Console) and Simulator binaries on the system. The Simulator installation creates the following directories:

Directory	Content
attrpool	Information about attributes associated with VCS objects
bin	VCS Simulator binaries
default_clus	Files for the default cluster configuration

Directory	Content
sample_clus	A sample cluster configuration, which serves as a template for each new cluster configuration
templates	Various templates that are used by the Java Console
types	The types.cf files for all supported platforms
conf	Contains another directory called types. This directory contains assorted resource type definitions that are useful for the Simulator. The type definition files are present in platform-specific sub directories.

Additionally, VCS Simulator installs directories for various cluster configurations.

VCS Simulator creates a directory for every new simulated cluster and copies the contents of the sample_clus directory. Simulator also creates a log directory within each cluster directory for logs that are associated with the cluster.

Upgrading VCS Simulator

Use the following procedure to upgrade VCS Simulator.

To upgrade VCS Simulator on a Windows client

1. Stop all instances of VCS Simulator.
2. Stop VCS Simulator, if it is running.
3. Remove VCS Simulator from the system.
   - From the Control Panel, double-click **Add/Remove Programs**
   - Select **VCS Simulator**.
   - Click **Add/Remove**.
   - Follow the uninstall wizard instructions.
4. Install the new Simulator.

   See "Installing VCS Simulator on Windows systems" on page 296.

Upgrading the VCS agents

The installvcs program does not upgrade the VCS agents for DB2, Oracle, and Sybase. If previous versions of these agents are installed on your cluster, you must uninstall the previous version of the agents and manually install the new agent version.

The Veritas Cluster Server product installer includes the VCS agents for DB2, Oracle, and Sybase as a bundled package.

See the agent Installation and Configuration Guide for more information on the agent that you want to upgrade.

See *Veritas Cluster Server Release Notes* for supported versions of the agents.

Chapter 25

Verifying the VCS installation

This chapter includes the following topics:

About verifying the VCS installation

After you install and configure VCS, you can inspect the contents of the key VCS configuration files that you have installed and modified during the process. These files reflect the configuration that is based on the information you supplied. You can also run VCS commands to verify the status of LLT, GAB, and the cluster.

About the cluster UUID

You can verify the existence of the cluster UUID.

To verify the cluster UUID exists

- From the prompt, run a more command.

```
more /etc/vx/.uuids/clusuuid
```

Verifying the LLT, GAB, and VCS configuration files

Make sure that the LLT, GAB, and VCS configuration files contain the information you provided during VCS installation and configuration.

To verify the LLT, GAB, and VCS configuration files

1. Navigate to the location of the configuration files:
   - LLT
     `/etc/llthosts`
     `/etc/llttab`
   - GAB
     `/etc/gabtab`
   - VCS
     `/etc/VRTSvcs/conf/config/main.cf`
2. Verify the content of the configuration files.
   See "About the LLT and GAB configuration files" on page 393.
   See "About the VCS configuration files" on page 396.

Verifying LLT, GAB, and cluster operation

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

To verify LLT, GAB, and cluster operation

1. Log in to any node in the cluster as superuser.
2. Make sure that the PATH environment variable is set to run the VCS commands.
   See "Setting the PATH variable" on page 67.
3. Verify LLT operation.
   See "Verifying LLT" on page 301.
4. Verify GAB operation.
   See "Verifying GAB" on page 303.
5. Verify the cluster operation.
   See "Verifying the cluster" on page 304.

Verifying LLT

Use the `lltstat` command to verify that links are active for LLT. If LLT is configured correctly, this command shows all the nodes in the cluster. The command also returns information about the links for LLT for the node on which you typed the command.

Refer to the `lltstat(1M)` manual page for more information.

To verify LLT

1. Log in as superuser on the node galaxy.
2. Run the `lltstat` command on the node galaxy to view the status of LLT.

   ```
   lltstat -n
   ```

   The output on galaxy resembles:

   ```
   LLT node information:
       Node             State           Links
       *0 galaxy          OPEN           2
        1 nebula          OPEN           2
   ```

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

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

   ```
   LLT node information:
       Node                State    Links
      * 0 galaxy           OPEN        2
        1 nebula           OPEN        2
        2 saturn           OPEN        1
   ```

3. Log in as superuser on the node nebula.
4. Run the `lltstat` command on the node nebula to view the status of LLT.

   ```
   lltstat -n
   ```

   The output on nebula resembles:

   ```
   LLT node information:
       Node             State           Links
        0 galaxy          OPEN           2
       *1 nebula          OPEN           2
   ```

5 To view additional information about LLT, run the `lltstat -nvv` command on each node.

For example, run the following command on the node galaxy in a two-node cluster:

```
lltstat -nvv active
```

The output on galaxy resembles:

```
Node          State      Link    Status      Address
*0 galaxy      OPEN
                         lan1 UP     08:00:20:93:0E:34
                         lan2 UP     08:00:20:93:0E:38
1 nebula       OPEN
                         lan1 UP     08:00:20:8F:D1:F2
                         lan2 DOWN
```

The command reports the status on the two active nodes in the cluster, galaxy and nebula.

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

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

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

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

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

```
lltstat -p
```

The output resembles:

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

```
63    gab          0x1F
      opens:       0 2 3 4 5 6 7 8 9 10 11 ... 60 61 62 63
      connects:    0 1
```

Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information.

The ports indicate the following:

Port a
- Nodes have GAB communication.
- gen a36e0003 is a randomly generated number
- membership 01 indicates that nodes 0 and 1 are connected

Port b
- Indicates that the I/O fencing driver is connected to GAB port b.

  Note: Port b appears in the `gabconfig` command output only if you had configured I/O fencing after you configured VCS.
- gen a23da40d is a randomly generated number
- membership 01 indicates that nodes 0 and 1 are connected

Port h
- VCS is started.
- gen fd570002 is a randomly generated number
- membership 01 indicates that nodes 0 and 1 are both running VCS

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

To verify GAB

1 To verify that GAB operates, type the following command on each node:

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

2 Review the output of the command:

- If GAB operates, the following GAB port membership information is returned:
  For a cluster where I/O fencing is not configured:

```
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
Port h gen fd570002 membership 01
```

For a cluster where I/O fencing is configured:

```
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
Port b gen a23da40d membership 01
Port h gen fd570002 membership 01
```

Note that port b appears in the `gabconfig` command output only if you had configured I/O fencing. You can also use the `vxfenadm -d` command to verify the I/O fencing configuration.

- If GAB does not operate, the command does not return any GAB port membership information:

```
GAB Port Memberships
===================================
```

- If only one network is connected, the command returns the following GAB port membership information:

```
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
Port a gen a36e0003 jeopardy   ;1
Port h gen fd570002 membership 01
Port h gen fd570002 jeopardy   ;1
```

Verifying the cluster

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

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

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

To verify the cluster

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

```
hastatus -summary
```

The output resembles:

```
-- SYSTEM STATE
-- System               State                Frozen

A  galaxy               RUNNING               0
A  nebula               RUNNING               0

-- GROUP STATE
-- Group           System        Probed  AutoDisabled   State

B  ClusterService  galaxy         Y       N              ONLINE
B  ClusterService  nebula         Y       N              OFFLINE

B  VxSS            galaxy         Y       N              ONLINE
B  VxSS            nebula         Y       N              ONLINE
```

Note that the VxSS service group is displayed only if you have configured the cluster in secure mode.

2 Review the command output for the following information:

- The system state
  If the value of the system state is RUNNING, the cluster is successfully started.
- The ClusterService group state
  In the sample output, the group state lists the ClusterService group, which is ONLINE on galaxy and OFFLINE on nebula.

Verifying the cluster nodes

Verify the information of the cluster systems using the `hasys -display` command. The information for each node in the output should be similar.

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

Refer to the *Veritas Cluster Server Administrator's Guide* for information about the system attributes for VCS.

To verify the cluster nodes

- On one of the nodes, type the `hasys -display` command:

```
hasys -display
```

The example shows the output when the command is run on the node galaxy. The list continues with similar information for nebula (not shown) and any other nodes in the cluster.

```
#System    Attribute             Value

galaxy     AgentsStopped         0

galaxy     AvailableCapacity     100

galaxy     CPUBinding            BindTo None CPUNumber 0

galaxy     CPUThresholdLevel     Critical 90 Warning 80 Note 70
                                 Info 60

galaxy     CPUUsage              0

galaxy     CPUUsageMonitoring    Enabled 0 ActionThreshold 0
                                 ActionTimeLimit 0 Action NONE
                                 NotifyThreshold 0 NotifyTimeLimit 0

galaxy     Capacity              100

galaxy     ConfigBlockCount      141

galaxy     ConfigCheckSum        33975

galaxy     ConfigDiskState       CURRENT

galaxy     ConfigFile            /etc/VRTSvcs/conf/config

galaxy     ConfigInfoCnt         0

galaxy     ConfigModDate         Wed 14 Oct 2009 17:22:48

galaxy     ConnectorState        Down

galaxy     CurrentLimits

galaxy     DiskHbStatus

galaxy     DynamicLoad           0

galaxy     EngineRestarted       0

galaxy     EngineVersion         5.1.10.0

galaxy     FencingWeight         0
```

```
galaxy    Frozen                0
galaxy    GUIIPAddr
galaxy    HostUtilization       CPU 0 Swap 0
galaxy    LLTNodeId             0
galaxy    LicenseType           DEMO
galaxy    Limits
galaxy    LinkHbStatus
galaxy    LoadTimeCounter       0
galaxy    LoadTimeThreshold     600
galaxy    LoadWarningLevel      80
galaxy    NoAutoDisable         0
galaxy    NodeId                0
galaxy    OnGrpCnt              1
galaxy    ShutdownTimeout
galaxy    SourceFile            ./main.cf
galaxy    SwapThresholdLevel    Critical 90 Warning 80 Note 70
                                Info 60
galaxy    SysInfo               HP-UX:galaxy,U,B.11.31,ia64
galaxy    SysName               galaxy
galaxy    SysState              RUNNING
galaxy    SystemLocation
galaxy    SystemOwner
galaxy    TFrozen               0
galaxy    TRSE                  0
galaxy    UpDownState           Up
galaxy    UserInt               0
galaxy    UserStr
```

```
galaxy     VCSFeatures            DR

galaxy     VCSMode                VCS
```

Performing a postcheck on a node

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

See "About using the postcheck option" on page 308.

Note: This command option requires downtime for the node.

To run the postcheck command on a node

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

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

  The installer reports some errors or warnings if any of the following issues occur:

  - Any processes or drivers do not start
  - LLT is not configured
  - GAB ports are not started
  - Etc.

About using the postcheck option

You can use the installer's post-check to determine installation-related problems.

Note: This command option requires downtime for the node.

When you use the `postcheck` option, it returns the results of the following commands for VCS and SFCFS:

- `lltconfig (to check LLT's status)`
- `lltstat -nvv (to check LLT's status)`
- `gabconfig -a` (to check ports a, b, and h)
- `vxfenadm -d (to check fencing)`

- `/opt/VRTS/bin/hasys -state` (to check systems' states)
- `/opt/VRTS/bin/hagrp -state` (to check service groups' states)
- `/opt/VRTS/bin/hares -state` (to check resources' states)

See "Performing a postcheck on a node" on page 308.

Section 9

Uninstalling VCS

Chapter 26

Uninstalling VCS using the installer

This chapter includes the following topics:

Preparing to uninstall VCS

Review the following prerequisites before you uninstall VCS:

- Before you remove VCS from any node in the cluster, shut down the applications that depend on VCS. For example, applications such as Java Console or any high availability agents for VCS.
- Before you remove VCS from fewer than all nodes in a cluster, stop the service groups on the nodes from which you uninstall VCS. You must also reconfigure VCS on the remaining nodes.
  See "About adding and removing nodes" on page 331.
- If you have manually edited any of the VCS configuration files, you need to reformat them.
  See "Reformatting VCS configuration files on a stopped cluster" on page 70.
- If you enabled AMF, stop the AMF driver.
  See "Stopping the AMF driver" on page 314.

Stopping the AMF driver

If the AMF driver is loaded, stop the driver before you run the uninstallation program. Check the setting of the `AMF_START` and `AMF_STOP` attributes in the `/etc/rc.config.d/amf` file to determine if the driver is loaded. The driver is loaded if the `AMF_START` is set to 1.

To stop the AMF driver

1. Update the `AMF_START` and `AMF_STOP` settings in the `/etc/rc.config.d/amf` file as follows:

```
AMF_START=0
AMF_STOP=1
```

2. Stop the AMF driver:

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

Uninstalling VCS using the script-based installer

You must meet the following conditions to use the uninstallvcs program to uninstall VCS on all nodes in the cluster at one time:

- Make sure that the communication exists between systems. By default, the uninstaller uses ssh.
- Make sure you can execute `ssh` or `remsh` commands as superuser on all nodes in the cluster.
- Make sure that the `ssh` or `remsh` is configured to operate without requests for passwords or passphrases.

If you cannot meet the prerequisites, then you must run the uninstallvcs program on each node in the cluster.

The uninstallvcs program removes all VCS depots.

The example demonstrates how to uninstall VCS using the uninstallvcs program. The uninstallvcs program uninstalls VCS on two nodes: galaxy nebula. The example procedure uninstalls VCS from all nodes in the cluster.

Removing VCS 5.1SP1 depots

The program stops the VCS processes that are currently running during the uninstallation process.

To uninstall VCS

1 Log in as superuser from the node where you want to uninstall VCS.

2 Start uninstallvcs program.

```
# cd /opt/VRTS/install
# ./uninstallvcs
```

The program specifies the directory where the logs are created. The program displays a copyright notice and a description of the cluster:

3 Enter the names of the systems from which you want to uninstall VCS.

The program performs system verification checks and asks to stop all running VCS processes.

4 Enter **y** to stop all the VCS processes.

The program stops the VCS processes and proceeds with uninstalling the software.

5 Review the output as the uninstallvcs program continues to do the following:

- Verifies the communication between systems
- Checks the installations on each system to determine the depots to be uninstalled.

6 Review the output as the uninstaller stops processes, unloads kernel modules, and removes the depots.

7 Note the location of summary, response, and log files that the uninstaller creates after removing all the depots.

Running uninstallvcs from the VCS 5.1SP1 disc

You may need to use the uninstallvcs program on the VCS 5.1 SP1 disc in one of the following cases:

- You need to uninstall VCS after an incomplete installation.
- The uninstallvcs program is not available in /opt/VRTS/install.

If you mounted the installation media to /mnt, access the uninstallvcs program by changing directory to:

```
cd /mnt/cluster_server/ ./ uninstallvcs
```

Uninstalling VCS with the Veritas Web-based installer

This section describes how to uninstall with the Veritas Web-based installer.

To uninstall VCS

1. Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.
2. In an HA configuration, stop VCS processes on either the local system or all systems.

   To stop VCS processes on the local system:

   ```
   # hastop -local
   ```

   To stop VCS processes on all systems:

   ```
   # hastop -all
   ```

3. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 168.
4. On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.
5. Select **Veritas Cluster Server** from the Product drop-down list, and click **Next**.
6. Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Validate**.
7. After the validation completes successfully, click **Next** to uninstall VCS on the selected system.
8. If there are any processes running on the target system, the installer stops the processes. Click **Next**.
9. After the installer stops the processes, the installer removes the products from the specified system.

   Click **Next**.
10. After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.
11. Click **Finish**.

    The Web-based installer prompts you for another task.

Removing the CP server configuration using the removal script

This section describes how to remove the CP server configuration from a node or cluster hosting the CP server.

Warning: Ensure that no VCS cluster is using the CP server that will have its CP server configuration removed.

A configuration utility that is part of VRTScps package is used to remove the CP server configuration. When using the configuration utility, a configuration removal script is run and the following tasks are performed:

- All CP server configuration files are removed
- The VCS configuration for CP server is removed

After running the utility and script, you can then uninstall VCS from the node or cluster.

Note: The configuration script has to run only once per CP server (which can be on a single node or SFHA cluster), when removing the CP server configuration.

The configuration utility performs the following steps to remove the CP server configuration:

- Takes the the CP server service group (CPSSG) offline, if it is online
- Removes the CPSSG service group from the VCS configuration

The following procedure describes how to remove the CP server configuration.

To remove the CP server configuration

1 To run the configuration removal script, enter the following command on the node where you want to remove the CP server configuration:

```
root@mycps1.symantecexample.com # /opt/VRTScps/bin/configure_cps.pl
```

2 The Veritas Coordination Point Server Configuration utility appears with an option menu.

```
VERITAS COORDINATION POINT SERVER CONFIGURATION UTILITY
=======================================================

Select one of the following:

[1] Configure Coordination Point Server on single node VCS system

[2] Configure Coordination Point Server on SFHA cluster

[3] Unconfigure Coordination Point Server
```

3 Select option 3 to unconfigure the Coordination Point Server.

4 A warning appears and prompts you to confirm the action to unconfigure the Coordination Point Server.

Enter "y" to proceed.

```
WARNING: Unconfiguring Coordination Point Server stops the
vxcpserv process. VCS clusters using this server for
coordination purpose will have one less coordination point.

Are you sure you want to bring down the cp server? (y/n)
(Default:n) :y
```

5 After entering "y" to proceed, messages appear informing you of the progress in removing the CP server configuration.

When the CP server configuration has been unconfigured, a success message appears.

For an example of the messages from a single node VCS cluster:

```
A single node VCS cluster is currently configured.
Stopping the CP server ...

Removing the CP Server from VCS configuration..

Removing resource dependencies...
Deleting the resources configured under CPSSG service group...
Deleting the CPSSG service group...

Successfully unconfigured the Veritas Coordination Point Server.
```

For an example of the messages from a CP server on an SFHA cluster:

```
A multinode CP Server cluster is currently configured.
Stopping the CP server ...

Removing the CP Server from VCS configuration..

Removing resource dependencies...
Deleting the resources configured under CPSSG service group...
Deleting the CPSSG service group...

Successfully unconfigured the Veritas Coordination Point Server.
```

6 You are then prompted to delete the CP server database. Enter "y" to delete the database. For example:

```
Do you want to delete the CP Server database? (y/n) (Default:n) :
```

7 Enter "y" at the prompt to confirm the deletion of the CP server database.

```
Warning: This database won't be available if CP server
is reconfigured on the cluster. Are you sure you want to
proceed with the deletion of database? (y/n) (Default:n) :
```

8 Enter "y" to delete the CP server configuration file and log files. For example:

```
Do you want to delete the CP Server configuration file
(/etc/vxcps.conf) and log files (in /var/VRTScps)? (y/n)
(Default:n) : y
```

9 Run the `hagrp -state` command to ensure that the CPSSG service group has been removed from the node. For example:

```
root@mycps1.symantecexample.com # hagrp -state CPSSG

VCS WARNING V-16-1-40131 Group CPSSG does not exist
in the local cluster
```

Chapter 27

Uninstalling VCS using response files

This chapter includes the following topics:

Uninstalling VCS using response files

Typically, you can use the response file that the installer generates after you perform VCS uninstallation on one cluster to uninstall VCS on other clusters.

To perform an automated uninstallation

1. Make sure that you meet the prerequisites to uninstall VCS.
2. Copy the response file to one of the cluster systems where you want to uninstall VCS.

   See "Sample response file for uninstalling VCS" on page 323.
3. Edit the values of the response file variables as necessary.

   See "Response file variables to uninstall VCS" on page 322.
4. Start the uninstallation from the system to which you copied the response file. For example:

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

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

Response file variables to uninstall VCS

Table 27-1 lists the response file variables that you can define to uninstall VCS.

Table 27-1 Response file variables specific to uninstalling VCS

Variable	List or Scalar	Description
CFG{opt}{uninstall}	Scalar	Uninstalls VCS depots. (Required)
CFG{systems}	List	List of systems on which the product is to be uninstalled. (Required)
CFG{prod}	Scalar	Defines the product to be uninstalled. The value is VCS51 for VCS. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *remsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for uninstalling VCS

Review the response file variables and their definitions.

