Veritas™ Cluster Server Installation Guide

Solaris

6.0 Platform Release 1

March 2012

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: 6.0 PR1

Document version: 6.0PR1.0

Legal Notice

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

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:

doc_feedback@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

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.

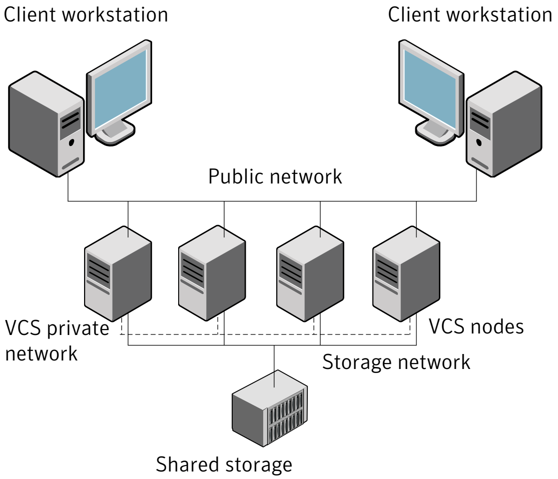
About VCS basics

A single VCS cluster consists of multiple systems that are connected in various combinations to storage devices. When a system is part of a VCS cluster, it is called 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, nodes that join or leave the cluster, and failed nodes. The private network requires two communication channels to guard against network partitions.

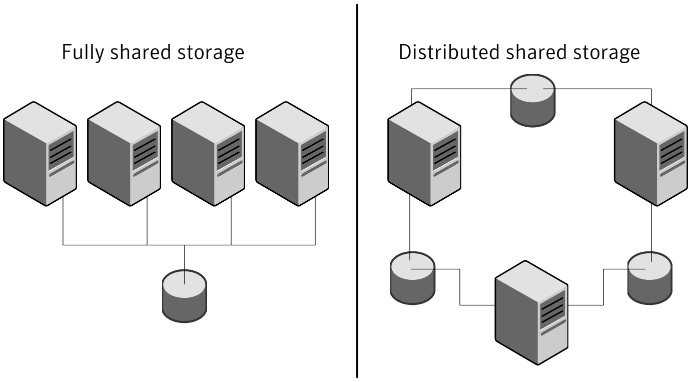
About shared storage

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 globally ordered message that is required to maintain a synchronized state among the nodes.

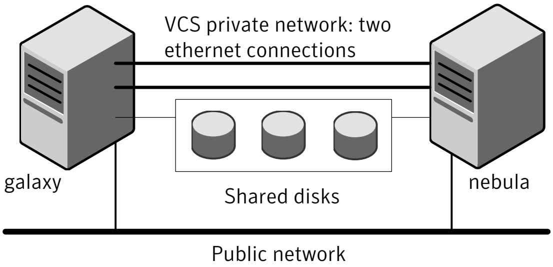
About network channels for heartbeating

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 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 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. However, if you have I/O fencing enabled in your cluster, you can still configure GAB to automatically seed the cluster even when some cluster nodes are unavailable.

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

About VCS features

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

VCS notifications	See "About VCS notifications" on page 23.
VCS global clusters	See "About global clusters" on page 23.
I/O fencing	See "About I/O fencing" on page 23.

About VCS notifications

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

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

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

About global clusters

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

I/O fencing coordination points can be coordinator disks or coordination point servers (CP servers) or both. You can configure disk-based or server-based I/O fencing:

Disk-based I/O fencing	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.
Server-based I/O fencing	I/O fencing that uses at least one CP server system is referred to as server-based I/O fencing. Server-based fencing can include only CP servers, or a mix of CP servers and coordinator disks. Server-based I/O fencing ensures data integrity in multiple clusters. In virtualized environments that do not support SCSI-3 PR, VCS supports non-SCSI-3 server-based I/O fencing.

See "About planning to configure I/O fencing" on page 83.

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:

Veritas Operations Manager	See "About Veritas Operations Manager" on page 25.
Cluster Manager (Java console)	See "About Cluster Manager (Java Console)" on page 25.
VCS Simulator	See About VCS Simulator on page 25.

About Veritas Operations Manager

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

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

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

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

If you want to manage a single cluster using Cluster Manager (Java Console), a version is available for download from http://go.symantec.com/vcsm_download. You cannot manage the new features of this release using the Java Console. Veritas Cluster Server Management Console is deprecated.

About Cluster Manager (Java Console)

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

See *Veritas Cluster Server Administrator's Guide*.

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

About 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 Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

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

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

To access SORT, go to:

https://sort.symantec.com

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 corrective action would cause a split-brain situation.

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

- Broken set of private networks
  If a system in a two-node cluster fails, the system stops sending heartbeats over the private interconnects. The remaining node then takes corrective action. The failure of the private interconnects, instead of the actual nodes, presents identical symptoms and causes each node to determine its peer has departed. This situation typically results in data corruption because both nodes try to take control of data storage in an uncoordinated manner
- System that appears to have a system-hang
  If a system is so busy that it appears to stop responding, the other nodes could declare it as dead. This declaration may also occur for the nodes that use the hardware that supports a "break" and "resume" function. When a node drops

to PROM level with a break and subsequently resumes operations, the other nodes may declare the system dead. They can declare it dead even if the system later returns and begins write operations.

I/O fencing is a feature that prevents data corruption in the event of a communication breakdown in a cluster. 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 83.

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-SCSI-3 server-based I/O fencing in such environments. Non-SCSI-3 fencing uses CP servers as coordination points with some additional configuration changes to support I/O fencing in such environments.

See "Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program" on page 135.

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 28.
- Coordination points—Act as a global lock during membership changes
  See "About coordination points" on page 28.

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. VCS prevents split-brain when vxfen races for control of the coordination points and the winner partition fences the ejected nodes from accessing the data disks.

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 either be disks or 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.
  You can configure coordinator disks to use Veritas Volume Manager Dynamic Multi-pathing (DMP) feature. Dynamic Multi-pathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. So, you can configure I/O fencing to use either DMP devices or the underlying raw character devices. I/O fencing uses SCSI-3 disk policy that is either raw or dmp based on the disk device that you use. The disk policy is dmp by default.
  See the *Veritas Storage Foundation 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 active VCS 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 136.

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://www.symantec.com/docs/TECH170013
  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/TECH164885
- You can install VCS on clusters of up to 64 systems.

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 64 SPARC or x64 systems running Oracle Solaris 11 as appropriate.
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).
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). See "About planning to configure I/O fencing" on page 83.
Disk space	**Note:** VCS may require more temporary disk space during installation than the specified disk space.
Ethernet controllers	In addition to the built-in public Ethernet controller, VCS requires at least one more Ethernet interface per system. Symantec recommends two additional network interfaces for private interconnects. You can also configure aggregated interfaces. Symantec recommends that you turn off the spanning tree algorithm on the switches used to connect private network interfaces..
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.

Disk space requirements

Before installing your products, confirm that your system has enough free disk space.

Use the script-based installer `-precheck` option to determine if there is sufficient space.

```
# ./installer -precheck
```

If you have downloaded VCS, use the following command:

```
# ./installvcs -precheck
```

Supported operating systems

For information on supported operating systems, see the *Veritas Cluster Server Release Notes*.

Supported software for VCS

VCS supports the following volume managers and file systems:

- Veritas Storage Foundation (SF): Veritas Volume Manager (VxVM) with Veritas File System (VxFS)

  VCS 6.0 PR1 supports the following versions of SF:

  - SF 6.0PR1
    - VxVM 6.0PR1 with VxFS 6.0 PR1

Note: VCS supports the previous and the next versions 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 34.
- CP servers

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-SCSI-3 server-based fencing.

Coordinator disk requirements for I/O fencing

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

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

CP server requirements

VCS 6.0 PR1 clusters (application clusters) support coordination point servers (CP servers) which are hosted on the following VCS and SFHA versions:

- VCS 6.0PR1, VCS 6.0, 5.1SP1, or 5.1 single-node cluster
  Single-node VCS clusters with VCS 5.1 SP1 RP1 and later or VCS 6.0 and later that hosts CP server does not require LLT and GAB to be configured.
- SFHA 6.0PR1, SFHA 6.0, 5.1SP1, or 5.1 cluster

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*.