See "Response file variables to uninstall VCS" on page 322.

```
#
# Configuration Values:
#
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="VCS51";
$CFG{systems}=[ qw(galaxy nebula) ];
1;
```

Chapter 28

Manually uninstalling VCS

This chapter includes the following topics:

Removing VCS depots manually

You must remove the VCS depots from each node in the cluster to uninstall VCS.

To manually remove VCS depots on a node

1 Shut down VCS on the local system using the `hastop` command.

```
# hastop -local
```

2 Unconfigure the fencing, GAB, LLT, and AMF modules.

```
# /sbin/gabconfig -U
# /sbin/lltconfig -Uo
# /sbin/vxfenconfig -U
# /opt/VRTSamf/bin/amfconfig -U
```

3 If you installed VRTSvxfen, then:

```
# kcmodule vxfen=unused
```

4 Unload the GAB driver:

```
# kcmodule gab=unused
```

5 Unload the LLT driver:

```
# kcmodule llt=unused
```

6 Remove the VCS 5.1 SP1 depots in the following order:

```
# swremove VRTScmccc VRTScmcs VRTScssim VRTScscw  VRTSweb
VRTScscm VRTSjre15 VRTSjre VRTSvcsdc VRTSvcsmn VRTSvcsmg
VRTSvcsag VRTSacclib VRTSvcs VRTSamf VRTSvxfen VRTSgab
VRTSllt SYMClma VRTSspt VRTSat VRTSsmf VRTSpbx VRTSicsco
VRTSperl VRTSvlic
```

Manually remove the CP server fencing configuration

The following procedure describes how to manually remove the CP server fencing configuration from the CP server. This procedure is performed as part of the process to stop and remove server-based IO fencing.

Note: This procedure must be performed after the VCS cluster has been stopped, but before the VCS cluster software is uninstalled.

This procedure is required so that the CP server database can be reused in the future for configuring server-based fencing on the same VCS cluster(s).

Perform the steps in the following procedure to manually remove the CP server fencing configuration.

Note: The `cpsadm` command is used in the following procedure. For detailed information about the `cpsadm` command, see the *Veritas Cluster Server Administrator's Guide*.

To manually remove the CP server fencing configuration

1 Unregister all VCS cluster nodes from all CP servers using the following command:

```
# cpsadm -s cp_server -a unreg_node -u uuid -n nodeid
```

2 Remove the VCS cluster from all CP servers using the following command:

```
# cpsadm -s cp_server -a rm_clus -u uuid
```

3 Remove all the VCS cluster users communicating to CP servers from all the CP servers using the following command:

```
# cpsadm -s cp_server -a rm_user -e user_name -g domain_type
```

4 Proceed to uninstall the VCS cluster software.

Section 10

Adding and removing nodes

Chapter 29

Adding and removing cluster nodes

This chapter includes the following topics:

About adding and removing nodes

After you install VCS and create a cluster, you can add and remove nodes from the cluster. You can create a cluster of up to 64 nodes.

VCS is capable of supporting clusters with up to 64 nodes. Symantec has tested and qualified VCS configurations of up to 32 nodes at the time of the release. For more updates on this support, see the Late-Breaking News TechNote.

See "Important preinstallation information for VCS" on page 33.

Adding nodes using the VCS installer

The VCS installer performs the following tasks:

- Verifies that the node and the existing cluster meet communication requirements.
- Verifies the products and packages installed on the new node.

- Discovers the network interfaces on the new node and checks the interface settings.
- Creates the following files on the new node:

  `/etc/llttab`

  `/etc/VRTSvcs/conf/sysname`
- Updates the following configuration files and copies them on the new node:

  `/etc/llthosts`

  `/etc/gabtab`

  `/etc/VRTSvcs/conf/config/main.cf`
- Copies the following files from the existing cluster to the new node
  /etc/vxfenmode
  /etc/vxfendg
  /etc/vx/.uuids/clusuuid
- Configures security on the new node if the existing cluster is a secure cluster.

  Warning: If the root broker system has failed, then you must recover or reconfigure the root broker system before you add a new node to the cluster.

  See "Adding a node to the secure cluster whose root broker system has failed" on page 440.
- Configures disk-based or server-based fencing depending on the fencing mode in use on the existing cluster.

At the end of the process, the new node joins the VCS cluster.

Note: If you have configured server-based fencing on the existing cluster, make sure that the CP server does not contain entries for the new node. If the CP server already contains entries for the new node, remove these entries before adding the node to the cluster, otherwise the process may fail with an error.

To add the node to an existing VCS cluster using the VCS installer

1. Log in as the root user on one of the nodes of the existing cluster.
2. Run the VCS installer with the -addnode option.

   ```
   # cd /opt/VRTS/install

   # ./installvcs -addnode
   ```

   The installer displays the copyright message and the location where it stores the temporary installation logs.
3. Enter the name of a node in the existing VCS cluster. The installer uses the node information to identify the existing cluster.

   ```
   Enter a node name in the VCS cluster to which
   you want to add a node: galaxy
   ```

4. Review and confirm the cluster information.
5. Enter the name of the systems that you want to add as new nodes to the cluster.

   ```
   Enter the system names separated by spaces
   to add to the cluster: saturn
   ```

   The installer checks the installed products and packages on the nodes and discovers the network interfaces.
6. Enter the name of the network interface that you want to configure as the first private heartbeat link.

   Note: The LLT configuration for the new node must be the same as that of the existing cluster. If your existing cluster uses LLT over UDP, the installer asks questions related to LLT over UDP for the new node.

   See "Configuring private heartbeat links" on page 124.

   ```
   Enter the NIC for the first private heartbeat
   link on saturn: [b,q,?] lan1
   ```

7 Enter **y** to configure a second private heartbeat link.

Note: At least two private heartbeat links must be configured for high availability of the cluster.

```
Would you like to configure a second private
heartbeat link? [y,n,q,b,?] (y)
```

8 Enter the name of the network interface that you want to configure as the second private heartbeat link.

```
Enter the NIC for the second private heartbeat link
on saturn: [b,q,?] lan2
```

9 Depending on the number of LLT links configured in the existing cluster, configure additional private heartbeat links for the new node.

The installer verifies the network interface settings and displays the information.

10 Review and confirm the information.

11 If you have configured SMTP, SNMP, or the global cluster option in the existing cluster, you are prompted for the NIC information for the new node.

```
Enter the NIC for VCS to use on saturn: lan3
```

12 If the existing cluster uses server-based fencing in secure mode, provide responses to the following installer prompts.

If you are using different root brokers for the CP server and the client VCS cluster, enter **y** to confirm the use of different root brokers. The installer attempts to establish trust between the new node being added to the cluster and the authentication broker of the CP server.

```
Are you using different Root Brokers for the CP Server(s) and the
client cluster? (If so then installer will try to establish trust
between the new node(s) being added and CP Server's
Authentication Broker) [y,n,q] (n) y
```

Enter the host name of the authentication broker used for any one of the CP servers.

```
Enter hostname of the Authentication Broker being used for any one
of the CP Server(s): [b] mycps1.symantecexample.com
```

Enter the port number where the authentication broker for the CP server listens to establish trust with the new node:

```
Enter the port where the Authentication Broker
mycps1.symantecexample.com for the CP Server(s) is listening
for establishing trust: [b] (2821)
```

Adding a node using the Web-based installer

You can use the Web-based installer to add a node to a cluster.

To add a node to a cluster using the Web-based installer

1. From the Task pull-down menu, select **Add a Cluster** node.

   From the product pull-down menu, select the product.

   Click the **Next** button.

2. In the System Names field enter a name of a node in the cluster where you plan to add the node.

   The installer program checks inter-system communications and compatibility. If the node fails any of the checks, review the error and fix the issue.

   If prompted, review the cluster's name, ID, and its systems. Click the **Yes** button to proceed.

3. In the System Names field, enter the names of the systems that you want to add to the cluster as nodes. Separate system names with spaces. Click the **Validate** button to check if the system can work in the cluster.

   The installer program checks inter-system communications and compatibility. If the system fails any of the checks, review the error and fix the issue.

   Click the **Next** button. If prompted, click the **Yes** button to add the system and to proceed.

4. From the heartbeat NIC pull-down menus, select the heartbeat NICs for the cluster. Click the **Next** button.

5. Once the addition is complete, review the log files. Optionally send installation information to Symantec. Click the **Finish** button to complete the node's addition to the cluster.

Manually adding a node to a cluster

The system you add to the cluster must meet the hardware and software requirements.

See "Hardware requirements for VCS" on page 34.

Table 29-1 specifies the tasks that are involved in adding a cluster. The example demonstrates how to add a node saturn to already existing nodes, galaxy and nebula.

Table 29-1 Tasks that are involved in adding a node to a cluster

Task	Reference
Set up the hardware.	See "Setting up the hardware" on page 337.

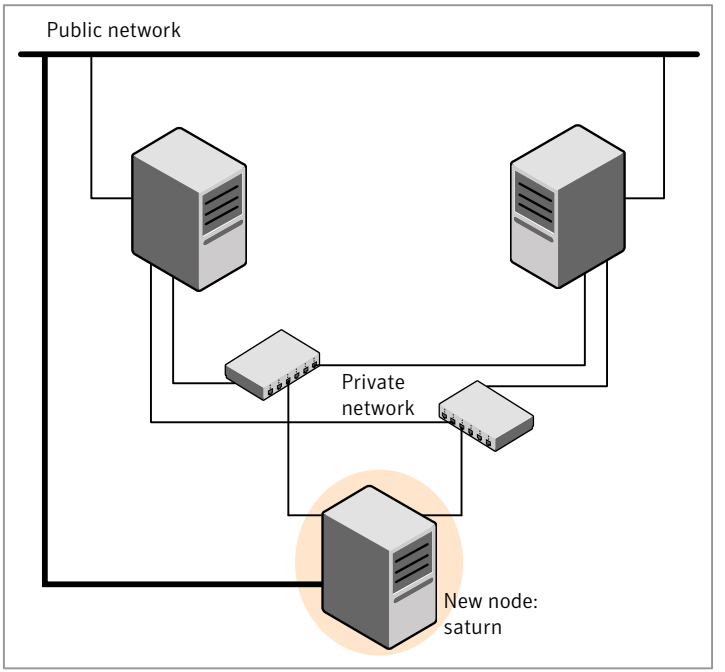
Table 29-1 Tasks that are involved in adding a node to a cluster *(continued)*

Task	Reference
Install the software manually.	See " Preparing for a manual installation" on page 211. See "Installing VCS depots for a manual installation" on page 215.
Add a license key.	See "Adding a license key for a manual installation" on page 216.
If the existing cluster runs in secure mode, set up the new node to run in secure mode.	See "Setting up the node to run in secure mode" on page 339.
Configure LLT and GAB.	See "Configuring LLT and GAB when adding a node to the cluster" on page 341.
If the existing cluster is configured for I/O fencing, configure I/O fencing on the new node.	See "Configuring I/O fencing on the new node" on page 344.
Add the node to the existing cluster.	See "Adding the node to the existing cluster" on page 348.
Start VCS and verify the cluster.	See "Starting VCS and verifying the cluster" on page 349.

Setting up the hardware

Figure 29-1 shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.

Figure 29-1 Adding a node to a two-node cluster using two switches



To set up the hardware

1 Connect the VCS private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a two-node cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a two-node cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 29-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Connect the system to the shared storage, if required.

Installing the VCS software manually when adding a node

Install the VCS 5.1SP1 depots manually and add a license key.

For more information, see the following:

- See "Adding a license key for a manual installation" on page 216.

Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

See "Configuring LLT and GAB when adding a node to the cluster" on page 341.

Table 29-2 uses the following information for the following command examples.

Table 29-2 The command examples definitions

Name	Fully-qualified host name (FQHN)	Function
saturn	saturn.nodes.example.com	The new node that you are adding to the cluster.
RB1	RB1.brokers.example.com	The root broker for the cluster
RB2	RB2.brokers.example.com	Another root broker, not the cluster's RB

To verify the existing security setup on the node

1. If node saturn is configured as an authentication broker (AB) belonging to a root broker, perform the following steps. Else, proceed to configuring the authentication broker on node saturn.

   See "Configuring the authentication broker on node saturn" on page 340.

2. Find out the root broker to which the node saturn belongs using the following command.

   ```
   # vssregctl -l -q -b \
   "Security\Authentication\Authentication Broker" \
    -k "BrokerName"
   ```

3. If the node saturn already belongs to root broker RB1, it is configured as part of the cluster. Proceed to setting up VCS related security configuration.

   See "Setting up VCS related security configuration" on page 341.

4. If the node saturn belongs to a different root broker (for example RB2), perform the following steps to remove the security credentials from node saturn.

- Kill /opt/VRTSat/bin/vxatd process.
- Remove the credential that RB2 has given to AB on node saturn.

```
# vssat deletecred --domain type:domainname \
--prplname prplname
```

For example:

```
# vssat deletecred --domain vx:root@RB2.brokers.example.com \
--prplname saturn.nodes.example.com
```

Configuring the authentication broker on node saturn

Configure a new authentication broker (AB) on node saturn. This AB belongs to root broker RB1.

To configure the authentication broker on node saturn

1. Create a principal for node saturn on root broker RB1. Execute the following command on root broker RB1.

```
# vssat addprpl --pdrtype root --domain domainname \
 --prplname prplname --password password \
 --prpltype service
```

For example:

```
# vssat addprpl --pdrtype root \
--domain root@RB1.brokers.example.com \
--prplname saturn.nodes.example.com \
--password flurbdicate --prpltype service
```

2. Ensure that there is no clock skew between the times on node saturn and RB1.
3. Copy the /opt/VRTSat/bin/root_hash file from RB1 to node saturn.

4 Configure AB on node saturn to talk to RB1.

```
# vxatd -o -a -n prplname -p password -x vx -y domainname -q \
rootbroker -z 2821 -h roothash_file_path
```

For example:

```
# vxatd -o -a -n saturn.nodes.example.com -p flurbdicate \
-x vx -y root@RB1.brokers.example.com -q RB1 \
-z 2821 -h roothash_file_path
```

5 Verify that AB is configured properly.

```
# vssat showbrokermode
```

The command should return 1, indicating the mode to be AB.

Setting up VCS related security configuration

Perform the following steps to configure VCS related security settings.

Setting up VCS related security configuration

1 Start /opt/VRTSat/bin/vxatd process.

2 Create HA_SERVICES domain for VCS.

```
# vssat createpd --pdrtype ab --domain HA_SERVICES
```

3 Add VCS and webserver principal to AB on node saturn.

```
# vssat addprpl --pdrtype ab --domain HA_SERVICES --prplname
webserver_VCS_prplname --password new_password --prpltype
service --can_proxy
```

4 Create /etc/VRTSvcs/conf/config/.secure file.

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

Configuring LLT and GAB when adding a node to the cluster

Create the LLT and GAB configuration files on the new node and update the files on the existing nodes.

To configure LLT when adding a node to the cluster

1 Create the file /etc/llthosts on the new node. You must also update it on each of the current nodes in the cluster.

For example, suppose you add saturn to a cluster consisting of galaxy and nebula:

- If the file on one of the existing nodes resembles:

```
0 galaxy
1 nebula
```

- Update the file for all nodes, including the new one, resembling:

```
0 galaxy
1 nebula
2 saturn
```

2 Create the file /etc/llttab on the new node, making sure that line beginning "`set-node`" specifies the new node.

The file /etc/llttab on an existing node can serve as a guide.

3 Copy the following file from one of the nodes in the existing cluster to the new node:

/etc/rc.config.d/lltconf

4 On the new system, run the command:

```
# /sbin/lltconfig -c
```

In a setup that uses LLT over UDP, new nodes automatically join the existing cluster if the new nodes and all the existing nodes in the cluster are not separated by a router. However, if you use LLT over UDP6 link with IPv6 address and if the new node and the existing nodes are separated by a router, then do the following:

- Edit the `/etc/llttab` file on each node to reflect the link information about the new node.
- Specify the IPv6 address for UDP link of the new node to all existing nodes. Run the following command on each existing node for each UDP link:

```
# /sbin/lltconfig -a set systemid device_tag address
```

To configure GAB when adding a node to the cluster

1 Create the file /etc/gabtab on the new system.

- If the /etc/gabtab file on the existing nodes resembles:

```
/sbin/gabconfig -c
```

The file on the new node should be the same. Symantec recommends that you use the `-c -n`*N* option, where *N* is the total number of cluster nodes.

- If the /etc/gabtab file on the existing nodes resembles:

  ```
  /sbin/gabconfig -c -n2
  ```

  The file on all nodes, including the new node, should change to reflect the change in the number of cluster nodes. For example, the new file on each node should resemble:

  ```
  /sbin/gabconfig -c -n3
  ```

  The `-n` flag indicates to VCS the number of nodes that must be ready to form a cluster before VCS starts.

2 Copy the following file from one of the nodes in the existing cluster to the new node:

  /etc/rc.config.d/gabconf

3 On the new node, to configure GAB run the command:

  ```
  # /sbin/gabconfig -c
  ```

To verify GAB

1 On the new node, run the command:

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

  The output should indicate that port a membership shows all nodes including the new node. The output should resemble:

  ```
  GAB Port Memberships
  ===================================
  Port a gen a3640003 membership 012
  ```

  See "Verifying GAB" on page 303.

2 Run the same command on the other nodes (galaxy and nebula) to verify that the port a membership includes the new node:

  ```
  # /sbin/gabconfig -a
  GAB Port Memberships
  ===================================
  Port a gen a3640003 membership 012
  Port h gen fd570002 membership 01
  Port h gen fd570002    visible ; 2
  ```

Configuring I/O fencing on the new node

If the existing cluster is configured for I/O fencing, perform the following tasks on the new node:

- Prepare to configure I/O fencing on the new node.
  See "Preparing to configure I/O fencing on the new node" on page 344.
- If the existing cluster runs server-based fencing, configure server-based fencing on the new node.
  See "Configuring server-based fencing on the new node" on page 345.
  If the existing cluster runs disk-based fencing, you need not perform any additional step. Skip to the next task. After you copy the I/O fencing files and start I/O fencing, disk-based fencing automatically comes up.
- Copy the I/O fencing files from an existing node to the new node and start I/O fencing on the new node.
  See "Starting I/O fencing on the new node" on page 348.

If the existing cluster is not configured for I/O fencing, perform the procedure to add the new node to the existing cluster.

See "Adding the node to the existing cluster" on page 348.

Preparing to configure I/O fencing on the new node

Perform the following tasks before you configure and start I/O fencing on the new node.

To prepare to configure I/O fencing on the new node

1. Determine whether the existing cluster runs disk-based or server-based fencing mechanism. On one of the nodes in the existing cluster, run the following command:

   ```
   # vxfenadm -d
   ```

   If the fencing mode in the output is SCSI3, then the cluster uses disk-based fencing.

   If the fencing mode in the output is CUSTOMIZED, then the cluster uses server-based fencing.

2. In the following cases, install and configure Veritas Volume Manager (VxVM) on the new node.
   - The existing cluster uses disk-based fencing.
   - The existing cluster uses server-based fencing with at least one coordinator disk.

You need not perform this step if the existing cluster uses server-based fencing with all coordination points as CP servers.

See the *Veritas Storage Foundation and High Availability Installation Guide* for installation instructions.

Configuring server-based fencing on the new node

This section describes the procedures to configure server-based fencing on a new node. Depending on whether server-based fencing is configured in secure or non-secure mode on the existing cluster, perform the tasks in one of the following procedures:

- Server-based fencing in non-secure mode:
  To configure server-based fencing in non-secure mode on the new node
- Server-based fencing in secure mode:
  To configure server-based fencing with security on the new node

To configure server-based fencing in non-secure mode on the new node

1. Log in to each CP server as the root user.
2. Update each CP server configuration with the new node information:

```
# cpsadm -s mycps1.symantecexample.com \
-a add_node -c clus1 -h saturn -n2

Node 2 (saturn) successfully added
```

3. Verify that the new node is added to the CP server configuration:

```
# cpsadm -s mycps1.symantecexample.com \
-a list_nodes
```

   The new node must be listed in the command output.

4. Add the VCS user cpsclient@saturn to each CP server:

```
# cpsadm -s mycps1.symantecexample.com \
-a add_user -e cpsclient@saturn \
-f cps_operator -g vx

User cpsclient@saturn successfully added
```

Perform the following procedure for a secure configuration.

To configure server-based fencing with security on the new node

1 As the root user, create the VCS user and the domain on the new node:

- Create a dummy configuration file /etc/VRTSvcs/conf/config/main.cf that resembles the following example:

```
# cat main.cf

include "types.cf"
cluster clus1 {
     SecureClus = 1
     }

system saturn {
    }
```

- Verify the dummy configuration file:

```
# cd /etc/VRTSvcs/conf/config

# /opt/VRTSvcs/bin/hacf -verify .
```

- Start VCS in one node mode on the new node:

```
# /opt/VRTSvcs/bin/hastart -onenode
```

2 Verify that the VCS user and the domain are created on the new node:

```
# /opt/VRTScps/bin/cpsat showcred | grep _HA_VCS_

# /opt/VRTScps/bin/cpsat listpd -t local | grep HA_SERVICES
```

3 Stop VCS if the VCS user and domain are created successfully on the new node:

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

4 If the root broker for the CP server and the new node are different, run the following command to establish trust between the authentication broker of the CP Server and the new node:

```
# /usr/bin/echo y | /opt/VRTScps/bin/cpsat setuptrust \
-b mycps1.symantecexample.com -s high
```

5 Log in to each CP server as the root user.

6 Update each CP server configuration with the new node information:

```
# cpsadm -s mycps1.symantecexample.com \
-a add_node -c clus1 -h saturn -n2

Node 2 (saturn) successfully added
```

7 Verify that the new node is added to the CP server configuration:

```
# cpsadm -s mycps1.symantecexample.com -a list_nodes
```

The new node must be listed in the output.

8 Add the VCS user _HA_VCS_saturn@HA_SERVICES@saturn.symantec.com to each CP server:

```
# cpsadm -s mycps1.symantecexample.com \
-a add_user -e _HA_VCS_ssaturn@HA_SERVICES@saturn.symantec.com \
-f cps_operator -g vx

User _HA_VCS_saturn@HA_SERVICES@saturn.symantec.com successfully added
```

Adding the new node to the vxfen service group

Perform the steps in the following procedure to add the new node to the vxfen service group.

To add the new node to the vxfen group using the CLI

1 On one of the nodes in the existing VCS cluster, set the cluster configuration to read-write mode:

```
# haconf -makerw
```

2 Add the node saturn to the existing vxfen group.

```
# hagrp -modify vxfen SystemList -add saturn 2
```

3 Save the configuration by running the following command from any node in the VCS cluster:

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

Starting I/O fencing on the new node

Copy the I/O fencing files from an existing node to the new node and start I/O fencing on the new node. This task starts I/O fencing based on the fencing mechanism that is configured in the existing cluster.

To start I/O fencing on the new node

1. Copy the following I/O fencing configuration files from one of the nodes in the existing cluster to the new node:
   - /etc/vxfenmode
   - /etc/vxfendg—This file is required only for disk-based fencing.
   - /etc/rc.config.d/vxfenconf
2. Start I/O fencing on the new node.

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

3. Run the GAB configuration command on the new node to verify that the port b membership is formed.

   ```
   # gabconfig -a
   ```

Adding the node to the existing cluster

Perform the tasks on one of the existing nodes in the cluster.

To add the new node to the existing cluster

1. Copy the cluster UUID from the one of the nodes in the existing cluster to the new node:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl -clus -copy -from_sys \
   node_name_in_running_cluster -to_sys new_sys1 ... new_sysn
   ```

   Where you are copying the cluster UUID from a node in the cluster (*node_name_in_running_cluster*) to systems from *new_sys1* through *new_sysn* that you want to join the cluster.
2. Copy the following file from one of the nodes in the existing cluster to the new node:

   /etc/rc.config.d/vcsconf
3. Enter the command:

   ```
   # haconf -makerw
   ```

4 Add the new system to the cluster:

```
# hasys -add saturn
```

5 Copy the main.cf file from an existing node to your new node:

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

6 Check the VCS configuration file. No error message and a return value of zero indicates that the syntax is legal.

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

7 If necessary, modify any new system attributes.

8 Enter the command:

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

Starting VCS and verifying the cluster

Start VCS after adding the new node to the cluster and verify the cluster.

To start VCS and verify the cluster

1 Start VCS on the newly added system:

```
# hastart
```

2 Run the GAB configuration command on each node to verify that port a and port h include the new node in the membership:

```
# /sbin/gabconfig -a
  GAB Port Memberships
  ===================================
  Port a gen a3640003 membership 012
  Port h gen fd570002 membership 012
```

If the cluster uses I/O fencing, then the GAB output also shows port b membership.

Removing a node from a cluster

Table 29-3 specifies the tasks that are involved in removing a node from a cluster. In the example procedure, the cluster consists of nodes galaxy, nebula, and saturn; node saturn is to leave the cluster.

Table 29-3 Tasks that are involved in removing a node

Task	Reference
■ Back up the configuration file. ■ Check the status of the nodes and the service groups.	See "Verifying the status of nodes and service groups" on page 350.
■ Switch or remove any VCS service groups on the node departing the cluster. ■ Delete the node from VCS configuration.	See "Deleting the departing node from VCS configuration" on page 351.
Modify the llthosts and gabtab files to reflect the change.	See "Modifying configuration files on each remaining node" on page 354.
If the existing cluster is configured to use server-based I/O fencing, remove the node configuration from the CP server.	See "Removing the node configuration from the CP server" on page 354.
For a cluster that is running in a secure mode, remove the security credentials from the leaving node.	See "Removing security credentials from the leaving node " on page 355.
On the node departing the cluster: ■ Modify startup scripts for LLT, GAB, and VCS to allow reboot of the node without affecting the cluster. ■ Unconfigure and unload the LLT and GAB utilities. ■ Remove the VCS depots.	See "Unloading LLT and GAB and removing VCS on the departing node" on page 356.

Verifying the status of nodes and service groups

Start by issuing the following commands from one of the nodes to remain, node galaxy or node nebula.

To verify the status of the nodes and the service groups

1 Make a backup copy of the current configuration file, main.cf.

```
# cp -p /etc/VRTSvcs/conf/config/main.cf\
/etc/VRTSvcs/conf/config/main.cf.goodcopy
```

2 Check the status of the systems and the service groups.

```
# hastatus -summary

-- SYSTEM STATE
-- System      State          Frozen
A  galaxy      RUNNING        0
A  nebula      RUNNING        0
A  saturn      RUNNING        0

-- GROUP STATE
-- Group    System      Probed   AutoDisabled   State
B  grp1     galaxy      Y        N              ONLINE
B  grp1     nebula      Y        N              OFFLINE
B  grp2     galaxy      Y        N              ONLINE
B  grp3     nebula      Y        N              OFFLINE
B  grp3     saturn      Y        N              ONLINE
B  grp4     saturn      Y        N              ONLINE
```

The example output from the `hastatus` command shows that nodes galaxy, nebula, and saturn are the nodes in the cluster. Also, service group grp3 is configured to run on node nebula and node saturn, the departing node. Service group grp4 runs only on node saturn. Service groups grp1 and grp2 do not run on node saturn.

Deleting the departing node from VCS configuration

Before you remove a node from the cluster you need to identify the service groups that run on the node.

You then need to perform the following actions:

- Remove the service groups that other service groups depend on, or
- Switch the service groups to another node that other service groups depend on.

To remove or switch service groups from the departing node

1 Switch failover service groups from the departing node. You can switch grp3 from node saturn to node nebula.

```
# hagrp -switch grp3 -to nebula
```

2 Check for any dependencies involving any service groups that run on the departing node; for example, grp4 runs only on the departing node.

```
# hagrp -dep
```

3 If the service group on the departing node requires other service groups—if it is a parent to service groups on other nodes—unlink the service groups.

```
# haconf -makerw
# hagrp -unlink grp4 grp1
```

These commands enable you to edit the configuration and to remove the requirement grp4 has for grp1.

4 Stop VCS on the departing node:

```
# hastop -sys saturn
```

5 Check the status again. The state of the departing node should be EXITED. Make sure that any service group that you want to fail over is online on other nodes.

```
# hastatus -summary

    -- SYSTEM STATE
    -- System      State          Frozen
    A  galaxy      RUNNING        0
    A  nebula      RUNNING        0
    A  saturn      EXITED         0

    -- GROUP STATE
    -- Group    System      Probed   AutoDisabled   State
    B  grp1     galaxy      Y        N              ONLINE
    B  grp1     nebula      Y        N              OFFLINE
    B  grp2     galaxy      Y        N              ONLINE
    B  grp3     nebula      Y        N              ONLINE
    B  grp3     saturn      Y        Y              OFFLINE
    B  grp4     saturn      Y        N              OFFLINE
```

6 Delete the departing node from the SystemList of service groups grp3 and grp4.

```
# hagrp -modify grp3 SystemList -delete saturn
# hagrp -modify grp4 SystemList -delete saturn
```

7 For the service groups that run only on the departing node, delete the resources from the group before you delete the group.

```
# hagrp -resources grp4
    processx_grp4
    processy_grp4
# hares -delete processx_grp4
# hares -delete processy_grp4
```

8 Delete the service group that is configured to run on the departing node.

```
# hagrp -delete grp4
```

9 Check the status.

```
# hastatus -summary
    -- SYSTEM STATE
    -- System      State          Frozen
    A  galaxy      RUNNING        0
    A  nebula      RUNNING        0
    A  saturn      EXITED         0

    -- GROUP STATE
    -- Group    System      Probed   AutoDisabled   State
    B  grp1     galaxy      Y        N              ONLINE
    B  grp1     nebula      Y        N              OFFLINE
    B  grp2     galaxy      Y        N              ONLINE
    B  grp3     nebula      Y        N              ONLINE
```

10 Delete the node from the cluster.

```
# hasys -delete saturn
```

11 Save the configuration, making it read only.

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

Modifying configuration files on each remaining node

Perform the following tasks on each of the remaining nodes of the cluster.

To modify the configuration files on a remaining node

1 If necessary, modify the `/etc/gabtab` file.

No change is required to this file if the `/sbin/gabconfig` command has only the argument `-c`. Symantec recommends using the `-nN` option, where *N* is the number of cluster systems.

If the command has the form `/sbin/gabconfig -c -nN`, where *N* is the number of cluster systems, make sure that *N* is not greater than the actual number of nodes in the cluster. When *N* is greater than the number of nodes, GAB does not automatically seed.

Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`.

2 Modify the `/etc/llthosts` file on each remaining nodes to remove the entry of the departing node.

For example, change:

```
0 galaxy
1 nebula
2 saturn
```

To:

```
0 galaxy
1 nebula
```

Removing the node configuration from the CP server

After removing a node from a VCS cluster, perform the steps in the following procedure to remove that node's configuration from the CP server.

Note: The `cpsadm` command is used to perform the steps in this procedure. For detailed information about the `cpsadm` command, see the *Veritas Cluster Server Administrator's Guide*.

To remove the node configuration from the CP server

1. Log into the CP server as the root user.
2. View the list of VCS users on the CP server, using the following command:

   ```
   # cpsadm -s cp_server -a list_users
   ```

   Where *cp_server* is the virtual IP/ virtual hostname of the CP server.
3. Remove the VCS user associated with the node you previously removed from the cluster.

   For CP server in secure mode:

   ```
   # cpsadm -s cp_server -a rm_user \
   -e _HA_VCS_saturn@HA_SERVICES@saturn.nodes.example.com \
   -f cps_operator  -g vx
   ```

   For CP server in non-secure mode:

   ```
    # cpsadm -s cp_server  -a rm_user \
    -e cpsclient@saturn  -f cps_operator  -g vx
   ```
4. Remove the node entry from the CP server:

   ```
   # cpsadm -s cp_server -a rm_node  -h saturn -c clus1 -n 2
   ```
5. View the list of nodes on the CP server to ensure that the node entry was removed:

   ```
   # cpsadm -s cp_server -a list_nodes
   ```

Removing security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node saturn. Perform the following steps.

To remove the security credentials

1. Kill the `/opt/VRTSat/bin/vxatd` process.
2. Remove the root credentials on node saturn.

   ```
   # vssat deletecred --domain type:domainname --prplname prplname
   ```

Unloading LLT and GAB and removing VCS on the departing node

On the node departing the cluster, unconfigure and unload the LLT and GAB utilities, and remove the VCS depots.

See "Removing VCS depots manually" on page 325.

If you have configured VCS as part of the Storage Foundation and High Availability products, you may have to delete other dependent depots before you can delete all of the following ones.

Chapter 30

Adding a node to a single-node cluster

This chapter includes the following topics:

Adding a node to a single-node cluster

All nodes in the new cluster must run the same version of VCS. The example procedure refers to the existing single-node VCS node as Node A. The node that is to join Node A to form a multiple-node cluster is Node B.

Table 30-1 specifies the activities that you need to perform to add nodes to a single-node cluster.

Table 30-1 Tasks to add a node to a single-node cluster

Task	Reference
Set up Node B to be compatible with Node A.	See "Setting up a node to join the single-node cluster" on page 358.
■ Add Ethernet cards for private heartbeat network for Node B. ■ If necessary, add Ethernet cards for private heartbeat network for Node A. ■ Make the Ethernet cable connections between the two nodes.	See "Installing and configuring Ethernet cards for private network" on page 359.
Connect both nodes to shared storage.	See "Configuring the shared storage" on page 359.

Table 30-1 Tasks to add a node to a single-node cluster *(continued)*

Task	Reference
■ Bring up VCS on Node A. ■ Edit the configuration file.	See "Bringing up the existing node" on page 360.
If necessary, install VCS on Node B and add a license key. Make sure Node B is running the same version of VCS as the version on Node A.	See "Installing the VCS software manually when adding a node to a single node cluster" on page 360.
Edit the configuration files on Node B.	
Start LLT and GAB on Node B.	See "Starting LLT and GAB" on page 360.
■ Start LLT and GAB on Node A. ■ Restart VCS on Node A. ■ Modify service groups for two nodes.	See "Reconfiguring VCS on the existing node" on page 361.
■ Start VCS on Node B. ■ Verify the two-node cluster.	See "Verifying configuration on both nodes" on page 362.

Setting up a node to join the single-node cluster

The new node to join the existing single node that runs VCS must run the same operating system.

To set up a node to join the single-node cluster

1 Do one of the following tasks:

- If VCS is not currently running on Node B, proceed to step 2.
- If the node you plan to add as Node B is currently part of an existing cluster, remove the node from the cluster. After you remove the node from the cluster, remove the VCS depots and configuration files.
  See "Removing a node from a cluster" on page 350.
- If the node you plan to add as Node B is also currently a single VCS node, uninstall VCS.
- If you renamed the LLT and GAB startup files, remove them.

See "Renaming the LLT and GAB startup files" on page 414.

2 If necessary, install VxVM and VxFS.

See "Installing VxVM or VxFS if necessary" on page 359.

Installing VxVM or VxFS if necessary

If you have either VxVM or VxFS with the cluster option installed on the existing node, install the same version on the new node.

Refer to the appropriate documentation for VxVM and VxFS to verify the versions of the installed products. Make sure the same version runs on all nodes where you want to use shared storage.

Installing and configuring Ethernet cards for private network

Both nodes require Ethernet cards (NICs) that enable the private network. If both Node A and Node B have Ethernet cards installed, you can ignore this step.

For high availability, use two separate NICs on each node. The two NICs provide redundancy for heartbeating.

See "Setting up the private network" on page 60.

To install and configure Ethernet cards for private network

1 Shut down VCS on Node A.

```
# hastop -local
```

2 Install the Ethernet card on Node A.

If you want to use aggregated interface to set up private network, configure aggregated interface.

3 Install the Ethernet card on Node B.

If you want to use aggregated interface to set up private network, configure aggregated interface.

4 Configure the Ethernet card on both nodes.

5 Make the two Ethernet cable connections from Node A to Node B for the private networks.

Configuring the shared storage

Make the connection to shared storage from Node B. Configure VxVM on Node B and reboot the node when you are prompted.

See “Setting up shared storage” on page 63.

Bringing up the existing node

Bring up the node.

To bring up the node

1. Log in as superuser.
2. Make the VCS configuration writable.

   ```
   # haconf -makerw
   ```

3. Display the service groups currently configured.

   ```
   # hagrp -list
   ```

4. Freeze the service groups.

   ```
   # hagrp -freeze group -persistent
   ```

   Repeat this command for each service group in step 3.
5. Make the configuration read-only.

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

6. Stop VCS on Node A.

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

Installing the VCS software manually when adding a node to a single node cluster

Install the VCS 5.1SP1 depots manually and install the license key.

Refer to the following sections:

- See “ Preparing for a manual installation” on page 211.
- See “Adding a license key for a manual installation” on page 216.

Starting LLT and GAB

On the new node, start LLT and GAB.

To start LLT and GAB

1 Start LLT on Node B.

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

2 Start GAB on Node B.

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

Reconfiguring VCS on the existing node

Reconfigure VCS on the existing nodes.

To reconfigure VCS on existing nodes

1 On Node A, create the files /etc/llttab, /etc/llthosts, and /etc/gabtab. Use the files that are created on Node B as a guide, customizing the /etc/llttab for Node A.

2 Start LLT on Node A.

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

3 Start GAB on Node A.

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

4 Check the membership of the cluster.

```
# gabconfig -a
```

5 Copy the cluster UUID from the existing node to the new node:

```
# /opt/VRTSvcs/bin/uuidconfig.pl -clus -copy -from_sys \
node_name_in_running_cluster -to_sys new_sys1 ... new_sysn
```

Where you are copying the cluster UUID from a node in the cluster (*node_name_in_running_cluster*) to systems from *new_sys1* through *new_sysn* that you want to join the cluster.

6 Start VCS on Node A.

```
# hastart
```

7 Make the VCS configuration writable.

```
# haconf -makerw
```

8 Add Node B to the cluster.

```
# hasys -add sysB
```

9 Add Node B to the system list of each service group.

- List the service groups.

```
# hagrp -list
```

- For each service group that is listed, add the node.

```
# hagrp -modify group SystemList -add sysB 1
```

Verifying configuration on both nodes

Verify the configuration for the nodes.

To verify the nodes' configuration

1 On Node B, check the cluster membership.

```
# gabconfig -a
```

2 Start the VCS on Node B.

```
# hastart
```

3 Verify that VCS is up on both nodes.

```
# hastatus
```

4 List the service groups.

```
# hagrp -list
```

5 Unfreeze the service groups.