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

Table 2-2 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 ■ 10 MB in /etc (for the CP server database) See “Disk space requirements” on page 33.
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.
Network	Network hardware capable of providing TCP/IP connection between CP servers and VCS clusters (application clusters).

Table 2-3 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 2-3 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 6.1 and 7.1 - HP-UX 11i v3 - Linux: - RHEL 5 - RHEL 6 - SLES 10 - SLES 11 - Solaris 10 - Oracle Solaris 11 Review other details such as supported operating system levels and architecture for the supported operating systems. See the *Veritas Cluster Server Release Notes* or the *Veritas Storage Foundation High Availability Release Notes* 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.

  Symantec recommends that you configure multiple network paths to access a CP server. If a network path fails, CP server does not require a restart and continues to listen on one of the other available virtual IP addresses.
- 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 and network latency 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 communication between the VCS cluster (application cluster) and the CP server, review the following support matrix:

	CP server in secure mode	CP server in non-secure mode
VCS cluster in secure mode	Yes	Yes
VCS cluster in non-secure mode	Yes	Yes
CP server cluster in secure mode	Yes	No
CP server cluster in non-secure mode	No	Yes

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.
- 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-SCSI-3 I/O fencing requirements

Supported virtual environment for non-SCSI-3 fencing:

- Oracle Solaris 11
  Oracle VM Server for SPARC 2.1
  Guest operating system: Solaris 10, Oracle Solaris 11

Make sure that you also meet the following requirements to configure non-SCSI-3 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 supports cluster configurations with up to 64 nodes.

Discovering product versions and various requirement information

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

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

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

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

To run the version checker

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

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

Chapter 3

Planning to install VCS

This chapter includes the following topics:

- VCS installation methods
- Typical VCS cluster setup models

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.
Automated installation using the VCS response files	Use response files to perform unattended installations. You can generate a response file in one of the following ways: ■ Use the automatically generated response file after a successful installation. ■ Use the -makeresponsefile option to create a response file.

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 packages 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
- VCS configuration in secure mode
- 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 53.

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

See “Preparing to uninstall VCS” on page 193.

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 66.
- Upgrade VCS if a previous version of VCS currently runs on a cluster.
- Start or stop VCS processes
  See “Starting and stopping processes for the Veritas products ” on page 288.
- Enable or disable a cluster to run in secure mode
  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 127.
See “Setting up server-based I/O fencing using installvcs program” on page 134.
See “Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program” on page 135.

- Create a single-node cluster
  See “Creating a single-node cluster using the installer program” on page 259.
- Add a node to an existing cluster
  See “Adding nodes using the VCS installer” on page 215.
- Perform automated installations using the values that are stored in a configuration file.
  See “Installing VCS using response files” on page 141.
  See “Configuring VCS using response files” on page 147.

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 packages 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 193.

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.

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, 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 141.
- To upgrade VCS on multiple systems in a large VCS cluster.
- To uninstall VCS from multiple systems in a large VCS cluster.
  See "Uninstalling VCS using response files" on page 199.

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
- VCS clusters in secure mode
  See "Typical configuration of VCS clusters in secure mode" on page 44.
- VCS clusters centrally managed using Veritas Operations Manager (VOM)
  See "Typical configuration of VOM-managed VCS clusters" on page 45.
- VCS clusters with I/O fencing for data protection
- 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 Solaris SPARC systems.

Figure 3-1 Typical two-node VCS cluster (Solaris SPARC systems)

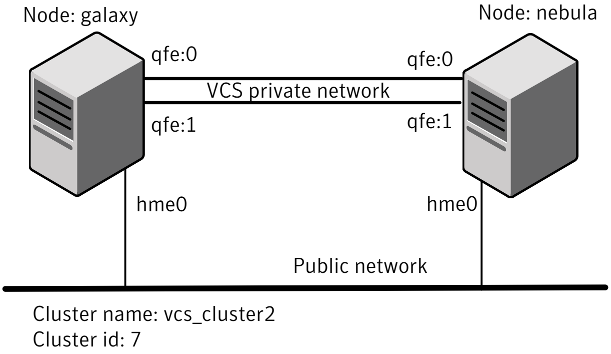
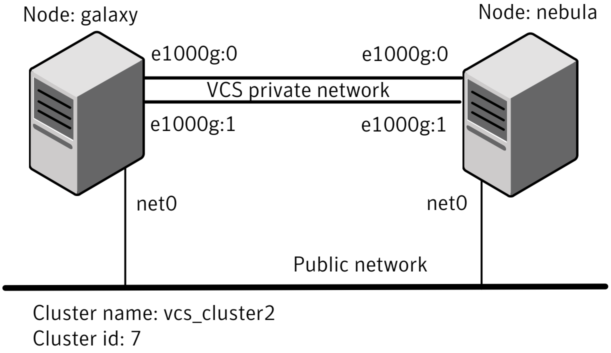


Figure 3-2 illustrates a a simple VCS cluster setup with two Solaris x64 systems.

Figure 3-2 Typical two-node VCS cluster (Solaris x64 systems)

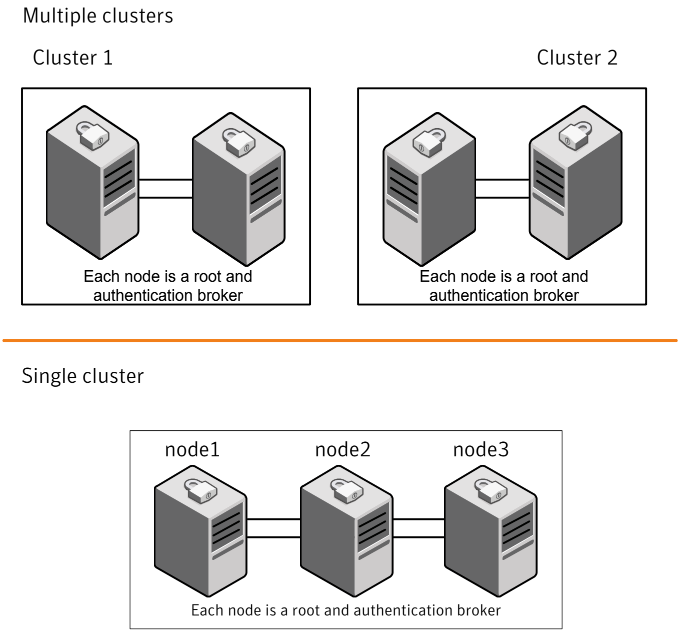


Typical configuration of VCS clusters in secure mode

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

Figure 3-3 illustrates typical configuration of VCS clusters in secure mode.

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


Multiple clusters
Cluster 1
Cluster 2
Each node is a root and authentication broker
Each node is a root and authentication broker
Single cluster
node1
node2
node3
Each node is a root and authentication broker

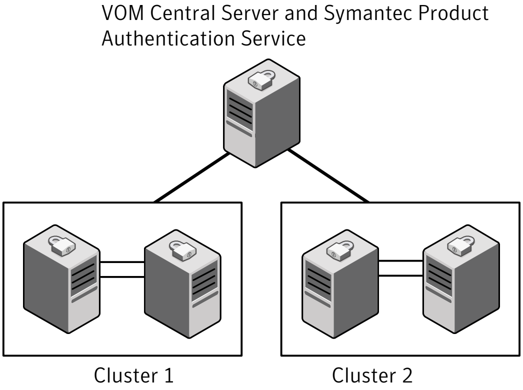
Typical configuration of VOM-managed VCS clusters

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

See "About Veritas Operations Manager" on page 25.

Figure 3-4 illustrates a typical setup of VCS clusters that are centrally managed using Veritas Operations Manager.

Figure 3-4 Typical configuration of VOM-managed clusters


VOM Central Server and Symantec Product Authentication Service
Cluster 1
Cluster 2

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, such as Veritas Operations Manager (VOM). If you do not comply with the above terms, continuing to use the Symantec product is a violation of your end user license agreement, and results in warning messages.
For more information about keyless licensing, see the following URL:
http://go.symantec.com/sfhakeyless

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See 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 49.
  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 47.

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

See "Installing Veritas product license keys" on page 49.

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin

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

Section 2

Preinstallation tasks

Chapter 5

Preparing to install VCS

This chapter includes the following topics:

- About preparing to install VCS
- Performing preinstallation tasks
- Getting your VCS installation and configuration information ready

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 31.

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 48.
Set up the private network.	See "Setting up the private network" on page 54.
Enable communication between systems.	See "Setting up inter-system communication" on page 281.

Table 5-1 Preinstallation tasks *(continued)*

Task	Reference
Set up ssh on cluster systems.	See "Setting up ssh on cluster systems" on page 281.
Set up shared storage for I/O fencing (optional)	See "Setting up shared storage" on page 58.
Creating root user	See "Creating root user" on page 62.
Set the PATH and the MANPATH variables.	See "Setting the PATH variable" on page 63. See "Setting the MANPATH variable" on page 63.
Disable the abort sequence on SPARC systems.	See "Disabling the abort sequence on SPARC systems" on page 63.
Review basic instructions to optimize LLT media speeds.	See "Optimizing LLT media speed settings on private NICs" on page 65.
Review guidelines to help you set the LLT interconnects.	See "Guidelines for setting the media speed of the LLT interconnects" on page 65.
Install the compatibility or ucb packages from the Oracle Solaris repository.	For instructions, see the Oracle documentation.
Prepare zone environments	See "Preparing zone environments" on page 65.
Mount the product disc	See "Mounting the product disc" on page 65.
Verify the systems before installation	See "Performing automated preinstallation check" on page 66.

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. However, Oracle systems assign the same MAC address to all interfaces by default. Thus, connecting two or more interfaces to a network switch can cause problems.

For example, consider the following case where:

- The IP address is configured on one interface and LLT on another
- Both interfaces are connected to a switch (assume separate VLANs)

The duplicate MAC address on the two switch ports can cause the switch to incorrectly redirect IP traffic to the LLT interface and vice versa. To avoid this issue, configure the system to assign unique MAC addresses by setting the `eeprom(1M)` parameter local-mac-address to true.

The following products make extensive use of the private cluster interconnects for distributed locking:

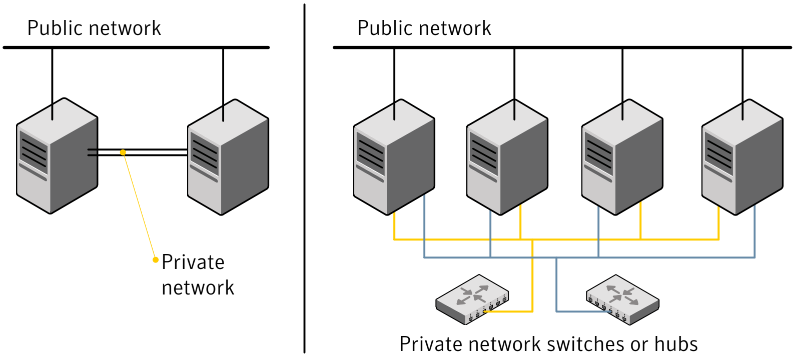
- Veritas Storage Foundation Cluster File System (SFCFS)
- Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)

Symantec recommends network switches for the SFCFS and the SF Oracle RAC clusters due to their performance characteristics.

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.

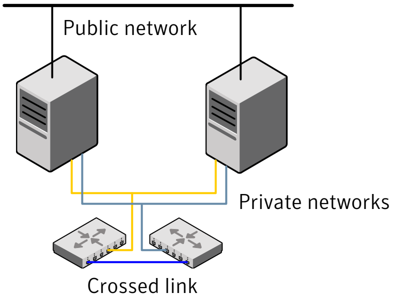
Figure 5-1 Private network setups: two-node and four-node clusters



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 Ethernet controllers 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. Configure the Ethernet devices that are used for the private network such that the autonegotiation protocol is not used. You can achieve a more stable configuration with crossover cables if the autonegotiation protocol is not used.

To achieve this stable configuration, do one of the following:

- Edit the /etc/system file to disable autonegotiation on all Ethernet devices system-wide.
- Create a qfe.conf or bge.conf file in the /kernel/drv directory to disable autonegotiation for the individual devices that are used for private network.

Refer to the Oracle Ethernet driver product documentation for information on these methods.

5 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.

About using ssh or rsh with the Veritas installer

The installer uses passwordless secure shell (ssh) or remote shell (rsh) communications among systems. The installer uses the ssh or rsh 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. The ssh or rsh 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 rsh configuration from the systems.

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

- When you add new nodes to an existing cluster.
- When the nodes are in a subcluster during a phased upgrade.
- When you perform installer sessions using a response file.

See "Setting up inter-system communication" on page 281.

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 83.

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

Setting up shared storage: SCSI disks

When SCSI devices are used for shared storage, the SCSI address or SCSI initiator ID of each node must be unique. Since each node typically has the default SCSI address of "7," the addresses of one or more nodes must be changed to avoid a conflict. In the following example, two nodes share SCSI devices. The SCSI address of one node is changed to "5" by using `nvedit` commands to edit the `nvramrc` script.

If you have more than two systems that share the SCSI bus, do the following:

- Use the same procedure to set up shared storage.
- Make sure to meet the following requirements:
  - The storage devices have power before any of the systems
  - Only one node runs at one time until each node's address is set to a unique value

To set up shared storage

1. Install the required SCSI host adapters on each node that connects to the storage, and make cable connections to the storage.

   Refer to the documentation that is shipped with the host adapters, the storage, and the systems.

2. With both nodes powered off, power on the storage devices.

3. Power on one system, but do not allow it to boot. If necessary, halt the system so that you can use the ok prompt.

   Note that only one system must run at a time to avoid address conflicts.

4. Find the paths to the host adapters:

   ```
   {0} ok show-disks
   ...b) /sbus@6,0/QLGC,isp@2,10000/sd
   ```

   The example output shows the path to one host adapter. You must include the path information without the "/sd" directory, in the `nvramrc` script. The path information varies from system to system.

5. Edit the `nvramrc` script on to change the scsi-initiator-id to 5. (The *Solaris OpenBoot 3.x Command Reference Manual* contains a full list of `nvedit` commands and keystrokes.) For example:

   ```
   {0} ok nvedit
   ```

   As you edit the script, note the following points:

   - Each line is numbered, 0:, 1:, 2:, and so on, as you enter the `nvedit` commands.
   - On the line where the scsi-initiator-id is set, insert exactly one space after the first quotation mark and before scsi-initiator-id.

   In this example, edit the nvramrc script as follows:

   ```
   0: probe-all
   1: cd /sbus@6,0/QLGC,isp@2,10000
   2: 5 " scsi-initiator-id" integer-property
   3: device-end
   4: install-console
   5: banner
   6: <CTRL-C>
   ```

6 Store the changes you make to the `nvramrc` script. The changes you make are temporary until you store them.

```
{0} ok nvstore
```

If you are not sure of the changes you made, you can re-edit the script without risk before you store it. You can display the contents of the `nvramrc` script by entering:

```
{0} ok printenv nvramrc
```

You can re-edit the file to make corrections:

```
{0} ok nvedit
```

Or, discard the changes if necessary by entering:

```
{0} ok nvquit
```

7 Instruct the OpenBoot PROM Monitor to use the `nvramrc` script on the node.

```
{0} ok setenv use-nvramrc? true
```

8 Reboot the node. If necessary, halt the system so that you can use the ok prompt.

9 Verify that the scsi-initiator-id has changed. Go to the ok prompt. Use the output of the show-disks command to find the paths for the host adapters. Then, display the properties for the paths. For example:

```
{0} ok show-disks
...b) /sbus@6,0/QLGC,isp@2,10000/sd
{0} ok cd /sbus@6,0/QLGC,isp@2,10000
{0} ok .properties
scsi-initiator-id     00000005
```

Permit the system to continue booting.

10 Boot the second node. If necessary, halt the system to use the ok prompt. Verify that the scsi-initiator-id is 7. Use the output of the `show-disks` command to find the paths for the host adapters. Then, display the properties for that paths. For example:

```
{0} ok show-disks
...b) /sbus@6,0/QLGC,isp@2,10000/sd
{0} ok cd /sbus@6,0/QLGC,isp@2,10000
{0} ok .properties
scsi-initiator-id      00000007
```

Permit the system to continue booting.