```
# hagrp -unfreeze group -persistent
```

6 Implement the new two-node configuration.

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

Section 11

Installation reference

Appendix A

VCS installation depots

This appendix includes the following topics:

- Veritas Cluster Server installation depots

Veritas Cluster Server installation depots

Table A-1 shows the depot name and contents for each Veritas Cluster Server depot.

Table A-1 Veritas Cluster Server depots

Depot	Contents	Required/Optional
VRTSamf	Contains the binaries for the Veritas Asynchronous Monitoring Framework kernel driver functionality for the process and mount based agents.	Required
VRTSat	Contains the binaries for Symantec Product Authentication Service. Installs Symantec Product Authentication Service, which provides authentication services for other Symantec products. VRTSat contains a server component and a client component. The server provides services for a root broker, authentication broker, or both. The client allows Symantec products to communicate with the brokers.	Required

Table A-1 Veritas Cluster Server depots *(continued)*

Depot	Contents	Required/Optional
VRTScps	Contains the binaries for the Veritas Coordination Point Server.	Optional. Required to Coordination Point Server (CPS). Depends on VRTSvxfen.
VRTSgab	Contains the binaries for Veritas Cluster Server group membership and atomic broadcast services.	Required Depends on VRTSllt.
VRTSllt	Contains the binaries for Veritas Cluster Server low-latency transport.	Required
VRTSperl	Contains Perl for Veritas.	Required
VRTSspt	Contains the binaries for Veritas Software Support Tools.	Recommended depot, optional
VRTSvcs	VRTSvcs 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.	Required Depends on VRTSperl, VRTSvlic, and VRTSgab.
VRTSvcsag	Contains the binaries for Veritas Cluster Server bundled agents.	Required Depends on VRTSvcs.
VRTSvcsea	VRTSvcsea contains the binaries for Veritas high availability agents for DB2, Sybase, and Oracle.	Optional for VCS. Required to use VCS with the high availability agents for DB2, Sybase, or Oracle.
VRTSvlic	Contains the binaries for Symantec License Utilities.	Required

Table A-1 Veritas Cluster Server depots *(continued)*

Depot	Contents	Required/Optional
VRTSvxfen	Contains the binaries for Veritas I/O Fencing .	Required to use fencing. Depends on VRTSgab.

Appendix B

Installation command options

This appendix includes the following topics:

Command options for installvcs program

The `installvcs` command usage takes the following form:

```
installvcs [ system1 system2 ... ]
 [ -configure | -install | -license | -precheck | -requirements | -start
              | -stop | -uninstall | -upgrade | -postcheck]
 [ -logpath log_path ]
 [ -responsefile response_file ]
 [ -tmppath tmp_path ]
 [ -hostfile hostfile_path ]

[ -keyfile ssh_key_file

[ -patchpath patch_path ]

[ -pkgpath pkg_path ]

[ -rsh | -redirect | -installminpkgs | -installrecpkgs | -installallpkgs
        | -minpkgs | -recpkgs | -allpkgs | -listpatches | -pkgset
        | -copyinstallscripts | -pkginfo | -serial | -comcleanup
        | -makeresponsefile | -pkgtable | -security | -addnode
        | -fencing | -upgrade_kernelpkgs | -upgrade_nonkernelpkgs
        | -ignorepatchreqs | -version | -nolic]
```

Table B-1 lists the `installvcs` command options.

Table B-1 installvcs options

Option and Syntax	Description
`-addnode`	Add the nodes that you specify to a cluster. The cluster must be online to use this command option to add nodes.
`-allpkgs`	View a list of all VCS depots and patches. The installvcs program lists the depots and patches in the correct installation order. You can use the output to create scripts for command-line installation, or for installations over a network. See the -minpkgs and the -recpkgs options.
`-comcleanup`	Remove the ssh or remsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or remsh are abruptly terminated.
`-configure`	Configure VCS after using `-install` option to install VCS.

Table B-1 installvcs options *(continued)*

Option and Syntax	Description
`-copyinstallscripts`	Use this option when you manually install products and want to use the installation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./installer -rootpath` *`alt_root_path`* `-copyinstallscripts` The path *alt_root_path* can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the *release_name* is UXRT51SP1.
`-fencing`	Configure I/O fencing after you configure VCS. The script provides an option to configure disk-based I/o fencing or server-based I/O fencing.
`-hostfile`	Specify the location of a file that contains the system names for the installer.
`-ignorepatchreqs`	Allow installation or upgrading even if the prerequisite depots or patches are missed on the system.
`-install`	Install product depots on systems without configuring VCS.
`-installallpkgs`	Select all the depots for installation. See the `-allpkgs` option.

Table B-1 installvcs options *(continued)*

Option and Syntax	Description
`-installminpkgs`	Select the minimum depots for installation. See the `-minpkgs` option.
`-installrecpkgs`	Select the recommended depots for installation. See the `-recpkgs` option.
`-keyfile` *`ssh_key_file`*	Specify a key file for SSH. The option passes `-i` *`ssh_key_file`* with each SSH invocation.
`-license`	Register or update product licenses on the specified systems. This option is useful to replace a demo license.
`-listpatches`	Display product patches in correct installation order.
`-logpath` *`log_path`*	Specify that log_path, not /opt/VRTS/install/logs, is the location where installvcs log files, summary file, and response file are saved.
`-makeresponsefile`	Generates a response file without performing an actual installation. Install, uninstall, start, and stop output are simulations. These actions are not performed on the system.
`-minpkgs`	View a list of the minimal depots and the patches that are required for VCS. The installvcs program lists the depots and patches in the correct installation order. The list does not include the optional depots. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -recpkgs options.
`-nolic`	Install product depots on systems without licensing or configuration. License-based features or variants are not installed when you use this option.
`-patchpath` *`patch_path`*	Specify that *patch_path* contains all patches that the installvcs program is about to install on all systems. The *patch_path* is the complete path of a directory. **Note:** You can use this option when you download recent versions of patches.

Table B-1 installvcs options *(continued)*

Option and Syntax	Description
`-pkginfo`	Display a list of depots in the order of installation in a user-friendly format. Use this option with one of the following options: ■ -allpkgs ■ -minpkgs ■ -recpkgs If you do not specify an option, all three lists of depots are displayed.
`-pkgpath` *pkg_path*	Specify that *pkg_path* contains all depots that the installvcs program is about to install on all systems. The *pkg_path* is the complete path of a directory, usually NFS mounted.
`-pkgset`	Discover and lists the 5.1 SP1 depots installed on the systems that you specify.
`-pkgtable`	Display the VCS 5.1 SP1 depots in the correct installation order.
`-postcheck`	Check for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.
`-precheck`	Verify that systems meet the installation requirements before proceeding with VCS installation. Symantec recommends doing a precheck before you install VCS. See "Performing automated preinstallation check" on page 70.
`-recpkgs`	View a list of the recommended depots and the patches that are required for VCS. The installvcs program lists the depots and patches in the correct installation order. The list does not include the optional depots. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -minpkgs options.
`-requirements`	View a list of required operating system version, required patches, file system space, and other system requirements to install VCS.

Table B-1 installvcs options *(continued)*

Option and Syntax	Description
`-responsefile` *`response_file`*	Perform automated VCS installation using the system and the configuration information that is stored in a specified file instead of prompting for information. The response file must be specified with the -responsefile option. If not specified, the response file is automatically generated as `installer`*`number`*`.response` where *number* is random. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. See "Installing VCS using response files" on page 181. See "Configuring VCS using response files" on page 187. See "Upgrading VCS using response files" on page 277.
`-redirect`	Specify that the installer need not display the progress bar details during the installation.
`-rsh`	Specify that *remsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *remsh* commands between systems execute without prompting for passwords or confirmations
`-security`	Enable or disable Symantec Product Authentication Service in a VCS cluster that is running. See the *Veritas Cluster Server Administrator's Guide* for instructions. See "About Symantec Product Authentication Service (AT)" on page 26.
`-serial`	Perform the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.

Table B-1 installvcs options *(continued)*

Option and Syntax	Description
`-start`	Start the daemons and processes for VCS. If the installvcs program failed to start up all the VCS processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -stop option. See "Starting and stopping processes for the Veritas products " on page 436.
`-stop`	Stop the daemons and processes for VCS. If the installvcs program failed to start up all the VCS processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -start option. See "Starting and stopping processes for the Veritas products " on page 436.
`-tmppath` *tmp_path*	Specify that *tmp_path* is the working directory for installvcs program. This path is different from the /var/tmp path. This destination is where the installvcs program performs the initial logging and where the installvcs program copies the depots on remote systems before installation.
`-uninstall`	Uninstall VCS from the systems that you specify.
`-upgrade`	Upgrade the installed depots on the systems that you specify.
`-upgrade_kernelpkgs`	Upgrade the product kernel depots to the latest version during rolling upgrade Phase-I.
`-upgrade_nonkernelpkgs`	Upgrade the VCS and other agent depots to the latest version during rolling upgrade Phase-II. Product kernel drivers are rolling-upgraded to the latest protocol version.
`-version`	Check and display the installed product and version. Identify the installed and missing depots and patches for the product. Provide a summary that includes the count of the installed and any missing depots and patches.

Command options for uninstallvcs program

The `uninstallvcs` command usage takes the following form:

```
uninstallvcs [ system1 system2 ... ]
 [ -logpath <log_path> ]
 [ -responsefile <response_file> ]
 [ -tmppath <tmp_path> ]
 [ -hostfile <hostfile_path> ]
 [ -keyfile <shh_key_file> ]

 [ -rsh | -redirect | -copyinstallscripts | -serial | -comcleanup
        |-makeresponsefile | -version | -nolic]
```

Table B-2 lists the `uninstallvcs` command options.

Table B-2 uninstallvcs options

Option and Syntax	Description
`-comcleanup`	Removes the ssh or remsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or remsh are abruptly terminated.

Table B-2 uninstallvcs options *(continued)*

Option and Syntax	Description
`-copyinstallscripts`	Use this option when you manually install products and want to use the installation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./installer -rootpath` *`alt_root_path`* `-copyinstallscripts` The path *alt_root_path* can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the *release_name* is UXRT51SP1.
`-hostfile`	Specifies the location of a file that contains the system names for the installer.
`-keyfile` *`ssh_key_file`*	Specifies a key file for SSH. The option passes `-i` *`ssh_key_file`* with each SSH invocation.
`-logpath` *`log_path`*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where installvcs log files, summary file, and response file are saved.
`-makeresponsefile`	Use this option to create a response file or to verify that your system configuration is ready for uninstalling VCS.
`-nolic`	Install product depots on systems without licensing or configuration. License-based features or variants are not installed when you use this option.

Table B-2 uninstallvcs options *(continued)*

Option and Syntax	Description
`-redirect`	Displays progress details without showing progress bar.
`-responsefile` *`response_file`*	Perform automated VCS uninstallation using the system and the configuration information that is stored in a specified file instead of prompting for information. The *response_file* must be a full path name. If not specified, the response file is automatically generated as `installer`*`number`*`.response` where *number* is random. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. See "Uninstalling VCS using response files" on page 321.
`-rsh`	Specifies that *remsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *remsh* commands between systems execute without prompting for passwords or confirmations
`-serial`	Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.
`-tmppath` *`tmp_path`*	Specifies that *tmp_path* is the working directory for uninstallvcs program. This path is different from the /var/tmp path. This destination is where the uninstallvcs program performs the initial logging and where the installvcs program copies the depots on remote systems before installation.
`-version`	Specifies the installed product and version. Identifies the installed and missing depots and patches for the product. Provides a summary that includes the count of the installed and any missing depots and patches.

Appendix C

Changes to bundled agents in VCS 5.1 SP1

This appendix includes the following topics:

Deprecated agents

The following agents are no longer supported:

- CampusCluster
- ClusterMonitorConfig
- Service group heartbeat (ServiceGroupHB)
- VRTSWebApp—VCS does not support the VRTSWebApp agent in this release.

New agents

The following new agents are in the 5.1 SP1 release:

- VolumeSet—Brings Veritas Volume Manager (VxVM) volume sets online and offline, and monitors them.

The following new agents were added in the 5.0.1 release:

- CoordPoint—Provides server-based I/O fencing.

The following new agents were added in the 5.0 release:

- Apache (now bundled on all platforms)—Provides high availability to an Apache Web server.
- NFSRestart—Provides high availability for NFS record locks.

Refer to the *Veritas Cluster Server Bundled Agents Reference Guide* for more information on these new agents.

New and modified attributes for 5.1 SP1 agents

Table C-1 lists the attributes that VCS adds or modifies when you upgrade from VCS 5.0.1 to VCS 5.1SP1.

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1

Agent	New and modified attributes	Default value
Apache		
Modified attribute		
	IntentionalOffline (change in attribute type from int to boolean)	static boolean IntentionalOffline = 0
Application		
New attributes		
	EnvFile	""
	UseSUDash	0
	IMFRegList[]	{ MonitorProcesses, User, PidFiles, MonitorProgram }
	RegList	{ MonitorProcesses, User, PidFiles, MonitorProgram }
Modified attribute		

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
	ArgList[] (new attributes added to list)	{ User, StartProgram, StopProgram, CleanProgram, MonitorProgram, PidFiles, MonitorProcesses, EnvFile, UseSUDash }
DNS		
Modified attributes		
	Alias (deleted attribute)	
	Hostname (deleted attribute)	
	ArgList[] (deleted attributes removed from list)	{ Domain, TTL, TSIGKeyFile, StealthMasters, ResRecord, CreatePTR, OffDelRR }
DiskGroup		
New attributes		
	Reservation	ClusterDefault
Modified attributes		
	StartVolumes (change in attribute type from str to boolean)	StartVolumes = 1
	StopVolumes (change in attribute type from str to boolean)	StopVolumes = 1
	UmountVolumes (change in attribute type from boolean to int)	UmountVolumes = 0

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
	ArgList[] (new attributes added to list)	{ DiskGroup, StartVolumes, StopVolumes, MonitorOnly, MonitorReservation, tempUseFence, PanicSystemOnDGLoss, UmountVolumes, Reservation }
IP		
New attributes		
	PrefixLen	0
	RouteOptions	""
Modified attribute		
	ArgList[] (new attributes added to list)	{"MultiNICResName:Device", Address, NetMask, "MultiNICResName:ArpDelay", Options, "MultiNICResName:Probed", MultiNICResName , IfconfigTwice, "MultiNICResName:Protocol", PrefixLen }
IPMultiNIC		
New attribute		
	PrefixLen	0
Modified attribute		

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
	ArgList[] (new attributes added to list)	{ "MultiNICResName:Device", Address, NetMask, "MultiNICResName:ArpDelay", Options, "MultiNICResName:Probed", MultiNICResName, IfconfigTwice, "MultiNICResName:Protocol", PrefixLen }
IPMultiNIB		
New attributes		
	PrefixLen	0
	RouteOptions	""
	Options	""
Modified attribute		
	ArgList[] (new attributes added to list)	{ BaseResName, Address, NetMask, DeviceChoice, "BaseResName:Protocol", PrefixLen, RouteOptions, Options }
Mount		
New attributes		
	OptCheck	0
	CreateMntPt	0
	ReuseMntPt	0
	MntPtPermission	""
	MntPtOwner	""
	MntPtGroup	""
	AccessPermissionChk	0

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
	RecursiveMnt	0
	IMFRegList[]	{MountPoint, BlockDevice, FSType }
Modified attribute		
	ArgList[] (new attributes added to list)	{ MountPoint, BlockDevice, FSType, MountOpt, FsckOpt, SnapUmount, CkptUmount, SecondLevelMonitor, SecondLevelTimeout, OptCheck, CreateMntPt, MntPtPermission, MntPtOwner, MntPtGroup, AccessPermissionChk, RecursiveMnt, VxFSMountLock, State }
MultiNICA		
New attributes		
	Protocol	"IPv4"
	PrefixLen	0
Modified attribute		
	ArgList[] (new attributes added to list)	{ Device, NetMask, ArpDelay, RetestInterval, Options, RouteOptions, PingOptimize, MonitorOnly, IfconfigTwice, HandshakeInterval, NetworkHosts, Protocol, PrefixLen }
MultiNICB		
New attribute		
	Protocol	"IPv4"
Modified attribute		

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
	DefaultRouter	""
	ArgList[] (new attributes added to list)	{ Device, NetworkHosts, LinkTestRatio, IgnoreLinkStatus, NetworkTimeout, OnlineTestRepeatCount, OfflineTestRepeatCount, NoBroadcast, DefaultRouter, Failback, Protocol }
NFSRestart		
New attributes		
	NFSLockFailover	0
	Lower	0
Modified attributes		
	NFSLockFailOver (deleted attribute)	
	ArgList[] (new attributes added to list)	{ "NFSRes:LockFileTimeout", "NFSRes:Nservers", "NFSRes:Version", LocksPathName, NFSLockFailover, Lower, State }
NIC		
New attribute		
	Protocol	"IPv4"
Modified attribute		
	ArgList[] (new attributes added to list)	{ Device, NetworkType, PingOptimize, NetworkHosts, Protocol }
NetBios		

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
New attribute		
	PidFile	""
Modified attribute		
	ArgList[] (new attributes added to list)	{ "SambaServerRes:ConfFile", "SambaServerRes:LockDir", NetBiosName, NetBiosAliases, Interfaces, WinsSupport, DomainMaster, "SambaServerRes:SambaTopDir", "SambaServerRes:PidFile", SambaServerRes, PidFile }
NotifierMngr		
New attribute		
	NotifierSourceIP	""
Modified attribute		
	ArgList[] (new attributes added to list)	{ EngineListeningPort, MessagesQueue, NotifierListeningPort, NotifierSourceIP, SnmpdTrapPort, SnmpCommunity, SnmpConsoles, SmtpServer, SmtpServerVrfyOff, SmtpServerTimeout, SmtpReturnPath, SmtpFromPath, SmtpRecipients }
RemoteGroup		
New attributes		
	ReturnIntOffline[]	{}
	OfflineMonitoringNode	""

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
	IntentionalOffline	1
Modified attribute		
	ArgList[] (new attributes added to list)	{ IpAddress, Port, Username, Password, GroupName, VCSSysName, ControlMode, OfflineWaitTime, DomainType, BrokerIp, ReturnIntOffline }
RVG (new agent)		
New attributes		
	NumThreads	1
	ArgList[]	{ RVG, DiskGroup }
	RVG	
	DiskGroup	
	StorageRVG	
	StorageDG	
	StorageHostIds	
RVGShared (new agent)		
New attributes		
	NumThreads	1
	ArgList[]	{ RVG, DiskGroup }
	RVG	
	DiskGroup	

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
RVGLogowner (new agent) New attributes		
	NumThreads	1
	ArgList[]	{ RVG, DiskGroup }
	OnlineRetryLimit	5
	RVG	
	DiskGroup	
	StorageRVG	
	StorageDG	
	StorageHostIds	
RVGPrimary (new agent)		
New attributes		
	SupportedActions	{ fbsync, ElectPrimary }
	NumThreads	1
	OnlineRetryLimit	1
	ArgList[]	{ RvgResourceName, AutoTakeover, AutoResync, BunkerSyncTimeOut, BunkerSyncElapsedTime }
	RvgResourceName	
	AutoTakeover	1
	AutoResync	0
	VCSResLock	""

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
SambaServer		
New attributes		
	SambaTopDir	""
	PidFile	""
	SocketAddress	""
Modified attribute		
	ArgList[]	{ ConfFile, LockDir, Ports, IndepthMonitorCyclePeriod, ResponseTimeout, SambaTopDir, PidFile, SocketAddress }
SambaShare		
Modified attribute		
	ArgList[]	{ "SambaServerRes:ConfFile", "SambaServerRes:LockDir", ShareName, ShareOptions, "SambaServerRes:Ports", SambaServerRes, "SambaServerRes:SambaTopDir", "SambaServerRes:PidFile", "SambaServerRes:SocketAddress" }
Share		
Modified attribute		
	ArgList[] (change in default value)	{ PathName, Options }
VRTSWebApp (deleted agent)		

Table C-1 New and modified attributes from VCS 5.0.1 to VCS 5.1 SP1 *(continued)*

Agent	New and modified attributes	Default value
VolumeSet (new agent)		
New attributes		
	DiskGroup	""
	VolumeSet	""
	ArgList[]	{ DiskGroup, VolumeSet }

Manually removing deprecated resource types and modifying attributes

With VCS 5.1, certain resource type definitions are no longer used. Before you start the upgrade process, you must remove the resources of the deprecated resource types from your cluster configuration.

If you use the resource type ServiceGroupHB, Symantec recommends the use of I/O fencing.

VCS 5.1 does not support gabdiskhb. So, the installvcs program removes the gabdiskhb entry from the /etc/gabtab file.

Note: Make sure you start VCS on the local node before starting on the other nodes. This standard ensures that HAD reads the configuration from the local node and updates it on the remaining nodes.

To remove the deprecated resource types and modify attributes

1 Save the VCS configuration and stop the VCS engine.