Setting up shared storage: Fibre Channel

Perform the following steps to set up Fibre Channel.

To set up shared storage

1 Install the required FC-AL controllers.

2 Connect the FC-AL controllers and the shared storage devices to the same hub or switch.

All systems must see all the shared devices that are required to run the critical application. If you want to implement zoning for a fibre switch, make sure that no zoning prevents all systems from seeing all these shared devices.

3 Boot each system with the reconfigure devices option:

```
 ok boot -r
```

4 After all systems have booted, use the `format(1m)` command to verify that each system can see all shared devices.

If Volume Manager is used, the same number of external disk devices must appear, but device names (c#t#d#s#) may differ.

If Volume Manager is not used, then you must meet the following requirements:

- The same number of external disk devices must appear.
- The device names must be identical for all devices on all systems.

Creating root user

On Oracle Solaris 11, you need to change the root role into a user as you cannot directly log in as root user.

To change root role into a user

1. Log in as local user and assume the root role.

   ```
   % su  - root
   ```

2. Remove the root role from local users who have been assigned the role.

   ```
   # roles admin

   root

   # usermod -R " " admin
   ```

3. Change the root role into a user.

   ```
   # rolemod -K type=normal root
   ```

4. Verify the change.

   - `# getent user_attr root`

     ```
     root::::auths=solaris.*;profiles=All;audit_flags=lo\
     :no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
     ```

     If the `type` keyword is missing in the output or is equal to normal, the account is not a role.

   - `# userattr type root`

     If the output is empty or lists normal, the account is not a role.

Note: For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

Note: After installation, you may want to change root user into root role to allow local users to assume the root role.

See "Changing root user into root role" on page 177.

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), Bourne-again Shell (bash), or Korn shell (ksh), type:

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

- For the C Shell (csh) or enhanced C Shell (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), Bourne-again Shell (bash), or Korn shell (ksh), type:

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

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

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

Disabling the abort sequence on SPARC systems

Most UNIX operating systems provide a method to perform a "break" or "console abort." The inherent problem when you abort a hung system is that it ceases to heartbeat in the cluster. When other cluster members believe that the aborted node is a failed node, these cluster members may begin corrective action.

Keep the following points in mind:

- The only action that you must perform following a system abort is to reset the system to achieve the following:
  - Preserve data integrity
  - Prevent the cluster from taking additional corrective actions
- Do not resume the processor as cluster membership may have changed and failover actions may already be in progress.
- To remove this potential problem on SPARC systems, you should alias the `go` function in the OpenBoot eeprom to display a message.

To alias the go function to display a message

1 At the ok prompt, enter:

```
nvedit
```

2 Press Ctrl+L to display the current contents of the nvramrc buffer.

3 Press Ctrl+N until the editor displays the last line of the buffer.

4 Add the following lines exactly as shown. Press Enter after adding each line.

```
." Aliasing the OpenBoot 'go' command! "
: go ." It is inadvisable to use the 'go' command in a clustered
environment. " cr
." Please use the 'power-off' or 'reset-all' commands instead. "
cr
." Thank you, from your friendly neighborhood sysadmin. " ;
```

5 Press Ctrl+C to exit the nvramrc editor.

6 To verify that no errors exist, type the `nvrun` command. You should see only the following text:

```
Aliasing the OpenBoot 'go' command!
```

7 Type the `nvstore` command to commit your changes to the non-volatile RAM (NVRAM) for use in subsequent reboots.

8 After you perform these commands, at reboot you see this output:

```
Aliasing the OpenBoot 'go' command! go isn't unique.
```

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.

Preparing zone environments

Note the following point when you install or upgrade VCS in a zone environment.

With Oracle Solaris 11, after installing packages in the global zone, you need to install the required packages in the non-global zone.

See "Manually installing packages on solaris brand non-global zones" on page 81.

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 into a DVD drive that is connected to your system.

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

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

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

Where c0t6d0s2 is the default address for the disc drive.

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 ...
```

You can also run the `installer -precheck` command.

See “Symantec Operations Readiness Tools” on page 26.

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 /cdrom/cdrom0/cluster_server
```

2 Start the preinstallation check:

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

The program proceeds in a noninteractive mode to examine the systems for licenses, packages, 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.

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 packages.

Table 5-2 Information to install the VCS packages

Information	Description and sample value	Your value
System names	The system names where you plan to install VCS Example: **galaxy**, **nebula**	
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 47. 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 48.	
Decide which packages to install	■ Minimum packages—provides basic VCS functionality. ■ Recommended packages—provides full functionality of VCS without advanced features. ■ All packages—provides advanced feature functionality of VCS. The default option is to install the recommended packages.	

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: **my_cluster**	
A unique ID number for the cluster	A number in the range of 0-65535. If multiple distinct and separate clusters share the same network, then each cluster must have a unique cluster ID. Example: **12133**	

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 263.	
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.	

Table 5-4 Information you need to configure VCS private heartbeat links *(continued)*

Information	Description and sample value	Your value
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 hme0 for SPARC and net0 for x64. For example on a SPARC system: `qfe0, qfe1` For example on an x64 system: `e1000g1, e1000g2` ■ 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: hme0	
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	

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

Information	Description and sample value	Your value
The prefix for the virtual IPv6 address	The prefix length for the virtual IPv6 address. Example: 64	

Table 5-6 lists the information you need to add VCS users.

Table 5-6 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**	
User passwords	VCS passwords are restricted to 255 characters. Enter the password at the prompt. **Note:** VCS leverages native authentication in secure mode. Therefore, user passwords are not needed in secure mode.	
To decide user privileges	Users have three levels of privileges: Administrator, Operator, or Guest. Example: Administrator	

Table 5-7 lists the information you need to configure SMTP email notification (optional).

Table 5-7 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. Examples: **hme0**	
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 5-7 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: ■ Information VCS sends notifications for important events that exhibit normal behavior. ■ Warning VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events. ■ Error VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events. ■ 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: **Error**	

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

Table 5-8 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. Examples: **hme0**	
The port number for the SNMP trap daemon	The default port number is 162.	
The system name for each SNMP console	Example: **saturn**	

Table 5-8 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: ■ Information VCS sends notifications for important events that exhibit normal behavior. ■ Warning VCS sends notifications for events that exhibit any deviation from normal behavior. Notifications include both Warning and Information type of events. ■ Error VCS sends notifications for faulty behavior. Notifications include both Error, Warning, and Information type of events. ■ 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: **Error**	

Table 5-9 lists the information you need to configure global clusters (optional).

Table 5-9 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. For example for SPARC systems: **`hme0`** For example for x64 systems: **`net0`**	
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 5-9 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**	

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

See “About planning to configure I/O fencing” on page 83.

Section 3

Installation using the script-based installer

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 65.

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 /cdrom/cdrom0/cluster_server
```

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_6.0.pdf
file present on media? [y,n,q,?] y
```

4 Choose the VCS packages that you want to install.

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

`1` Installs only the minimal required VCS packages that provides basic functionality of the product.

`2` Installs the recommended VCS packages that provides complete functionality of the product. This option does not install the optional VCS packages.

Note that this option is the default.

`3` Installs all the VCS packages.

You must choose this option to configure any optional VCS feature.

`4` Displays the VCS packages for each option.

```
Select the packages 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 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 259.

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 rsh.
- 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.
- Makes sure the systems install from the global zone.
- 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 6.0 PR1.
- 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 packages already exists on a system.
  If the current version of any package exists, the installer removes the package from the installation list for the system. If a previous version of any package exists, the installer replaces the package with the current version.

6 Review the list of packages and patches that the installer would install on each node.

The installer installs the VCS packages and patches 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 103.

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 The installer checks for online updates and provides an installation summary.

12 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 packages 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 141.

Manually installing packages on solaris brand non-global zones

With Oracle Solaris 11, you need to manually install VCS packages inside non-global zones. The native non-global zones are called solaris brand zones.

1. Ensure that the SMF service, `svc:/application/pkg/system-repository:default` is online on the global zone.

   ```
   # svcs svc:/application/pkg/system-repository
   ```

2. Log on to the non-global zone as a superuser.
3. Copy the `VRTSpkgs.p5p` package from the pkgs directory from the installation media to the non-global zone.
4. Add a file-based repository in the non-global zone.

   ```
   # pkg set-publisher -P -g /<packagelocationpath>/VRTSpkgs.p5p Symantec
   ```

5. Install the required packages.

```
# pkg install VRTSperl VRTSvlic VRTSvcs VRTSvcsag VRTSvcsea
```

6. Remove the publisher on the non-global zone.

```
# pkg unset-publisher Symantec
```

Note: Perform Steps 2 through 6 on each non-global zone.

Manually installing packages on solaris10 brand zones

You need to manually install VCS 6.0 packages inside the solaris10 brand zones.

1. Boot the zone.
2. Log on to the solaris10 brand zone as a super user.
3. Install the following VCS packages on the brand zone.
   - `VRTSperl`
   - `VRTSvcs`
   - `VRTSvcsag`
   - `VRTSvcsea`

Note: Perform Steps 1 through 3 on each solaris10 brand zone.

Chapter 7

Preparing to configure VCS

This chapter includes the following topics:

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 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. Symantec recommends the use of single CP server-based fencing only in test environments.

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

Figure 7-1 illustrates a high-level flowchart to configure I/O fencing for the VCS cluster.

Figure 7-1 Workflow to configure I/O fencing

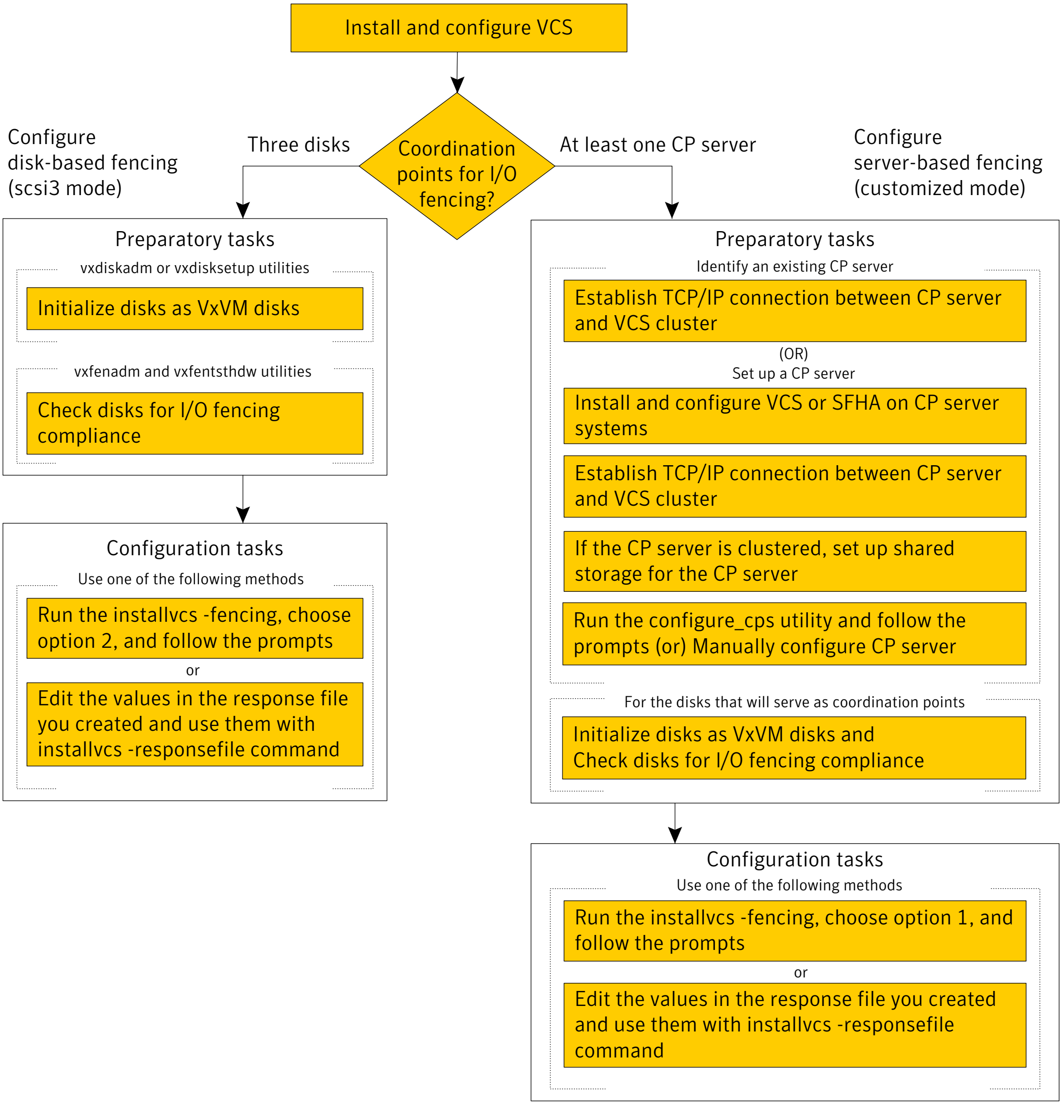
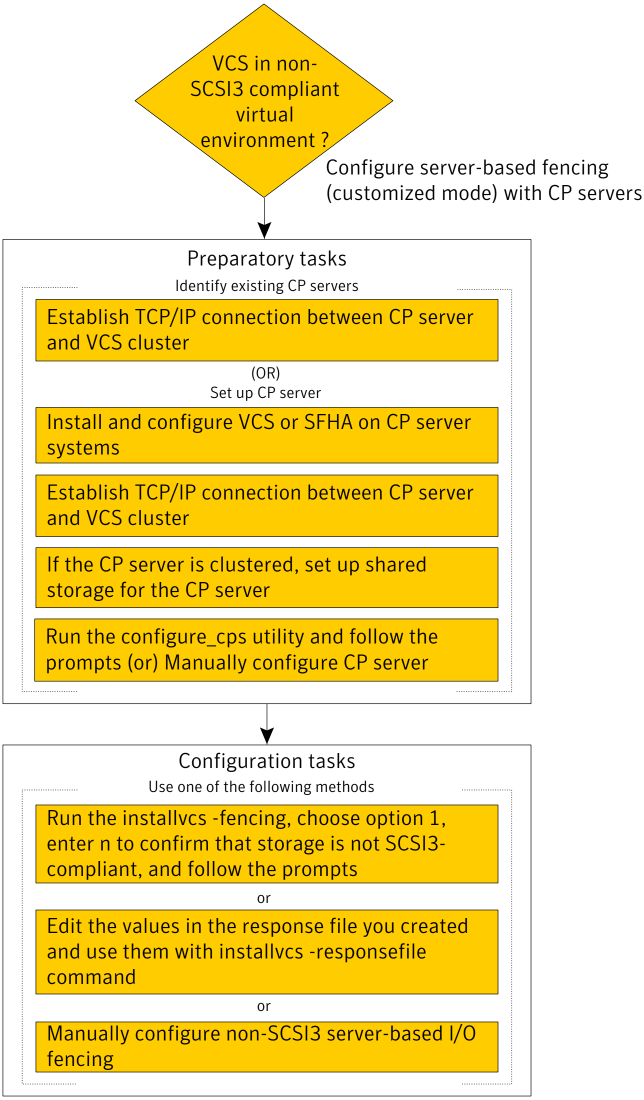

Install and configure VCS
Coordination points for I/O fencing?
Three disks
At least one CP server
Configure disk-based fencing (scsi3 mode)
Configure server-based fencing (customized mode)
Preparatory tasks
vxdiskadm or vxdisksetup utilities
Initialize disks as VxVM disks
vxfenadm and vxfentsthdw utilities
Check disks for I/O fencing compliance
Configuration tasks
Use one of the following methods
Run the installvcs -fencing, choose option 2, and follow the prompts
or
Edit the values in the response file you created and use them with installvcs -responsefile command
Preparatory tasks
Identify an existing CP server
Establish TCP/IP connection between CP server and VCS cluster
(OR)
Set up a CP server
Install and configure VCS or SFHA on CP server systems
Establish TCP/IP connection between CP server and VCS cluster
If the CP server is clustered, set up shared storage for the CP server
Run the configure_cps utility and follow the prompts (or) Manually configure CP server
For the disks that will serve as coordination points
Initialize disks as VxVM disks and Check disks for I/O fencing compliance
Configuration tasks
Use one of the following methods
Run the installvcs -fencing, choose option 1, and follow the prompts
or
Edit the values in the response file you created and use them with installvcs -responsefile command

Figure 7-2 illustrates a high-level flowchart to configure non-SCSI-3 server-based I/O fencing for the VCS cluster in virtual environments that do not support SCSI-3 PR.

Figure 7-2 Workflow to configure non-SCSI-3 server-based I/O fencing


VCS in non-SCSI3 compliant virtual environment ?
Configure server-based fencing (customized mode) with CP servers
Preparatory tasks
Identify existing CP servers
Establish TCP/IP connection between CP server and VCS cluster
(OR)
Set up CP server
Install and configure VCS or SFHA on CP server systems
Establish TCP/IP connection between CP server and VCS cluster
If the CP server is clustered, set up shared storage for the CP server
Run the configure_cps utility and follow the prompts (or) Manually configure CP server
Configuration tasks
Use one of the following methods
Run the installvcs -fencing, choose option 1, enter n to confirm that storage is not SCSI3-compliant, and follow the prompts
or
Edit the values in the response file you created and use them with installvcs -responsefile command
or
Manually 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 127. See "Setting up server-based I/O fencing using installvcs program" on page 134. See "Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program" on page 135.
Using response files	See "Response file variables to configure disk-based I/O fencing" on page 160. See "Response file variables to configure server-based I/O fencing" on page 162. See "Response file variables to configure non-SCSI-3 server-based I/O fencing" on page 164. See "Configuring I/O fencing using response files" on page 159.

You can also migrate from one I/O fencing configuration to another.

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

Setting up the CP server

Table 7-1 lists the tasks to set up the CP server for server-based I/O fencing.

Table 7-1 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 87.
Install the CP server	See "Installing the CP server using the installer" on page 88.
Configure the CP server cluster in secure mode	See "Configuring the CP server cluster in secure mode" on page 88.
Set up shared storage for the CP server database	See "Setting up shared storage for the CP server database" on page 89.
Configure the CP server	See " Configuring the CP server using the configuration utility" on page 90. See "Configuring the CP server manually" on page 99.
Verify the CP server configuration	See "Verifying the CP server configuration" on page 101.

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 to make the CP server highly available.

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 disk-based fencing 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.

   Symantec recommends configuring the CP server cluster in secure mode to secure the communication between the CP server and its clients (VCS clusters). It also secures the HAD communication on the CP server cluster.

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

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. CP server name can include alphanumeric characters, underscore, and hyphen.
   - 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
     You can configure multiple virtual IP addresses 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.

During installation, make sure to select all packages for installation. The VRTScps package is installed only if you select to install all packages.

Proceed to configure the CP server.

See “ Configuring the CP server using the configuration utility” on page 90.

See “Configuring the CP server manually” on page 99.

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 packages for installation. The VRTScps package is installed only if you select to install all packages.
- 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.

Note: If you already configured the CP server cluster in secure mode during the VCS configuration, then 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.

  If you have VCS installed on the CP server, run the following command:

  ```
  # installvcs -security
  ```

  If you have SFHA installed on the CP server, run the following command:

  ```
  # installsfha -security
  ```

Setting up shared storage for the CP server database

If you configured SFHA on the CP server cluster, perform the following procedure to set 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.

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 is 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 package.

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 90.
For CP servers on an SFHA cluster:	See "To configure the CP server on an SFHA cluster" on page 94.

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

1 Verify that the VRTScps package 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
```

5 Enter valid virtual IP addresses on which the CP server process should depend on:

- Enter the number of virtual IP addresses you want to configure:

  ```
  Enter the number of virtual IP(s) to configure : 2
  ```

- Enter valid virtual IP addresses:

  ```
  Enter a valid IP address for Virtual IP - 1 which the CP Server
  process should depend on : 10.209.83.85
  Enter a valid IP address for Virtual IP - 2 which the CP Server
  process should depend on : 10.209.83.87
  ```

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 for virtual IP 10.209.83.85 in range [49152,
65535], or press enter for default port (14250) :

Using default port: 14250

Enter a port number for virtual IP 10.209.83.87 in range
[49152, 65535], or press enter for default port (14250) :

Using 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
   (b)CP Server Virtual IP(s): 10.209.83.85 10.209.83.87
   (c)CP Server Port(s): 14250 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
----------------------------------------------
```

11 Enter the number of NIC resources that you want to configure. You must use a public NIC.

```
Enter how many NIC resources you want to configure [1 to 2]: 2
```

Answer the following questions for each NIC resource that you want to configure.

12 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: qfe0
Enter a valid network interface for virtual IP 10.209.83.87
on mycps1.symantecexample.com: qfe0
```

13 Enter the NIC resource you want to associate with the virtual IP addresses.

```
Enter the NIC resource you want to associate with the
virtual IP 10.209.83.85 [1 to 2] : 1
Enter the NIC resource you want to associate with the
virtual IP 10.209.83.87 [1 to 2] : 2
```

14 Enter networkhosts information for each 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 device
qfe0 on system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for
NIC qfe0 on system mycps1 : 10.209.83.86
Do you want to add another Network Host ?[y/n] : n
```

15 Enter the netmask for each virtual IP address. For example:

```
Enter the netmask for virtual IP 10.209.83.85 :
255.255.252.0
Enter the netmask for virtual IP 10.209.83.87 :
255.255.252.0
```

If you entered an IPv6 address, enter the prefix details at the prompt.

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

```
Successfully added the Quorum Agent Type to VCS configuration.
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.
```

17 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 252.

To configure the CP server on an SFHA cluster

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

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

3 Run the CP server configuration script on any node in the cluster:

```
# /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 rsh 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
```

6 Enter valid virtual IP addresses on which the CP server process should depend on:

- Enter the number of virtual IP addresses you want to configure:

  ```
  Enter the number of virtual IP(s) to configure : 2
  ```

- Enter valid virtual IP addresses:

  ```
  Enter a valid IP address for Virtual IP - 1 which the CP Server
  process should depend on : 10.209.83.85
  Enter a valid IP address for Virtual IP - 2 which the CP Server
  process should depend on : 10.209.83.87
  ```

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 for virtual IP 10.209.83.85 in range [49152,
   65535], or press enter for default port (14250) :

   Using default port: 14250

   Enter a port number for virtual IP 10.209.83.87 in range
   [49152, 65535], or press enter for default port (14250) :

   Using 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
(b)CP Server Virtual IP(s): 10.209.83.85 10.209.83.87
(c)CP Server Port(s): 14250 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 Enter the number of NIC resources that you want to configure. You must use a public NIC.

```
Enter how many NIC resources you want to configure [1 to 2]: 2
```

Answer the following questions for each NIC resource that you want to configure.

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

```
Is the name of network interfaces for NIC resource - 1
same on all the systems?[y/n] : y
```

14 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 : qfe0
```

15 Enter the NIC resource you want to associate with the virtual IP addresses.

```
Enter the NIC resource you want to associate with the
virtual IP 10.209.83.85 [1 to 2] : 1
Enter the NIC resource you want to associate with the
virtual IP 10.209.83.87 [1 to 2] : 2
```

16 Enter networkhosts information for each 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 device
qfe0 on system mycps1? [y/n] : y
Enter a valid IP address to configure NetworkHosts for
NIC qfe0 on system mycps1 : 10.209.83.86
Do you want to add another Network Host ?[y/n] : n
```

17 Enter the netmask for each virtual IP address.

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

If you entered an IPv6 address, enter the prefix details at the prompt.

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

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

19 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
```

20 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.
```

21 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   |ONLINE|
CPSSG     State      mycps2  |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 252.

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 252.

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 104.
Specify the systems where you want to configure VCS	See "Specifying systems for configuration" on page 105.
Configure the basic cluster	See "Configuring the cluster name" on page 106. See "Configuring private heartbeat links" on page 106.
Configure virtual IP address of the cluster (optional)	See "Configuring the virtual IP of the cluster" on page 109.
Configure the cluster in secure mode (optional)	See "Configuring the cluster in secure mode" on page 111.
Add VCS users (required if you did not configure the cluster in secure mode)	See "Adding VCS users" on page 116.
Configure SMTP email notification (optional)	See "Configuring SMTP email notification" on page 117.
Configure SNMP email notification (optional)	See "Configuring SNMP trap notification" on page 119.
Configure global clusters (optional) **Note:** You must have enabled Global Cluster Option when you installed VCS.	See "Configuring global clusters" on page 121.
Complete the software configuration	See "Completing the VCS configuration" on page 122.

Starting the software configuration

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

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 your product:

   Veritas Cluster Server

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
- Makes sure the installer started from the global zone
- Checks whether VCS is installed
- Exits if VCS 6.0 PR1 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 83.

Configuring the cluster name

Enter the cluster information when the installer prompts you.

To configure the cluster

1 Review the configuration instructions that the installer presents.

2 Enter a unique cluster name.