```
# haconf -dump -makero
# hastop -all -force
```

2 Back up the configuration file, main.cf to a location on the cluster node.

3 Edit the main.cf located under `/etc/VRTSvcs/conf/config`.

Perform the following instructions:

- Remove the resource of the deprecated resource types.
  You must modify the resource dependencies to ensure that the configuration works properly.
- Modify attribute values that might have changed.
- Save the main.cf.
- Reformat the main.cf file.

```
# hacf -cftocmd config
# hacf -cmdtocf config
```

4 Verify the configuration.

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

5 Start VCS on the local node.

6 Start VCS on other nodes.

Creating new VCS accounts if you used native operating system accounts

VCS has deprecated the AllowNativeCliUsers attribute. To use native OS accounts with VCS, use the halogin command. After you run the halogin command, VCS encrypts and stores your VCS credentials in your home directory for a specific time period. After you run the halogin command, you need not authenticate yourself every time you run a VCS command. In secure clusters, the command also sets up a trust relationship and retrieves a certificate from an authentication broker.

See the *Veritas Cluster Server Administrator's Guide* for information on assigning user privileges to OS user groups for clusters running in secure mode and clusters not running in secure mode.

Perform the following procedure if you used the AllowNativeCliUsers attribute. Ensure that each native user running VCS commands has a home directory on the system from which the user runs VCS commands.

To set up VCS authentication for clusters running in secure mode

1. Set the configuration (main.cf) mode to read/write.

   ```
   # haconf -makerw
   ```

2. Assign proper privileges to the OS users or user groups. Each operating system user must perform steps 3 and 4.
3. If the user executes VCS commands from a remote host, set the following environment variables:
   - VCS_HOST: Name of the VCS node on which you run commands. You may specify the virtual IP address associated with the cluster.
   - VCS_DOMAIN: Name of the VxSS domain to which the user belongs.
   - VCS_DOMAINTYPE: Type of VxSS domain: unixpwd, nt, nis, nisplus, or vx.
4. Run the halogin command:

   ```
   $ halogin vcsusername password
   ```

To set up VCS authentication for clusters not running in secure mode

1. Set the configuration (main.cf) mode to read/write.

   ```
   # haconf -makerw
   ```

2. Create VCS user accounts for all users and assign privileges to these users.
3. Each VCS user must run the halogin command:

   ```
   $ halogin vcsusername
     password
   ```

Appendix D

Configuration files

This appendix includes the following topics:

About the LLT and GAB configuration files

Low Latency Transport (LLT) and Group Membership and Atomic Broadcast (GAB) are VCS communication services. LLT requires `/etc/llthosts` and `/etc/llttab` files. GAB requires `/etc/gabtab` file.

Table D-1 lists the LLT configuration files and the information that these files contain.

Table D-1 LLT configuration files

File	Description
/etc/rc.config.d/lltconf	This file stores the start and stop environment variables for LLT: ■ LLT_START—Defines the startup behavior for the LLT module after a system reboot. Valid values include: 1—Indicates that LLT is enabled to start up. 0—Indicates that LLT is disabled to start up. ■ LLT_STOP—Defines the shutdown behavior for the LLT module during a system shutdown. Valid values include: 1—Indicates that LLT is enabled to shut down. 0—Indicates that LLT is disabled to shut down. The installer sets the value of these variables to 1 at the end of VCS configuration. If you manually configured VCS, make sure you set the values of these environment variables to 1.

/etc/llthosts	The file `llthosts` is a database that contains one entry per system. This file links the LLT system ID (in the first column) with the LLT host name. This file must be identical on each node in the cluster. A mismatch of the contents of the file can cause indeterminate behavior in the cluster.
	For example, the file `/etc/llthosts` contains the entries that resemble:
	`0 galaxy`
	`1 nebula`

/etc/lltab	The file `lltab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the LLT network links that correspond to the specific system.
	For example, the file `/etc/lltab` contains the entries that resemble:
	`set-node galaxy`
	`set-cluster 2`
	`link lan1 /dev/lan:1 - ether - -`
	`link lan2 /dev/lan:2 - ether - -`
	The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.
	If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.
	Refer to the `lltab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `lltab` file.

Table D-2 lists the GAB configuration files and the information that these files contain.

Table D-2 GAB configuration files

File	Description
/etc/rc.config.d/gabconf	This file stores the start and stop environment variables for GAB: ■ GAB_START—Defines the startup behavior for the GAB module after a system reboot. Valid values include: 1—Indicates that GAB is enabled to start up. 0—Indicates that GAB is disabled to start up. ■ GAB_STOP—Defines the shutdown behavior for the GAB module during a system shutdown. Valid values include: 1—Indicates that GAB is enabled to shut down. 0—Indicates that GAB is disabled to shut down. The installer sets the value of these variables to 1 at the end of VCS configuration. If you manually configured VCS, make sure you set the values of these environment variables to 1.
/etc/gabtab	After you install VCS, the file /etc/gabtab contains a `gabconfig(1)` command that configures the GAB driver for use. The file `/etc/gabtab` contains a line that resembles: `/sbin/gabconfig -c -nN` The `-c` option configures the driver for use. The `-nN` specifies that the cluster is not formed until at least `N` nodes are ready to form the cluster. Symantec recommends that you set N to be the total number of nodes in the cluster. **Note:** Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` can lead to a split-brain condition.

About the AMF configuration files

Asynchronous Monitoring Framework (AMF) kernel driver provides asynchronous event notifications to the VCS agents that are enabled for intelligent resource monitoring.

Table D-3 lists the AMF configuration files.

Table D-3 AMF configuration files

File	Description
/etc/rc.config.d/amfconf	This file stores the start and stop environment variables for AMF: ■ AMF_START—Defines the startup behavior for the AMF module after a system reboot or when AMF is attempted to start using the init script. Valid values include: 1—Indicates that AMF is enabled to start up. 0—Indicates that AMF is disabled to start up. (default) ■ AMF_STOP—Defines the shutdown behavior for the AMF module during a system shutdown or when AMF is attempted to stop using the init script. Valid values include: 1—Indicates that AMF is enabled to shut down. (default) 0—Indicates that AMF is disabled to shut down.
/etc/amftab	After you install VCS, the file `/etc/amftab` contains a `amfconfig`(1) command that configures the AMF driver for use. The AMF init script uses this `/etc/amftab` file to configure the AMF driver. The `/etc/amftab` file contains the following line by default: `/opt/VRTSamf/bin/amfconfig -c`

About the VCS configuration files

VCS configuration files include the following:

- `main.cf`
  The installer creates the VCS configuration file in the `/etc/VRTSvcs/conf/config` folder by default during the VCS configuration. The `main.cf` file contains the minimum information that defines the cluster and its nodes.
  See "Sample main.cf file for VCS clusters" on page 398.
  See "Sample main.cf file for global clusters" on page 400.
- `types.cf`
  The file `types.cf`, which is listed in the include statement in the `main.cf` file, defines the VCS bundled types for VCS resources. The file `types.cf` is also located in the folder `/etc/VRTSvcs/conf/config`.
  Additional files similar to `types.cf` may be present if agents have been added, such as `OracleTypes.cf`.

- `/etc/rc.config.d/vcsconf`

  This file stores the start and stop environment variables for VCS engine:

  - VCS_START—Defines the startup behavior for VCS engine after a system reboot. Valid values include:
    1—Indicates that VCS engine is enabled to start up.
    0—Indicates that VCS engine is disabled to start up.
  - VCS_STOP—Defines the shutdown behavior for VCS engine during a system shutdown. Valid values include:
    1—Indicates that VCS engine is enabled to shut down.
    0—Indicates that VCS engine is disabled to shut down.

  The installer sets the value of these variables to 1 at the end of VCS configuration.

  If you manually configured VCS, make sure you set the values of these environment variables to 1.

Note the following information about the VCS configuration file after installing and configuring VCS:

- The cluster definition includes the cluster information that you provided during the configuration. This definition includes the cluster name, cluster address, and the names of users and administrators of the cluster.

  Notice that the cluster has an attribute UserNames. The installvcs program creates a user "admin" whose password is encrypted; the word "password" is the default password.
- If you set up the optional I/O fencing feature for VCS, then the UseFence = SCSI3 attribute is present.
- If you configured the cluster in secure mode, the main.cf includes the VxSS service group and "SecureClus = 1" cluster attribute.
- The installvcs program creates the ClusterService service group if you configured the virtual IP, SMTP, SNMP, or global cluster options.

  The service group also has the following characteristics:

  - The group includes the IP and NIC resources.
  - The service group also includes the notifier resource configuration, which is based on your input to installvcs program prompts about notification.
  - The installvcs program also creates a resource dependency tree.
  - If you set up global clusters, the ClusterService service group contains an Application resource, wac (wide-area connector). This resource's attributes contain definitions for controlling the cluster in a global cluster environment.

Refer to the *Veritas Cluster Server Administrator's Guide* for information about managing VCS global clusters.

Refer to the *Veritas Cluster Server Administrator's Guide* to review the configuration concepts, and descriptions of main.cf and types.cf files for HP-UX systems.

Sample main.cf file for VCS clusters

The following sample main.cf file is for a cluster in secure mode.

```
include "types.cf"
include "OracleTypes.cf"
include "OracleASMTypes.cf"
include "Db2udbTypes.cf"
include "SybaseTypes.cf"


cluster vcs_cluster2 (
    UserNames = { admin = cDRpdxPmHpzS, smith = dKLhKJkHLh }
    ClusterAddress = "192.168.1.16"
    Administrators = { admin, smith }
    CounterInterval = 5
    SecureClus = 1
)

    system galaxy (
   )

    system nebula (
   )

    group ClusterService (
       SystemList = { galaxy = 0, nebula = 1 }
       UserStrGlobal = "LocalCluster@https://10.182.2.76:8443;"
       AutoStartList = { galaxy, nebula }
       OnlineRetryLimit = 3
       OnlineRetryInterval = 120
       )

    IP webip (
       Device = lan0
       Address = "192.168.1.16"
```

```
        NetMask = "255.255.240.0"
        )

NIC csgnic (
        Device = lan0
        NetworkHosts = { "192.168.1.17", "192.168.1.18" }
        )

NotifierMngr ntfr (
    SnmpConsoles = { "saturn" = Error, "jupiter" = SevereError }
    SmtpServer = "smtp.example.com"
    SmtpRecipients =  { "ozzie@example.com" = Warning,
                  "harriet@example.com" = Error }
    )

webip requires csgnic
    ntfr requires csgnic

// resource dependency tree
//
//     group ClusterService
//     {
//     NotifierMngr ntfr
//         {
//         NIC csgnic
//         }
// }



group VxSS (
    SystemList = { galaxy = 0, nebula = 1 }
    Parallel = 1
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Phantom phantom_vxss (
        )

    ProcessOnOnly vxatd (
        IgnoreArgs = 1
        PathName = "/opt/VRTSat/bin/vxatd"
        )
```

```
// resource dependency tree
   //
   // group VxSS
   // {
   // Phantom phantom_vxss
   // ProcessOnOnly vxatd
   // }
```

Sample main.cf file for global clusters

If you installed VCS with the Global Cluster option, note that the ClusterService group also contains the Application resource, wac. The wac resource is required to control the cluster in a global cluster environment.

```
    .
    .
    group ClusterService (
       SystemList = { galaxy = 0, nebula = 1 }

       UserStrGlobal = "LocalCluster@https://10.182.2.78:8443;"

       AutoStartList = { galaxy, nebula }
       OnlineRetryLimit = 3
       OnlineRetryInterval = 120
       )

       Application wac (
          StartProgram = "/opt/VRTSvcs/bin/wacstart"
          StopProgram = "/opt/VRTSvcs/bin/wacstop"
          MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
          RestartLimit = 3
          )
    .
    .
```

In the following main.cf file example, bold text highlights global cluster specific entries.

```
include "types.cf"

cluster vcs03 (
```

```
    ClusterAddress = "10.182.13.50"
    SecureClus = 1
    )

system sysA (
    )

system sysB (
    )

system sysC (
    )

group ClusterService (
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

Application wac (
    StartProgram = "/opt/VRTSvcs/bin/wacstart"
    StopProgram = "/opt/VRTSvcs/bin/wacstop"
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
    RestartLimit = 3
    )

IP gcoip (
    Device = lan0
    Address = "10.182.13.50"
    NetMask = "255.255.240.0"
    )

NIC csgnic (
    Device = lan0
    )

NotifierMngr ntfr (
   SnmpConsoles = { jupiter" = SevereError }
   SmtpServer = "smtp.example.com"
   SmtpRecipients =  { "ozzie@example.com" = SevereError }
   )
```

```
gcoip requires csgnic
ntfr requires csgnic
wac requires gcoip

// resource dependency tree
//
//     group ClusterService
//     {
//     NotifierMngr ntfr
//         {
//         NIC csgnic
//         }
//     Application wac
//         {
//         IP gcoip
//             {
//             NIC csgnic
//             }
//         }
//     }

group VxSS (
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    Parallel = 1
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

Phantom phantom_vxss (
    )

ProcessOnOnly vxatd (
    IgnoreArgs = 1
    PathName = "/opt/VRTSat/bin/vxatd"
    )

// resource dependency tree
//
//     group VxSS
//     {
//     Phantom phantom_vxss
```

```
//      ProcessOnOnly vxatd
//      }
```

About I/O fencing configuration files

Table D-4 lists the I/O fencing configuration files.

Table D-4 I/O fencing configuration files

File	Description
/etc/rc.config.d/vxfenconf	This file stores the start and stop environment variables for I/O fencing: ■ VXFEN_START—Defines the startup behavior for the I/O fencing module after a system reboot. Valid values include: 1—Indicates that I/O fencing is enabled to start up. 0—Indicates that I/O fencing is disabled to start up. ■ VXFEN_STOP—Defines the shutdown behavior for the I/O fencing module during a system shutdown. Valid values include: 1—Indicates that I/O fencing is enabled to shut down. 0—Indicates that I/O fencing is disabled to shut down. The installer sets the value of these variables to 1 at the end of VCS configuration. If you manually configured VCS, you must make sure to set the values of these environment variables to 1.
/etc/vxfendg	This file includes the coordinator disk group information. This file is not applicable for server-based fencing.

Table D-4 I/O fencing configuration files *(continued)*

File	Description
/etc/vxfenmode	This file contains the following parameters: ■ vxfen_mode ■ scsi3—For disk-based fencing ■ customized—For server-based fencing ■ disabled—To run the I/O fencing driver but not do any fencing operations. ■ vxfen_mechanism This parameter is applicable only for server-based fencing. Set the value as cps. ■ scsi3_disk_policy You must configure the vxfen module to use DMP devices or iSCSI devices, and set the SCSI-3 disk policy as dmp. ■ security This parameter is applicable only for server-based fencing. 1—Indicates that Symantec Product Authentication Service is used for CP server communications. This setting is the default. 0—Indicates that communication with the CP server is in non-secure mode. **Note:** The CP server and the VCS clusters must have the same security setting. ■ List of coordination points This list is required only for server-based fencing configuration. Coordination points in a server-based fencing can include coordinator disks, CP servers, or a mix of both. If you use coordinator disks, you must create a coordinator disk group with the coordinator disk names. Refer to the sample file /etc/vxfen.d/vxfenmode_cps for more information on how to specify the coordination points. ■ single_cp This parameter is applicable only for server-based fencing which uses a single highly available CP server as its coordination point.

Table D-4 I/O fencing configuration files *(continued)*

File	Description

/etc/vxfentab	When I/O fencing starts, the vxfen startup script creates this `/etc/vxfentab` file on each node. The startup script uses the contents of the `/etc/vxfendg` and `/etc/vxfenmode` files. Any time a system is rebooted, the fencing driver reinitializes the `vxfentab` file with the current list of all the coordinator points.
	Note: The `/etc/vxfentab` file is a generated file; do not modify this file.
	An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows:
	`/dev/vx/rdmp/c1t1d0`
	`/dev/vx/rdmp/c2t1d0`
	`/dev/vx/rdmp/c3t1d0`
	For server-based fencing, the `/etc/vxfentab` file also includes the security settings information.
	For server-based fencing with single CP server, the `/etc/vxfentab` file also includes the single_cp settings information.

Sample configuration files for CP server

This following are example main.cf files for a CP server that is hosted on a single node, and a CP server that is hosted on an SFHA cluster.

- The main.cf file for a CP server that is hosted on a single node:
  See "Sample main.cf file for CP server hosted on a single node that runs VCS" on page 405.
- The main.cf file for a CP server that is hosted on an SFHA cluster:
  See "Sample main.cf file for CP server hosted on a two-node SFHA cluster" on page 408.

Note: The CP server supports Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with VCS clusters. The following example main.cf files use IPv4 addresses.

Sample main.cf file for CP server hosted on a single node that runs VCS

The following is an example of a single CP server node main.cf.

For this CP server single node main.cf, note the following values:

- Cluster name: cps1
- Node name: mycps1

```
include "types.cf"

// cluster name:  cps1
// CP server: mycps1

cluster cps1 (
     UserNames = { admin = bMNfMHmJNiNNlVNhMK, haris = fopKojNvpHouNn,
             "mycps1.symantecexample.com@root@vx" = aj,
             "root@mycps1.symantecexample.com" = hq }
     Administrators = { admin, haris,
             "mycps1.symantecexample.com@root@vx",
             "root@mycps1.symantecexample.com" }
     SecureClus = 1
     HacliUserLevel = COMMANDROOT
     )

system mycps1 (
     )

group CPSSG (
      SystemList = { mycps1 = 0 }
      AutoStartList = { mycps1 }
      )

      IP cpsvip (
            Device @mycps1 = lan0
            Address = "10.209.3.1"
            NetMask = "255.255.252.0"
            )

      NIC cpsnic (
            Device @mycps1 = lan0
            )

     Process vxcpserv (
           PathName = "/opt/VRTScps/bin/vxcpserv"
           ConfInterval = 30
           RestartLimit = 3
```

```
        )

 cpsvip requires cpsnic
 vxcpserv requires cpsvip


 // resource dependency tree
 //
 // group CPSSG
 // {
 // Process vxcpserv
 //     {
 //     IP cpsvip
 //         {
 //         NIC cpsnic
 //         }
 //     }
 // }


group VxSS (
      SystemList = { mycps1 = 0 }
      Parallel = 1
      AutoStartList = { mycps1 }
      OnlineRetryLimit = 3
      OnlineRetryInterval = 120
      )

      Phantom phantom_vxss (
            )

      ProcessOnOnly vxatd (
            IgnoreArgs = 1
            PathName = "/opt/VRTSat/bin/vxatd"
            )



 // resource dependency tree
 //
 //    group VxSS
 //    {
 //    Phantom phantom_vxss
```

```
//    ProcessOnOnly vxatd
//    }
```

Sample main.cf file for CP server hosted on a two-node SFHA cluster

The following is an example of a main.cf, where the CP server is hosted on an SFHA cluster.

For this CP server hosted on an SFHA cluster main.cf, note the following values:

- Cluster name: cps1
- Nodes in the cluster: mycps1, mycps2

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"


// cluster: cps1
// CP servers:
// mycps1
// mycps2

cluster cps1 (
     UserNames = { admin = ajkCjeJgkFkkIskEjh,
            "mycps1.symantecexample.com@root@vx" = JK,
            "mycps2.symantecexample.com@root@vx" = dl }
     Administrators = { admin, "mycps1.symantecexample.com@root@vx",
            "mycps2.symantecexample.com@root@vx" }
     SecureClus = 1
     )

system mycps1 (
     )

system mycps2 (
     )

group CPSSG (
      SystemList = { mycps1 = 0, mycps2 = 1 }
      AutoStartList = { mycps1, mycps2 } )

      DiskGroup cpsdg (
            DiskGroup = cps_dg
```

```
        )

    IP cpsvip (
        Device @mycps1 = lan0
        Device @mycps2 = lan0
        Address = "10.209.81.88"
        NetMask = "255.255.252.0"
        )

    Mount cpsmount (
        MountPoint = "/etc/VRTScps/db"
        BlockDevice = "/dev/vx/dsk/cps_dg/cps_volume"
        FSType = vxfs
        FsckOpt = "-y"
        )

    NIC cpsnic (
        Device @mycps1 = lan0
        Device @mycps2 = lan0
        )

    Process vxcpserv (
        PathName = "/opt/VRTScps/bin/vxcpserv"
        )

    Volume cpsvol (
        Volume = cps_volume
        DiskGroup = cps_dg
        )

cpsmount requires cpsvol
cpsvip requires cpsnic
cpsvol requires cpsdg
vxcpserv requires cpsmount
vxcpserv requires cpsvip


// resource dependency tree
//
// group CPSSG
// {
// Process vxcpserv
//     {
```

```
//     Mount cpsmount
//         {
//         Volume cpsvol
//             {
//             DiskGroup cpsdg
//             }
//         }
//     IP cpsvip
//         {
//         NIC cpsnic
//         }
//     }
// }


group VxSS (
      SystemList = { mycps1 = 0, mycps2 = 1 }
      Parallel = 1
      AutoStartList = { mycps1, mycps2 }
      OnlineRetryLimit = 3
      OnlineRetryInterval = 120
      )

      Phantom phantom_vxss (
            )

      ProcessOnOnly vxatd (
            IgnoreArgs = 1
            PathName = "/opt/VRTSat/bin/vxatd"
            )



// resource dependency tree
//
// group VxSS
// {
// Phantom phantom_vxss
// ProcessOnOnly vxatd
// }
```

Appendix E

Installing VCS on a single node

This appendix includes the following topics:

About installing VCS on a single node

You can install VCS 5.1SP1 on a single node. You can subsequently add another node to the single-node cluster to form a multinode cluster. You can also prepare a single node cluster for addition into a multi-node cluster. Single node clusters can be used for testing as well.