```
Enter the unique cluster name: [q,?] clus1
```

Configuring private heartbeat links

You now configure the private 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 263.

The following procedure helps you configure LLT over Ethernet.

To configure private heartbeat links

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

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

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

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

The installer discovers and lists the network interface cards.

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

- For Solaris SPARC:
  You must not enter the network interface card that is used for the public network (typically qfe0.)

```
Enter the NIC for the first private heartbeat link on galaxy:
[b,q,?] qfe0
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,?] qfe1
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)
```

- For Solaris x64:
  You must not enter the network interface card that is used for the public network (typically qfe0.)

```
Enter the NIC for the first private heartbeat link on galaxy:
[b,q,?] e1000g1
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,?] e1000g2
Would you like to configure a third private heartbeat link?
[y,n,q,b,?](n)
```

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

```
Enter the NIC for the first private heartbeat
link on 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
link 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 Enter a unique cluster ID:

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

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

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

7 Verify and confirm the information that the installer summarizes.

Configuring the virtual IP of the cluster

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

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

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

To configure the virtual IP of the cluster

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

2. When the system prompts whether you want to configure the virtual IP, enter `y`.

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

   Do one of the following:

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

   ```
   Active NIC devices discovered on galaxy: qfe0
   Enter the NIC for Virtual IP of the Cluster to use on galaxy:
   [b,q,?](qfe0)
   ```

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 qfe0 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)
  ```

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

        NIC: hme0
        IP: 192.168.1.16
        Netmask: 255.255.240.0

  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
  ```

- Verify and confirm the Cluster Virtual IP information.

  ```
  Cluster Virtual IP verification:

        NIC: hme0
        IP: 2001:454e:205a:110:203:baff:feee:10
        Prefix: 64

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

Configuring the cluster in secure mode

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

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

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

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

```
# haclus -value SecureClus
```

```
1
```

Setting up trust relationships for your VCS cluster

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

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

To set up a trust relationship

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

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

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

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

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

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

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

   Specify a valid data directory or press Enter to accept the default directory.
4. The installer performs one of the following actions:

- If you specified a valid directory, the installer prompts for a confirmation.

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

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

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

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

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

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

Configuring a secure cluster node by node

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

Table 8-2 lists the tasks that you must perform to configure a secure cluster.

Table 8-2 Configuring a secure cluster node by node

Task	Reference
Configure security on one node	See "Configuring the first node" on page 113.
Configure security on the remaining nodes	See "Configuring the remaining nodes" on page 114.
Complete the manual configuration steps	See "Completing the secure cluster configuration" on page 115.

Configuring the first node

Perform the following steps on one node in your cluster.

To configure security on the first node

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

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

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

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

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

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

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

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

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

Configuring the remaining nodes

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

To configure security on each remaining node

1. Ensure that you are logged in as superuser.

2. Enter the following command:

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

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

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

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

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

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

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

Completing the secure cluster configuration

Perform the following manual steps to complete the configuration.

To complete the secure cluster configuration

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

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

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

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

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

2. On the first node, stop the VCS engine.

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

3 On all nodes, stop the CmdServer.

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

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

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

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

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

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

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

7 On all nodes, start CmdServer.

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

8 On the first node, unfreeze the service groups.

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

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

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

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

Adding VCS users

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

To add VCS users

1 Review the required information to add VCS users.

2 Reset the password for the Admin user, if necessary.

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

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

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

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

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

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

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

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

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

Configuring SMTP email notification

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

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

To configure SMTP email notification

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

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

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

   See "Configuring SNMP trap notification" on page 119.
3. Provide information to configure SMTP notification.

   Provide the following information:

   - Enter the NIC information.

     ```
     Active NIC devices discovered on galaxy: hme0
     Enter the NIC for the VCS Notifier to use on galaxy:
     [b,q,?] (hme0)
     Is hme0 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: hme0

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 121.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the NIC information.

  ```
  Active NIC devices discovered on galaxy: hme0
  Enter the NIC for the VCS Notifier to use on galaxy:
  [b,q,?] (hme0)
  Is hme0 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: hme0

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, and value for the netmask.

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

   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: hme0
         IP: 192.168.1.16
         Netmask: 255.255.240.0

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

   On Solaris x64, an example for the NIC's port is hme0.

   For IPv6

   ```
   Global Cluster Option configuration verification:

         NIC: hme0
         IP: 2001:454e:205a:110:203:baff:feee:10
         Prefix: 64

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

   On Solaris x64, an example for the NIC's port is hme0.

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.

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 147.

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 123.

See "Updating product licenses using vxlicinst" on page 124.

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                            = Solaris
   Version                             = 6.0 PR1
   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 125.

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:

   ```
   # devfsadm
   ```

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

   - Use the interactive vxdiskadm utility to initialize the disks as VxVM disks.

For more information see the *Veritas Storage Foundation Administrator's Guide*.

- Use the `vxdisksetup` command to initialize a disk as a VxVM disk.

  ```
  # vxdisksetup -i device_name
  ```

  The example specifies the CDS format:

  ```
    # vxdisksetup -i c2t13d0
  ```

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

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 6.0 PR1 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 [1-4,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.
    If the available VxVM CDS disks are less than the required, installer asks whether you want to initialize more disks as VxVM disks. Choose the disks you want to initialize as VxVM disks and then use them to create new disk group.
  - Enter the numbers corresponding to the disks that you want to use as coordinator disks.
  - Enter the disk group name.

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

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

See “Checking shared disks for I/O fencing” on page 130.

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

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

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

The program also does the following:

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

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

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

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

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

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

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

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

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

See the *Veritas 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 131.

- Verifying that nodes have access to the same disk
  See “Verifying that the nodes have access to the same disk” on page 132.
- Testing the shared disks for SCSI-3
  See “Testing the disks using vxfentsthdw utility” on page 132.

Verifying Array Support Library (ASL)

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

To verify Array Support Library (ASL)

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

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

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

  The following output is a sample:

```
# vxddladm listsupport all


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

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

```
# vxdisk scandisks
```

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

Verifying that the nodes have access to the same disk

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

To verify that the nodes have access to the same disk

1. Verify the connection of the shared storage for data to two of the nodes on which you installed 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/rdsk/c1t1d0s2 path on node A and the /dev/rdsk/c2t1d0s2 path on node B.

   From node A, enter:

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

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

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

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

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

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

Testing the disks using vxfentsthdw utility

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

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

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

```
The disk /dev/rdsk/c1t1d0s2 is ready to be configured for I/O Fencing on
node 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 281.

2 From one node, start the utility.

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

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

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

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

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

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

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

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

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

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

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

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

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

ALL tests on the disk /dev/rdsk/c1t1d0s2 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

See "Setting up server-based I/O fencing using installvcs program" on page 134.

Setting up non-SCSI-3 server-based I/O fencing in virtual environments using installvcs program

If you have installed VCS in virtual environments that do not support SCSI-3 PR-compliant storage, you can configure non-SCSI-3 fencing.

To configure I/O fencing using the installvcs program in a non-SCSI-3 PR-compliant setup

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.

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 6.0 PR1 is configured properly.

3 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
[1-4,b,q] 1
```

4 Enter **n** to confirm that your storage environment does not support SCSI-3 PR.

```
Does your storage environment support SCSI3 PR?
[y,n,q] (y) n
```

5 Confirm that you want to proceed with the non-SCSI-3 I/O fencing configuration at the prompt.

6 Enter the number of CP server coordination points you want to use in your setup.

7 Enter the following details for each CP server:

- Enter the virtual IP address or the fully qualified host name.
- Enter the port address on which the CP server listens for connections.
  The default value is 14250. You can enter a different port address. Valid values are between 49152 and 65535.