You can install VCS onto a single node using the installer program or you can add it manually.

See "Creating a single-node cluster using the installer program" on page 412.

See "Creating a single-node cluster manually" on page 413.

Creating a single-node cluster using the installer program

Table E-1 specifies the tasks that are involved to install VCS on a single node using the installer program.

Table E-1 Tasks to create a single-node cluster using the installer

Task	Reference
Prepare for installation.	See "Preparing for a single node installation" on page 412.
Install the VCS software on the system using the installer.	See "Starting the installer for the single node cluster" on page 412.

Preparing for a single node installation

You can use the installer program to install a cluster on a single system for either of the two following purposes:

- To prepare the single node cluster to join a larger cluster
- To prepare the single node cluster to be a stand-alone single node cluster

When you prepare it to join a larger cluster, install it with LLT and GAB. For a stand-alone cluster, you do not need to enable LLT and GAB.

For more information about LLT and GAB:

See "About LLT and GAB" on page 23.

Starting the installer for the single node cluster

When you install VCS on a single system, follow the instructions in this guide for installing VCS using the product installer.

During the installation, you need to answer two questions specifically for single node installations. When the installer asks:

```
Enter the system names separated by spaces on which to install
VCS[q,?]
```

Enter a single system name. The installer now asks if you want to enable LLT and GAB:

```
If you plan to run VCS on a single node without any need for
adding cluster node online, you have an option to proceed
```

```
without starting GAB and LLT.
Starting GAB and LLT is recommended.
Do you want to start GAB and LLT? [y,n,q,?] (y)
```

Answer `n` if you want to use the single node cluster as a stand-alone cluster.

Answer `y` if you plan to incorporate the single node cluster into a multi-node cluster in the future.

Continue with the installation.

Creating a single-node cluster manually

Table E-2 specifies the tasks that you need to perform to install VCS on a single node.

Table E-2 Tasks to create a single-node cluster manually

Task	Reference
Set the PATH variable	See "Setting the path variable for a manual single node installation" on page 413.
Install the VCS software manually and add a license key	See "Installing VCS software manually on a single node" on page 414.
Remove any LLT or GAB configuration files and rename LLT and GAB startup files. A single-node cluster does not require the node-to-node communication service, LLT, or the membership communication service, GAB.	See "Renaming the LLT and GAB startup files" on page 414.
Create and modify the VCS configuration files.	See "Configuring VCS" on page 414.
Start VCS and verify single-node operation.	See "Verifying single-node operation" on page 414.

Setting the path variable for a manual single node installation

Set the path variable.

See "Setting the PATH variable" on page 67.

Installing VCS software manually on a single node

Install the VCS 5.1SP1 depots and patches manually and install the license key.

Refer to the following sections:

- See “Installing VCS software manually” on page 213.
- See “Adding a license key for a manual installation” on page 216.

Renaming the LLT and GAB startup files

You may need the LLT and GAB startup files to upgrade the single-node cluster to a multiple-node cluster at a later time.

To rename the LLT and GAB startup files

- Rename the LLT and GAB startup files.

```
# mv /sbin/rc2.d/S68llt /sbin/rc2.d/s68llt
# mv /sbin/rc2.d/S92gab /sbin/rc2.d/s92gab
```

Configuring VCS

You now need to configure VCS.

See “Configuring VCS manually” on page 223.

Verifying single-node operation

After successfully creating a single-node cluster, start VCS and verify the cluster.

To verify single-node cluster

1. Bring up VCS manually as a single-node cluster using `hastart` with the `-onenode` option:

```
# hastart -onenode
```

2. Verify that the `had` and `hashadow` daemons are running in single-node mode:

```
# ps -ef | grep had
root  285   1  0 14:49:31 ?  0:02 /opt/VRTSvcs/bin/had -onenode
root  288   1  0 14:49:33 ?  0:00 /opt/VRTSvcs/bin/hashadow
```

Appendix F

Configuring LLT over UDP

This appendix includes the following topics:

Using the UDP layer for LLT

VCS 5.1SP1 provides the option of using LLT over the UDP (User Datagram Protocol) layer for clusters using wide-area networks and routers. UDP makes LLT packets routable and thus able to span longer distances more economically.

When to use LLT over UDP

Use LLT over UDP in the following situations:

- LLT must be used over WANs
- When hardware, such as blade servers, do not support LLT over Ethernet

LLT over UDP is slower than LLT over Ethernet. Use LLT over UDP only when the hardware configuration makes it necessary.

Manually configuring LLT over UDP using IPv4

The following checklist is to configure LLT over UDP:

- Make sure that the LLT private links are on different physical networks.

If the LLT private links are not on different physical networks, then make sure that the links are on separate subnets. Set the broadcast address in `/etc/lltab` explicitly depending on the subnet for each link.
See "Broadcast address in the /etc/lltab file" on page 416.

- Make sure that each NIC has an IP address that is configured before configuring LLT.
- Make sure the IP addresses in the `/etc/lltab` files are consistent with the IP addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port.
See "Selecting UDP ports" on page 418.
- Set the broadcast address correctly for direct-attached (non-routed) links.
See "Sample configuration: direct-attached links" on page 420.
- For the links that cross an IP router, disable broadcast features and specify the IP address of each link manually in the `/etc/lltab` file.
See "Sample configuration: links crossing IP routers" on page 422.

Broadcast address in the /etc/lltab file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the /etc/lltab file on the first node galaxy:

```
galaxy # cat /etc/lltab
set-node galaxy
set-cluster 1
link link1 /dev/udp - udp 50000 - 192.168.9.1 192.168.9.255
link link2 /dev/udp - udp 50001 - 192.168.10.1 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

```
galaxy # ifconfig lan1
lan1: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
        inet 192.168.9.1 netmask ffffff00 broadcast 192.168.9.255
galaxy # ifconfig lan2
lan2: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
        inet 192.168.10.1 netmask ffffff00 broadcast 192.168.10.255
```

- Display the content of the /etc/lltab file on the second node nebula:

```
nebula # cat /etc/lltab
set-node nebula
```

```
set-cluster 1
link link1 /dev/udp - udp 50000 - 192.168.9.2 192.168.9.255
link link2 /dev/udp - udp 50001 - 192.168.10.2 192.168.10.255
```

Verify the subnet mask using the `ifconfig` command to ensure that the two links are on separate subnets.

```
nebula # ifconfig lan1
lan1: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
        inet 192.168.9.2 netmask ffffff00 broadcast 192.168.9.255
nebula # ifconfig lan2
lan2: flags=1843<UP,BROADCAST,RUNNING,MULTICAST,CKO>
        inet 192.168.10.2 netmask ffffff00 broadcast 192.168.10.255
```

The link command in the /etc/lltab file

Review the link command information in this section for the `/etc/lltab` file. See the following information for sample configurations:

- See "Sample configuration: direct-attached links" on page 420.
- See "Sample configuration: links crossing IP routers" on page 422.

Table F-1 describes the fields of the link command that are shown in the `/etc/lltab` file examples. Note that some of the fields differ from the command for standard LLT links.

Table F-1 Field description for link command in /etc/lltab

Field	Description
tag-name	A unique string that is used as a tag by LLT; for example link1, link2,....
device	The device path of the UDP protocol; for example `/dev/udp`.
node-range	Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.
link-type	Type of link; must be "udp" for LLT over UDP.
udp-port	Unique UDP port in the range of 49152-65535 for the link. See "Selecting UDP ports" on page 418.
MTU	"-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the `lltstat -l` command to display the current value.

Table F-1 Field description for link command in /etc/lltab *(continued)*

Field	Description
IP address	IP address of the link on the local node.
bcast-address	■ For clusters with enabled broadcasts, specify the value of the subnet broadcast address. ■ "-" is the default for clusters spanning routers.

The set-addr command in the /etc/lltab file

The `set-addr` command in the `/etc/lltab` file is required when the broadcast feature of LLT is disabled, such as when LLT must cross IP routers.

See "Sample configuration: links crossing IP routers" on page 422.

Table F-2 describes the fields of the set-addr command.

Table F-2 Field description for set-addr command in /etc/lltab

Field	Description
node-id	The ID of the cluster node; for example, 0.
link tag-name	The string that LLT uses to identify the link; for example link1, link2,....
address	IP address assigned to the link for the peer node.

Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file `/etc/services`. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
# netstat -a | head -2 ; netstat -a | grep udp
Active Internet connections (including servers)
```

```
Proto Recv-Q Send-Q  Local Address Foreign Address        (state)
udp        0      0  *.ntalk                *.*
udp        0      0  *.*                    *.*
udp        0      0  *.49193                *.*
udp        0      0  *.49152                *.*
udp        0      0  *.portmap              *.*
udp        0      0  *.*                    *.*
udp        0      0  *.135                  *.*
udp        0      0  *.2121                 *.*
udp        0      0  *.xdmcp                *.*
udp        0      0  *.49196                *.*
udp        0      0  *.*                    *.*
udp        0      0  *.snmp                 *.*
udp        0      0  *.*                    *.*
udp        0      0  *.49153                *.*
udp        0      0  *.echo                 *.*
udp        0      0  *.discard              *.*
udp        0      0  *.daytime              *.*
udp        0      0  *.chargen              *.*
udp        0      0  *.syslog               *.*
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the `/etc/services` file, its associated name is displayed rather than the port number in the output.

Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:

```
# set_parms ip_address
```

For example:

- For the first network interface on the node galaxy:

  ```
  IP address=192.168.9.1, Broadcast address=192.168.9.255,
  Netmask=255.255.255.0
  ```

  For the first network interface on the node nebula:

  ```
  IP address=192.168.9.2, Broadcast address=192.168.9.255,
  Netmask=255.255.255.0
  ```

- For the second network interface on the node galaxy:

  ```
  IP address=192.168.10.1, Broadcast address=192.168.10.255,
  Netmask=255.255.255.0
  ```

  For the second network interface on the node nebula:

  ```
  IP address=192.168.10.2, Broadcast address=192.168.10.255,
  Netmask=255.255.255.0
  ```

Configuring the broadcast address for LLT

For nodes on different subnets, set the broadcast address in `/etc/llttab` depending on the subnet that the links are on.

An example of a typical `/etc/llttab` file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

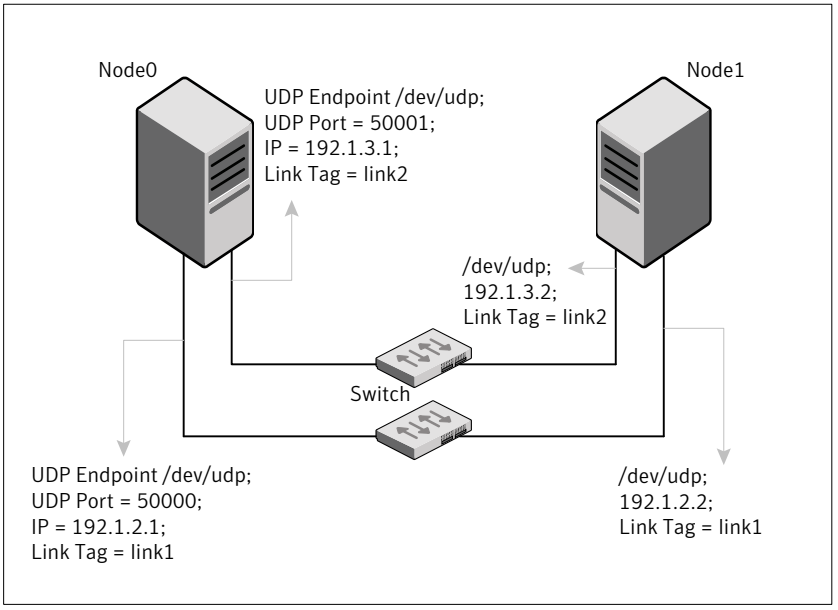
```
# cat /etc/llttab
set-node nodexyz
set-cluster 100

link link1 /dev/udp - udp 50000 - 192.168.30.1 192.168.30.255
link link2 /dev/udp - udp 50001 - 192.168.31.1 192.168.31.255
```

Sample configuration: direct-attached links

Figure F-1 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure F-1 A typical configuration of direct-attached links that use LLT over UDP



The configuration that the `/etc/lltab` file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the `/etc/lltab` file using the `set-addr` command. For direct attached links, you do need to set the broadcast address of the links in the `/etc/lltab` file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig` *`interface_name`* command.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.1 192.1.3.255
```

The file for Node 1 resembles:

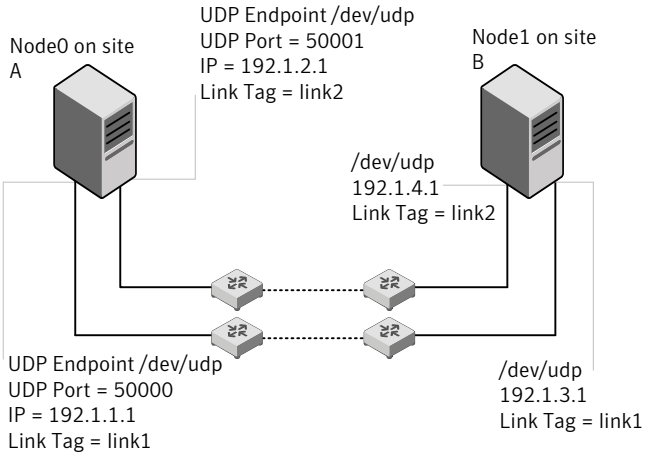
```
set-node Node1
set-cluster 1
```

```
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
link link1 /dev/udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 /dev/udp - udp 50001 - 192.1.3.2 192.1.3.255
```

Sample configuration: links crossing IP routers

Figure F-2 depicts a typical configuration of links crossing an IP router employing LLT over UDP. The illustration shows two nodes of a four-node cluster.

Figure F-2 A typical configuration of links crossing an IP router



The configuration that the following `/etc/lltab` file represents for Node 1 has links crossing IP routers. Notice that IP addresses are shown for each link on each peer node. In this configuration broadcasts are disabled. Hence, the broadcast address does not need to be set in the `link` command of the `/etc/lltab` file.

```
set-node Node1
set-cluster 1

link link1 /dev/udp - udp 50000 - 192.1.3.1 -
link link2 /dev/udp - udp 50001 - 192.1.4.1 -
#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr        0 link1 192.1.1.1
set-addr        0 link2 192.1.2.1
set-addr        2 link1 192.1.5.2
set-addr        2 link2 192.1.6.2
```

```
set-addr        3 link1 192.1.7.3
set-addr        3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb     0
set-arp         0
```

The `/etc/llttab` file on Node 0 resembles:

```
set-node Node0
set-cluster 1

link link1 /dev/udp - udp 50000 - 192.1.1.1 -
link link2 /dev/udp - udp 50001 - 192.1.2.1 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr        1 link1 192.1.3.1
set-addr        1 link2 192.1.4.1
set-addr        2 link1 192.1.5.2
set-addr        2 link2 192.1.6.2
set-addr        3 link1 192.1.7.3
set-addr        3 link2 192.1.8.3

#disable LLT broadcasts
set-bcasthb     0
set-arp         0
```

Manually configuring LLT over UDP using IPv6

The following checklist is to configure LLT over UDP:

- For UDP6, the multicast address is set to "-".
- Make sure that each NIC has an IPv6 address that is configured before configuring LLT.
- Make sure the IPv6 addresses in the /etc/llttab files are consistent with the IPv6 addresses of the network interfaces.
- Make sure that each link has a unique not well-known UDP port.
  See "Selecting UDP ports" on page 425.
- For the links that cross an IP router, disable multicast features and specify the IPv6 address of each link manually in the /etc/llttab file.
  See "Sample configuration: links crossing IP routers" on page 427.

The link command in the /etc/llttab file

Review the link command information in this section for the /etc/llttab file. See the following information for sample configurations:

- See "Sample configuration: direct-attached links" on page 426.
- See "Sample configuration: links crossing IP routers" on page 427.

Note that some of the fields in Table F-3 differ from the command for standard LLT links.

Table F-3 describes the fields of the link command that are shown in the /etc/llttab file examples.

Table F-3 Field description for link command in /etc/llttab

Field	Description
tag-name	A unique string that is used as a tag by LLT; for example link1, link2,....
device	The device path of the UDP protocol; for example /dev/udp6.
node-range	Nodes using the link. "-" indicates all cluster nodes are to be configured for this link.
link-type	Type of link; must be "udp6" for LLT over UDP.
udp-port	Unique UDP port in the range of 49152-65535 for the link. See "Selecting UDP ports" on page 425.
MTU	"-" is the default, which has a value of 8192. The value may be increased or decreased depending on the configuration. Use the `lltstat -l` command to display the current value.
IPv6 address	IPv6 address of the link on the local node.
mcast-address	"-" is the default for clusters spanning routers.

The set-addr command in the /etc/llttab file

The `set-addr` command in the /etc/llttab file is required when the multicast feature of LLT is disabled, such as when LLT must cross IP routers.

See "Sample configuration: links crossing IP routers" on page 427.

Table F-4 describes the fields of the set-addr command.

Table F-4 Field description for set-addr command in /etc/lltab

Field	Description
node-id	The ID of the cluster node; for example, 0.
link tag-name	The string that LLT uses to identify the link; for example link1, link2,....
address	IPv6 address assigned to the link for the peer node.

Selecting UDP ports

When you select a UDP port, select an available 16-bit integer from the range that follows:

- Use available ports in the private range 49152 to 65535
- Do not use the following ports:
  - Ports from the range of well-known ports, 0 to 1023
  - Ports from the range of registered ports, 1024 to 49151

To check which ports are defined as defaults for a node, examine the file /etc/services. You should also use the `netstat` command to list the UDP ports currently in use. For example:

```
# netstat -a | head -2 ; netstat -a | grep udp
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address Foreign Address        (state)
udp        0      0  *.ntalk                *.*
udp        0      0  *.*                    *.*
udp        0      0  *.49193                *.*
udp        0      0  *.49152                *.*
udp        0      0  *.portmap              *.*
udp        0      0  *.*                    *.*
udp        0      0  *.135                  *.*
udp        0      0  *.2121                 *.*
udp        0      0  *.xdmcp                *.*
udp        0      0  *.49196                *.*
udp        0      0  *.*                    *.*
udp        0      0  *.snmp                 *.*
udp        0      0  *.*                    *.*
udp        0      0  *.49153                *.*
udp        0      0  *.echo                 *.*
udp        0      0  *.discard              *.*
```

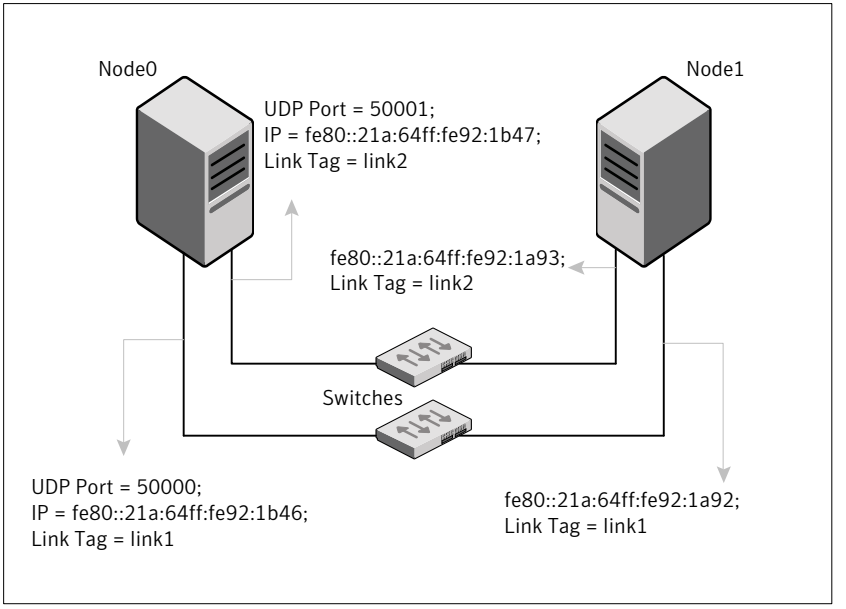
```
udp        0      0  *.daytime              *.*
udp        0      0  *.chargen              *.*
udp        0      0  *.syslog               *.*
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

Sample configuration: direct-attached links

Figure F-3 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure F-3 A typical configuration of direct-attached links that use LLT over UDP



The configuration that the /etc/llttab file for Node 0 represents has directly attached crossover links. It might also have the links that are connected through a hub or switch. These links do not cross routers.

LLT uses IPv6 multicast requests for peer node address discovery. So the addresses of peer nodes do not need to be specified in the /etc/llttab file using the `set-addr` command. Use the `ifconfig` *`interface_name`* command to verify that the IPv6 address is set correctly.

You can also use the `lanscan` command to verify the IPv6 address.

```
set-node Node0
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -
```

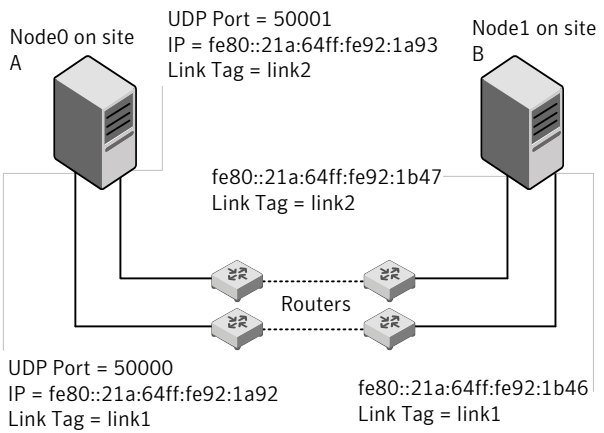
The file for Node 1 resembles:

```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address mcast-address
link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -
```

Sample configuration: links crossing IP routers

Figure F-4 depicts a typical configuration of links crossing an IP router employing LLT over UDP. The illustration shows two nodes of a four-node cluster.

Figure F-4 A typical configuration of links crossing an IP router



The configuration that the following `/etc/lltab` file represents for Node 1 has links crossing IP routers. Notice that IPv6 addresses are shown for each link on each peer node. In this configuration multicasts are disabled.

```
set-node Node1
set-cluster 1

link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1a92 -
link link1 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1a93 -
#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 0 link1 fe80::21a:64ff:fe92:1b46
set-addr 0 link2 fe80::21a:64ff:fe92:1b47
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb     0
set-arp         0
```

The `/etc/lltab` file on Node 0 resembles:

```
set-node Node0
set-cluster 1

link link1 /dev/udp6 - udp6 50000 - fe80::21a:64ff:fe92:1b46 -
link link2 /dev/udp6 - udp6 50001 - fe80::21a:64ff:fe92:1b47 -

#set address of each link for all peer nodes in the cluster
#format: set-addr node-id link tag-name address
set-addr 1 link1 fe80::21a:64ff:fe92:1a92
set-addr 1 link2 fe80::21a:64ff:fe92:1a93
set-addr 2 link1 fe80::21a:64ff:fe92:1d70
set-addr 2 link2 fe80::21a:64ff:fe92:1d71
set-addr 3 link1 fe80::209:6bff:fe1b:1c94
set-addr 3 link2 fe80::209:6bff:fe1b:1c95

#disable LLT multicasts
set-bcasthb     0
set-arp         0
```

LLT over UDP sample /etc/llttab

The following is a sample of LLT over UDP in the etc/llttab file.

```
set-node galaxy
set-cluster clus1
link lan1 /dev/udp - udp 50000 - 192.168.10.1 -
link lan2 /dev/udp - udp 50001 - 192.168.11.1 -
link-lowpri lan0 /dev/udp - udp 50004 - 10.200.58.205 -
set-addr 1 lan1 192.168.10.2
set-addr 1 lan2 192.168.11.2
set-addr 1 lan0 10.200.58.206
set-bcasthb 0
set-arp 0
```

Appendix G

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

Setting up inter-system communication

If you manually need to set up a communication mode, refer to these procedures. You must have root privilege to issue ssh or remsh commands on all systems in the cluster. If ssh is used to communicate between systems, it must be configured in a way such that it operates without requests for passwords or passphrases. Similarly, remsh must be configured in such a way to not prompt for passwords.

If system communication is not possible between systems using ssh or remsh, contact Symantec Support. See http://support.symantec.com.

Setting up ssh on cluster systems

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

Use Secure Shell (ssh) to do the following:

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

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

Configuring ssh

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

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

To configure ssh

1. Log on to the system from which you want to install VCS.
2. Generate a DSA key pair on this system by running the following command:

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

3. Accept the default location of ~/.ssh/id_dsa.
4. When the command prompts, enter a passphrase and confirm it.
5. Change the permissions of the .ssh directory by typing:

   ```
   # chmod 755 ~/.ssh
   ```

6. The file ~/.ssh/id_dsa.pub contains a line that begins with ssh_dss and ends with the name of the system on which it was created. Copy this line to the /.ssh/authorized_keys file on all systems where you plan to installVCS.

   If the local system is part of the cluster, make sure to edit the authorized_keys file on that system.
7. Run the following commands on the system where you are installing:

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

   This step is shell-specific and is valid for the duration the shell is alive.
8. When the command prompts, enter your DSA passphrase.

   You are ready to install VCS on several systems in one of the following ways:

   - Run the installvcs program on any one of the systems

- Run the installvcs program on an independent system outside the cluster

9 To verify that you can connect to the systems where you plan to install VCS, type:

```
# ssh -x -l root north ls
# ssh -x -l root south ifconfig lan0
```

The commands should execute on the remote system without having to enter a passphrase or password.

Appendix H

Troubleshooting VCS installation

This appendix includes the following topics:

What to do if you see a licensing reminder

In this release, you can install without a license key. In order to comply with the End User License Agreement, you must either install a license key or make the host managed by a Management Server. If you do not comply with these terms within 60 days, the following warning messages result:

```
WARNING V-365-1-1 This host is not entitled to run Veritas Storage
Foundation/Veritas Cluster Server.As set forth in the End User
License Agreement (EULA) you must complete one of the two options
set forth below. To comply with this condition of the EULA and
stop logging of this message, you have <nn> days to either:
```

```
- make this host managed by a Management Server (see
  http://go.symantec.com/sfhakeyless for details and free download),
  or
- add a valid license key matching the functionality in use on this host
  using the command 'vxlicinst'
```

To comply with the terms of the EULA, and remove these messages, you must do one of the following within 60 days:

- Install a valid license key corresponding to the functionality in use on the host. After you install the license key, you must validate the license key using the following command:

  ```
  # vxkeyless display
  ```

- Continue with keyless licensing by managing the server or cluster with a management server.
  For more information about keyless licensing, see the following URL: http://go.symantec.com/sfhakeyless

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

To stop the processes

- Use the `-stop` option to stop the product installation script.

  For example, to stop the product's processes, enter the following command:

  ```
  # ./installer -stop
  ```

To start the processes

- Use the `-start` option to start the product installation script.

  For example, to start the product's processes, enter the following command:

  ```
  # ./installer -start
  ```

Installer cannot create UUID for the cluster

The installer displays the following error message if the installer cannot find the uuidconfig.pl script before it configures the UUID for the cluster:

```
Couldn't find uuidconfig.pl for uuid configuration,
please create uuid manually before start vcs
```

You may see the error message during VCS configuration, upgrade, or when you add a node to the cluster using the installer.

Workaround: To start VCS, you must run the uuidconfig.pl script manually to configure the UUID on each cluster node.

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

LLT startup script displays errors

If more than one system on the network has the same clusterid-nodeid pair and the same Ethernet sap/UDP port, then the LLT startup script displays error messages similar to the following:

```
LLT lltconfig ERROR V-14-2-15238 node 1 already exists
in cluster 8383 and has the address - 00:18:8B:E4:DE:27
LLT lltconfig ERROR V-14-2-15241 LLT not configured,
use -o to override this warning
LLT lltconfig ERROR V-14-2-15664 LLT could not
configure any link
LLT lltconfig ERROR V-14-2-15245 cluster id 1 is
already being used by nid 0 and has the
address - 00:04:23:AC:24:2D
LLT lltconfig ERROR V-14-2-15664 LLT could not
configure any link
```

Recommended action: Ensure that all systems on the network have unique clusterid-nodeid pair. You can use the `lltdump -D` command to get the list of

unique clusterid-nodeid pairs connected to the network. This utility is available only for LLT-over-ethernet.

The vxfentsthdw utility fails when SCSI TEST UNIT READY command fails

While running the vxfentsthdw utility, you may see a message that resembles as follows:

```
Issuing SCSI TEST UNIT READY to disk reserved by other node
FAILED.
Contact the storage provider to have the hardware configuration
fixed.
```

The disk array does not support returning success for a `SCSI TEST UNIT READY` command when another host has the disk reserved using SCSI-3 persistent reservations. This happens with the Hitachi Data Systems 99XX arrays if bit 186 of the system mode option is not enabled.

Issues during fencing startup on VCS cluster nodes set up for server-based fencing

Table H-1 Fencing startup issues on VCS cluster (client cluster) nodes

Issue	Description and resolution
`cpsadm` command on the VCS cluster gives connection error	If you receive a connection error message after issuing the `cpsadm` command on the VCS cluster, perform the following actions: ■ Ensure that the CP server is reachable from all the VCS cluster nodes. ■ Check that the VCS cluster nodes use the correct CP server virtual IP or virtual hostname and the correct port number. Check the /etc/vxfenmode file. ■ Ensure that the running CP server is using the same virtual IP/virtual hostname and port number.

Table H-1 Fencing startup issues on VCS cluster (client cluster) nodes *(continued)*

Issue	Description and resolution
Authorization failure	Authorization failure occurs when the CP server's nodes or users are not added in the CP server configuration. Therefore, fencing on the VCS cluster (client cluster) node is not allowed to access the CP server and register itself on the CP server. Fencing fails to come up if it fails to register with a majority of the coordination points. To resolve this issue, add the CP server node and user in the CP server configuration and restart fencing. See "Preparing the CP servers manually for use by the VCS cluster" on page 233.
Authentication failure	If you had configured secure communication between the CP server and the VCS cluster (client cluster) nodes, authentication failure can occur due to the following causes: ■ Symantec Product Authentication Services (AT) is not properly configured on the CP server and/or the VCS cluster. ■ The CP server and the VCS cluster nodes use the same root broker but the certificate hash of the root broker is not same on the VCS cluster and the CP server. Run the following command on both the CP server and the VCS cluster to see the certificate hash: # **cpsat showalltrustedcreds** ■ The CP server and the VCS cluster nodes use different root brokers, and trust is not established between the authentication brokers: ■ The hostname of the VCS cluster nodes is not the same hostname used when configuring AT. The hostname of the VCS cluster nodes must be set to the hostname used when configuring AT. You can view the fully qualified hostname registered with AT using the `cpsat showcred` command. After entering this command, the hostname appears in the User Name field. ■ The CP server and VCS cluster do not have the same security setting. In order to configure secure communication, both the CP server and the VCS cluster must have same security setting. In order to have the same security setting, the security parameter must have same value in the `/etc/vxcps.conf` file on CP server and in the `/etc/vxfenmode` file on the VCS cluster (client cluster) nodes.

Table H-1 Fencing startup issues on VCS cluster (client cluster) nodes *(continued)*

Issue	Description and resolution
Preexisting split-brain	Assume the following situations to understand preexisting split-brain in server-based fencing: ■ There are three CP servers acting as coordination points. One of the three CP servers then becomes inaccessible. While in this state, also one client node leaves the cluster. When the inaccessible CP server restarts, it has a stale registration from the node which left the VCS cluster. In this case, no new nodes can join the cluster. Each node that attempts to join the cluster gets a list of registrations from the CP server. One CP server includes an extra registration (of the node which left earlier). This makes the joiner node conclude that there exists a preexisting split-brain between the joiner node and the node which is represented by the stale registration. ■ All the client nodes have crashed simultaneously, due to which fencing keys are not cleared from the CP servers. Consequently, when the nodes restart, the vxfen configuration fails reporting preexisting split brain. These situations are similar to that of preexisting split-brain with coordinator disks, where the problem is solved by the administrator running the `vxfenclearpre` command. A similar solution is required in server-based fencing using the `cpsadm` command. Run the `cpsadm` command to clear a registration on a CP server: `# cpsadm -s cp_server -a unreg_node -c cluster_name -n nodeid` where *cp_server* is the virtual IP address or virtual hostname on which the CP server is listening, *cluster_name* is the VCS name for the VCS cluster, and *nodeid* specifies the node id of VCS cluster node. Ensure that fencing is not already running on a node before clearing its registration on the CP server. After removing all stale registrations, the joiner node will be able to join the cluster.

Adding a node to the secure cluster whose root broker system has failed

If the root broker system of a cluster in secure mode has failed, you can do one of the following before you add a node to the cluster:

■ If you had backed up the AT configuration files after you configured the root broker and set up the security infrastructure, you can recover from a root broker failure. Thus, you can enable the root broker to use the same broker certificates and keys for the clusters that the root broker serves.

See the Symantec Product Authentication Service documentation for more information on backing up the AT configuration files and recovering the failed root broker system.

- If you did not back up the AT configuration files, then you must unconfigure the authentication brokers in the cluster and repeat the secure cluster configuration steps.

To unconfigure the authentication brokers and enable security in the cluster

1. Run the following command on one of the nodes in the cluster and follow the prompts to disable security in the cluster.

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

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

2. On each node , manually stop the vxatd process.

   ```
   # ps -ef | grep vxatd
   # kill -9 vxatd_process_number
   ```

3. On each node, run the following command to unconfigure the authentication broker. For example,

   ```
   galaxy> # vssregctl -l -s
   -b"Security\Authentication\Authentication Broker"
   -t"int" -k"Mode" -v0
   nebula> # vssregctl -l -s
   -b"Security\Authentication\Authentication Broker"
   -t"int" -k"Mode" -v0
   ```

4. Perform the following steps to configure the cluster in secure mode.

   - If you use an external root broker, you must reconfigure the root broker. See "Preparing to configure the clusters in secure mode" on page 89. If you use one of the nodes in the cluster as root broker, proceed to the next step to enable security in the cluster.
   - Run the following command on one of the nodes in the cluster and follow the prompts to enable security in the cluster.

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

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

5 Proceed to add a node to the secure cluster.

See "Adding nodes using the VCS installer" on page 331.

See "Manually adding a node to a cluster" on page 336.

Appendix I

Sample VCS cluster setup diagrams for CP server-based I/O fencing

This appendix includes the following topics:

Configuration diagrams for setting up server-based I/O fencing

The following CP server configuration diagrams can be used as guides when setting up CP server within your configuration:

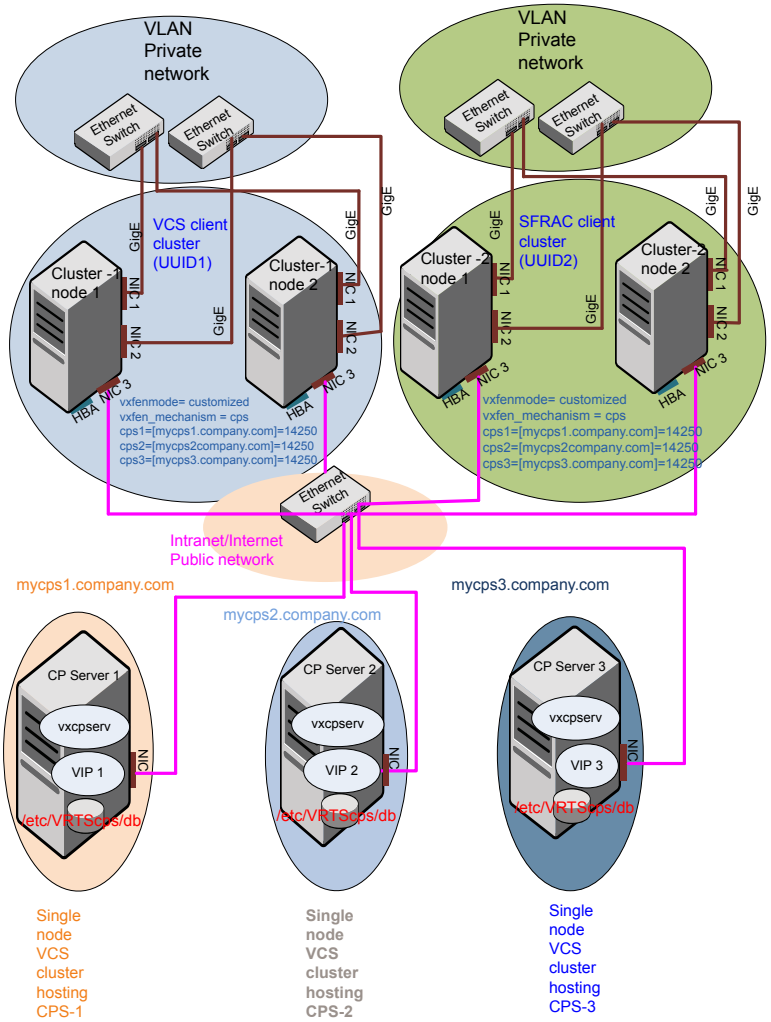
- Two unique client clusters that are served by 3 CP servers:
  See Figure I-1 on page 444.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
- Two node campus cluster that is served be remote CP server and 2 SCSI-3 disks:
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:

Two unique client clusters served by 3 CP servers

Figure I-1 displays a configuration where two unique client clusters are being served by 3 CP servers (coordination points). Each client cluster has its own unique user ID (UUID1 and UUID2).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

Figure I-1 Two unique client clusters served by 3 CP servers



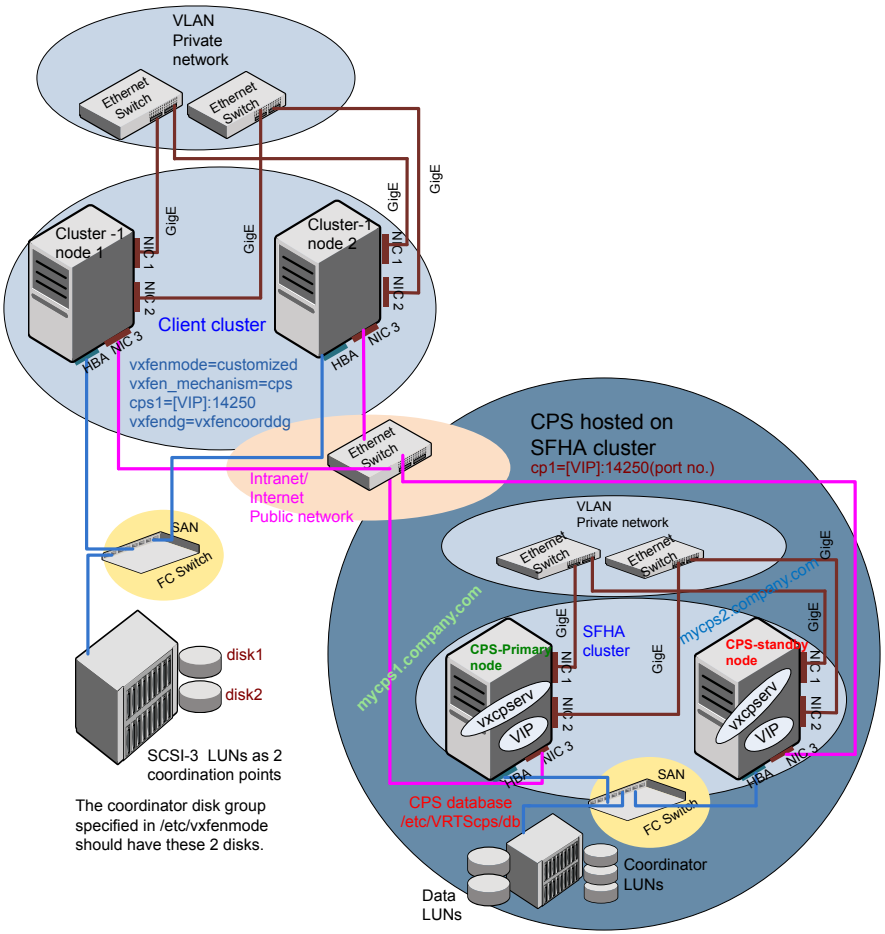
Client cluster served by highly available CPS and 2 SCSI-3 disks

Figure I-2 displays a configuration where a client cluster is served by one highly available CP server and 2 local SCSI-3 LUNs (disks).

In the `vxfenmode` file on the client nodes, `vxfenmode` is set to customized with vxfen mechanism set to `cps`.

The two SCSI-3 disks are part of the disk group vxfencoorddg. The third coordination point is a CP server hosted on an SFHA cluster, with its own shared database and coordinator disks.

Figure I-2 Client cluster served by highly available CP server and 2 SCSI-3 disks



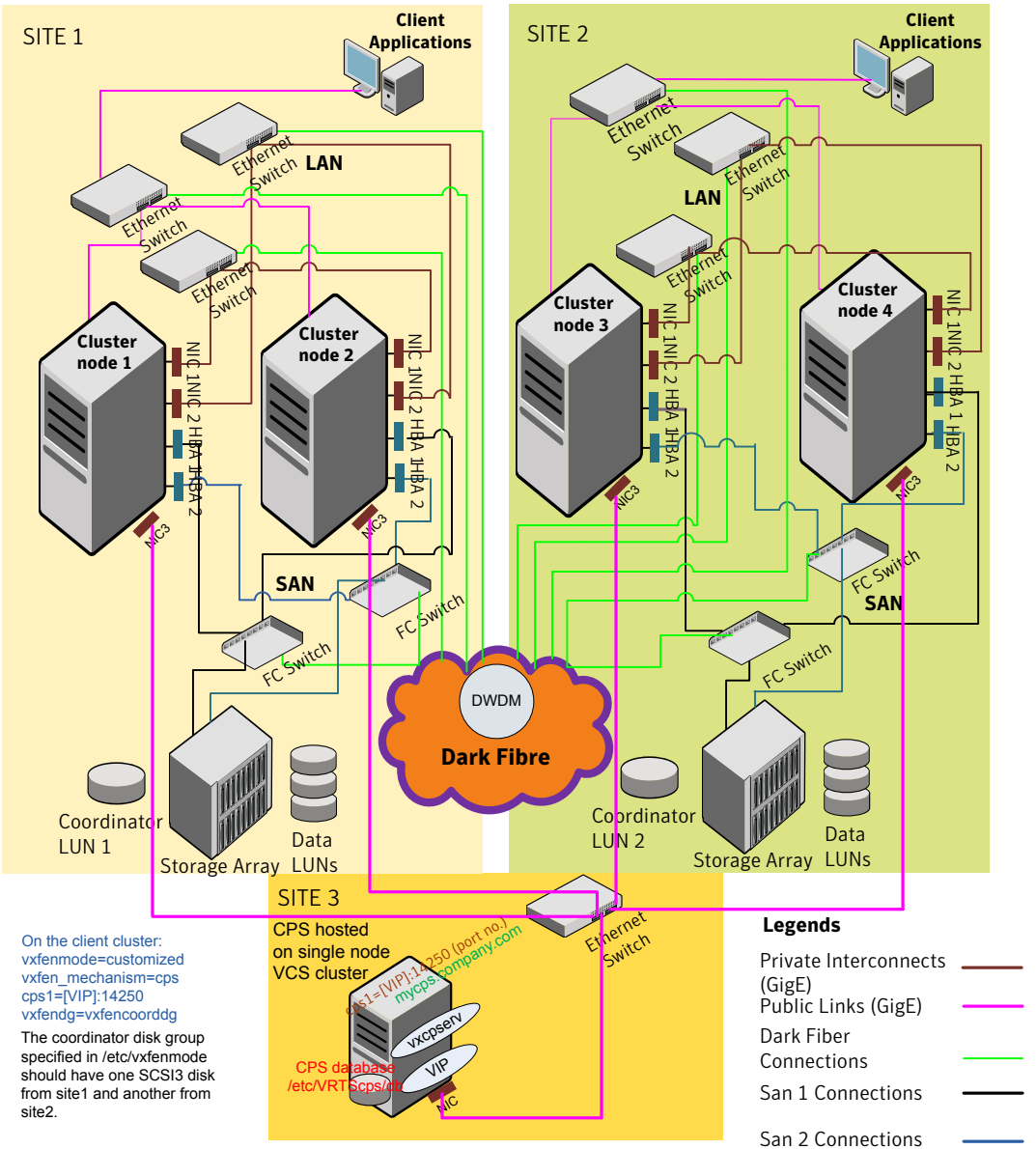
Two node campus cluster served by remote CP server and 2 SCSI-3 disks

Figure I-3 displays a configuration where a two node campus cluster is being served by one remote CP server and 2 local SCSI-3 LUN (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks (one from each site) are part of disk group vxfencoorddg. The third coordination point is a CP server on a single node VCS cluster.

Figure I-3 Two node campus cluster served by remote CP server and 2 SCSI-3



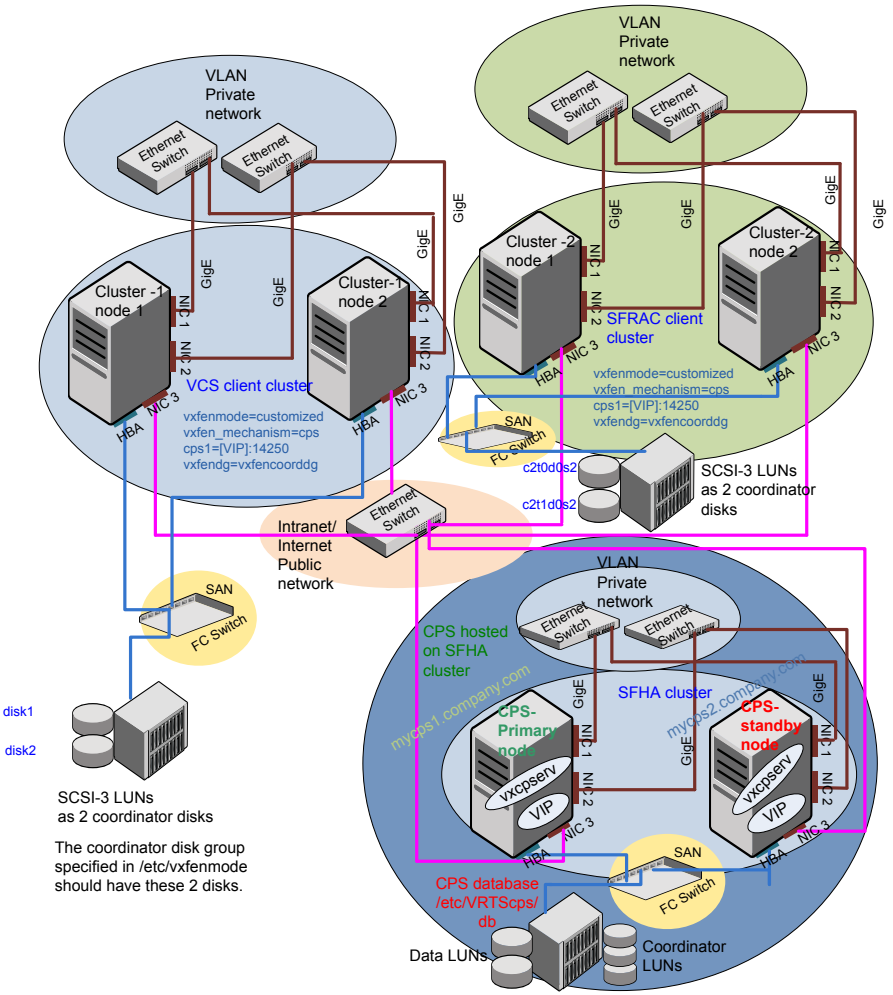
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

Figure I-4 displays a configuration where multiple client clusters are being served by one highly available CP server and 2 local SCSI-3 LUNS (disks).

In the `vxfenmode` file on the client nodes, vxfenmode is set to `customized` with vxfen mechanism set to `cps`.

The two SCSI-3 disks are are part of the disk group vxfencoorddg. The third coordination point is a CP server, hosted on an SFHA cluster, with its own shared database and coordinator disks.

Figure I-4 Multiple client clusters served by highly available CP server and 2 SCSI-3 disks



Appendix J

Reconciling major/minor numbers for NFS shared disks

This appendix includes the following topics:

Reconciling major/minor numbers for NFS shared disks

Your configuration may include disks on the shared bus that support NFS. You can configure the NFS file systems that you export on disk partitions or on Veritas Volume Manager volumes. An example disk partition name is `/dev/dsk/c1t1d0`. An example volume name is `/dev/vx/dsk/shareddg/vol3`. Each name represents the block device on which the file system is to be mounted.

In a VCS cluster, block devices providing NFS service must have the same major and minor numbers on each cluster node. Major numbers identify required device drivers (such as a HP-UX partition or a VxVM volume). Minor numbers identify the specific devices themselves. NFS also uses major and minor numbers to identify the exported file system.

Major and minor numbers must be verified to ensure that the NFS identity for the file system is the same when exported from each node.

Checking major and minor numbers for disk partitions

The following sections describe checking and changing, if necessary, the major and minor numbers for disk partitions used by cluster nodes.

To check major and minor numbers on disk partitions

- Use the following command on all nodes exporting an NFS file system. This command displays the major and minor numbers for the block device.

  ```
  # ls -lL block_device
  ```

  The variable *block_device* refers to a partition where a file system is mounted for export by NFS. Use this command on each NFS file system. For example, type:

  ```
  # ls -lL /dev/dsk/c1t1d0
  ```

  Output on Node A resembles:

  ```
  crw-r-----  1 root  sys  32,1 Dec 3 11:50 /dev/dsk/c1t1d0
  ```

  Output on Node B resembles:

  ```
  crw-r-----  1 root  sys  32,1 Dec 3 11:55 /dev/dsk/c1t1d0
  ```

  Note that the major numbers (32) and the minor numbers (1) match, satisfactorily meeting the requirement for NFS file systems.

To reconcile the major numbers that do not match on disk partitions

1. Reconcile the major and minor numbers, if required. For example, if the output in the previous section resembles the following, perform the instructions beginning step 2:

   Output on Node A:

   ```
   crw-r-----  1 root  sys  32,1 Dec 3 11:50 /dev/dsk/c1t1d0
   ```

   Output on Node B:

   ```
   crw-r-----  1 root  sys  36,1 Dec 3 11:55 /dev/dsk/c1t1d0
   ```

2. Place the VCS command directory in your path. For example:

   ```
   # export PATH=$PATH:/usr/sbin:/sbin:/opt/VRTS/bin
   ```

3 Attempt to change the major number on System B (now 36) to match that of System A (32). Use the command:

```
# haremajor -sd major_number
```

For example, on Node B, enter:

```
# haremajor -sd 32
```

4 If the command succeeds, go to step 8.

5 If the command fails, you may see a message resembling:

```
Error: Preexisting major number 32
These are available numbers on this system: 128...
Check /etc/name_to_major on all systems for
available numbers.
```

6 Notice that the number 36 (the major number on Node A) is not available on Node B. Run the `haremajor` command on Node B and change it to 128,

```
# haremajor -sd 128
```

7 Run the same command on Node A. If the command fails on Node A, the output lists the available numbers. Rerun the command on both nodes, setting the major number to one available to both.

8 Reboot each system on which the command succeeds.

9 Proceed to reconcile the major numbers for your next partition.

To reconcile the minor numbers that do not match on disk partitions

1 In the example, the minor numbers are `1` and `3` and are reconciled by setting to 30 on each node.

2 Type the following command on both nodes using the name of the block device:

```
# ls -1 /dev/dsk/c1t1d0
```

Output from this command resembles the following on Node A:

```
lrwxrwxrwx  1 root  root  83 Dec 3 11:50
 /dev/dsk/c1t1d0         -> ../../
 devices/sbus@1f,0/QLGC,isp@0,10000/sd@1,0:d,raw
```

The `device name` (in bold) includes the slash following the word `devices`, and continues to, but does not include, the colon.

3 Type the following command on both nodes to determine the instance numbers that the SCSI driver uses:

```
# grep sd /etc/path_to_inst | sort -n -k 2,2
```

Output from this command resembles the following on Node A:

```
"/sbus@1f,0/QLGC,isp@0,10000/sd@0,0" 0 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@1,0" 1 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@2,0" 2 "sd"
"/sbus@1f,0/QLGC,isp@0,10000/sd@3,0" 3 "sd"
.
.
"/sbus@1f,0/SUNW,fas@e,8800000/sd@d,0" 27 "sd"
"/sbus@1f,0/SUNW,fas@e,8800000/sd@e,0" 28 "sd"
"/sbus@1f,0/SUNW,fas@e,8800000/sd@f,0" 29 "sd"
```

In the output, the instance numbers are in the second field.

The instance number that is associated with the device name that matches the name for Node A displayed in step 2, is "1."

4 Compare instance numbers for the device in the output on each node.

After you review the instance numbers, perform one of the following tasks:

- If the instance number from one node is unused on the other— it does not appear in the output of step 3—edit `/etc/path_to_inst`.
  You edit this file to make the second node's instance number similar to the number of the first node.
- If the instance numbers in use on both nodes, edit `/etc/path_to_inst` on both nodes. Change the instance number that is associated with the device name to an unused number. The number needs to be greater than the highest number that other devices use. For example, the output of step 3 shows the instance numbers that all devices use (from 0 to 29). You edit the file `/etc/path_to_inst` on each node and reset the instance numbers to 30.

5 Type the following command to reboot each node on which `/etc/path_to_inst` was modified:

```
# reboot -- -rv
```

Checking the major and minor number for VxVM volumes

The following sections describe checking and changing, if necessary, the major and minor numbers for the VxVM volumes that cluster systems use.

To check major and minor numbers on VxVM volumes

1. Place the VCS command directory in your path. For example:

   ```
   # export PATH=$PATH:/usr/sbin:/sbin:/opt/VRTS/bin
   ```

2. To list the devices, use the `ls -lL` *block_device* command on each node:

   ```
   # ls -lL /dev/vx/dsk/shareddg/vol3
   ```

   On Node A, the output may resemble:

   ```
   brw-------   1 root  root  32,43000 Mar 22 16:4 1
   /dev/vx/dsk/shareddg/vol3
   ```

   On Node B, the output may resemble:

   ```
   brw-------   1 root  root  36,43000 Mar 22 16:4 1
   /dev/vx/dsk/shareddg/vol3
   ```

3. Import the associated shared disk group on each node.

4 Use the following command on each node exporting an NFS file system. The command displays the major numbers for `vxio` and `vxspec` that Veritas Volume Manager uses . Note that other major numbers are also displayed, but only `vxio` and `vxspec` are of concern for reconciliation:

```
# grep vx /etc/name_to_major
```

Output on Node A:

```
vxdmp 30
vxio 32
vxspec 33
vxfen 87
vxglm 91
```

Output on Node B:

```
vxdmp 30
vxio 36
vxspec 37
vxfen 87
vxglm 91
```

5 To change Node B's major numbers for `vxio` and `vxspec` to match those of Node A, use the command:

```
haremajor -vx major_number_vxio major_number_vxspec
```

For example, enter:

```
# haremajor -vx 32 33
```

If the command succeeds, proceed to step 8. If this command fails, you receive a report similar to the following:

```
Error: Preexisting major number 32
These are available numbers on this system: 128...
Check /etc/name_to_major on all systems for
available numbers.
```

6 If you receive this report, use the `haremajor` command on Node A to change the major number (`32/33`) to match that of Node B (`36/37`). For example, enter:

```
# haremajor -vx 36 37
```

If the command fails again, you receive a report similar to the following:

```
Error: Preexisting major number 36
These are available numbers on this node: 126...
Check /etc/name_to_major on all systems for
available numbers.
```

7 If you receive the second report, choose the larger of the two available numbers (in this example, `128`). Use this number in the `haremajor` command to reconcile the major numbers. Type the following command on both nodes:

```
# haremajor -vx 128 129
```

8 Reboot each node on which `haremajor` was successful.

9 If the minor numbers match, proceed to reconcile the major and minor numbers of your next NFS block device.

10 If the block device on which the minor number does not match is a volume, consult the `vxdg`(1M) manual page. The manual page provides instructions on reconciling the Veritas Volume Manager minor numbers, and gives specific reference to the `reminor` option.

Node where the vxio driver number have been changed require rebooting.

Reconciling major/minor numbers for NFS shared disks

Index

M

N

O

P

R

S

T

U

V

W