The installer assumes that these values are identical from the view of the VCS cluster nodes that host the applications for high availability.

8 Verify and confirm the CP server information that you provided.

9 Verify and confirm the VCS cluster configuration information.

Review the output as the installer performs the following tasks:

- Updates the CP server configuration files on each CP server with the following details:
  - Registers each node of the VCS cluster with the CP server.
  - Adds CP server user to the CP server.
  - Adds VCS cluster to the CP server user.
- Updates the following configuration files on each node of the VCS cluster
  - `/etc/vxfenmode` file
  - `/etc/vxenviron` file
  - `/etc/llttab` file

10 Review the output as the installer stops VCS on each node, starts I/O fencing on each node, updates the VCS configuration file main.cf, and restarts VCS with non-SCSI-3 server-based fencing.

Confirm to configure the CP agent on the VCS cluster.

11 Confirm whether you want to send the installation information to Symantec.

12 After the installer configures I/O fencing successfully, note the location of summary, log, and response files that installer creates.

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

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 29.

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 response files

Chapter 10

Performing automated VCS installation

This chapter includes the following topics:

- Installing VCS using response files
- Response file variables to install VCS
- Sample response file for installing VCS

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 31.

2. Make sure the preinstallation tasks are completed.

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 144.

4. Edit the values of the response file variables as necessary.

   See "Response file variables to install VCS" on page 142.

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 10-1 lists the response file variables that you can define to install VCS.

Table 10-1 Response file variables specific to installing VCS

Variable	List or Scalar	Description
CFG{opt}{install}	Scalar	Installs VCS packages. (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 VCS60 for VCS. (Required)

Table 10-1 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 packages based on the variable that has the value set to 1:
		■ installallpkgs: Installs all packages
		■ installrecpkgs: Installs recommended packages
		■ installminpkgs: Installs minimum packages
		Note: The installer requires only one of these variable values to be set to 1.
		(Required)

CFG{opt}{rsh}	Scalar	Defines that *rsh* 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 10-1 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 packages. The location must be accessible from all target systems. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. (Optional)
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 142.

```
#
# Configuration Values:
#
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installrecpkgs}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
1;
```

Performing automated VCS configuration

This chapter includes the following topics:

- Configuring VCS using response files
- Response file variables to configure Veritas Cluster Server
- Sample response file for configuring VCS

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 packages 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 157.

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 Veritas Cluster Server" on page 148.

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 Veritas Cluster Server

Table 11-1 lists the response file variables that you can define to configure VCS.

Table 11-1 Response file variables specific to configuring Veritas Cluster Server

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the packages are already installed. (Required) Set the value to 1 to configure VCS.
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{systems}	List	List of systems on which the product is to be configured. (Required)
CFG{prod}	Scalar	Defines the product to be configured. The value is VCS60 for VCS. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)

Table 11-1 Response file variables specific to configuring Veritas Cluster Server *(continued)*

Variable	List or Scalar	Description
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)
CFG{uploadlogs}	Scalar	Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (csgnic, csgvip, and csgnetmask) must be defined if any are defined. The same is true for the SMTP notification (smtpserver, smtprecp, and smtprsev), the SNMP trap notification (snmpport, snmpcons, and snmpcsev), and the Global Cluster Option (gconic, gcovip, and gconetmask).

Table 11-2 lists the response file variables that specify the required information to configure a basic VCS cluster.

Table 11-2 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 11-3 lists the response file variables that specify the required information to configure LLT over Ethernet.

Table 11-3 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 11-3 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 11-4 lists the response file variables that specify the required information to configure LLT over UDP.

Table 11-4 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 11-4 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)

Table 11-4 Response file variables specific to configuring LLT over UDP *(continued)*

Variable	List or Scalar	Description

CFG{vcs_udplinklowpri<n>_netmask}
{<system1>}
	Scalar	Stores the netmask (prefix for IPv6) that the low priority heartbeat link uses on node1.
		You can have four low priority heartbeat links and <n> for this response file variable can take values 1 to 4 for the respective low priority heartbeat links.
		(Required)

Table 11-5 lists the response file variables that specify the required information to configure virtual IP for VCS cluster.

Table 11-5 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 11-6 lists the response file variables that specify the required information to configure the VCS cluster in secure mode.

Table 11-6 Response file variables specific to configuring VCS cluster in secure mode

Variable	List or Scalar	Description
CFG{vcs_eat_security}	Scalar	Specifies if the cluster is in secure enabled mode or not.
CFG{opt}{securityonenode}	Scalar	Specifies that the securityonenode option is being used.
CFG{securityonenode_menu}	Scalar	Specifies the menu option to choose to configure the secure cluster one at a time. ■ 1—Configure the first node ■ 2—Configure the other node
CFG{security_conf_dir}	Scalar	Specifies the directory where the configuration files are placed.
CFG{opt}{security}	Scalar	Specifies that the security option is being used.

Table 11-7 lists the response file variables that specify the required information to configure VCS users.

Table 11-7 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 11-7 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 11-8 lists the response file variables that specify the required information to configure VCS notifications using SMTP.

Table 11-8 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, 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 11-9 lists the response file variables that specify the required information to configure VCS notifications using SNMP.

Table 11-9 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, 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 11-10 lists the response file variables that specify the required information to configure VCS global clusters.

Table 11-10 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 Veritas Cluster Server" on page 148.

Note: For Solaris x64 Platform Edition, read the values of NICs as e1000g0, e1000g2, and e1000g3 instead of hme0, qfe0, qfe1 in the sample response file.

```
#
# Configuration Values:
#
our %CFG;

$CFG{opt}{configure}=1;
$CFG{opt}{gco}=1;
$CFG{prod}="VCS60";
$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}="hme0";
$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}="qfe0";
$CFG{vcs_lltlink1}{nebula}="qfe0";
$CFG{vcs_lltlink2}{galaxy}="qfe1";
$CFG{vcs_lltlink2}{nebula}="qfe1";

$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 12

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 83.

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 161.

See "Sample response file for configuring server-based I/O fencing" on page 164.

4 Edit the values of the response file variables as necessary.

See "Response file variables to configure disk-based I/O fencing" on page 160.

See "Response file variables to configure server-based I/O fencing" on page 162.

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 12-1 lists the response file variables that specify the required information to configure disk-based I/O fencing for VCS.

Table 12-1 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{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 ■ 4—Fencing migration when the cluster is online (Required)

Table 12-1 Response file variables specific to configuring disk-based I/O fencing *(continued)*

Variable	List or Scalar	Description
CFG {fencing_scsi3_disk_policy}	Scalar	Specifies the I/O fencing mechanism. This variable is not required if you had configured fencing in disabled mode. For disk-based fencing, you must configure the fencing_scsi3_disk_policy variable and either the fencing_dgname variable or the fencing_newdg_disks variable. (Optional)
CFG{fencing_dgname}	Scalar	Specifies the disk group for I/O fencing. (Optional) **Note:** You must define the fencing_dgname variable to use an existing disk group. If you want to create a new disk group, you must use both the fencing_dgname variable and the fencing_newdg_disks variable.
CFG{fencing_newdg_disks}	List	Specifies the disks to use to create a new disk group for I/O fencing. (Optional) **Note:** You must define the fencing_dgname variable to use an existing disk group. If you want to create a new disk group, you must use both the fencing_dgname variable and the fencing_newdg_disks variable.

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 160.

```
#
# Configuration Values:
```

```
#
our %CFG;

$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;

$CFG{prod}="VCS60";

$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=13221;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_dgname}="fendg";
$CFG{fencing_scsi3_disk_policy}="dmp";
$CFG{fencing_newdg_disks}=
 [ qw(c1t1d0s2 c2t1d0s2 c3t1d0s2) ];
$CFG{fencing_option}=2;
```

Response file variables to configure server-based I/O fencing

You can use a coordination point server-based fencing response file to configure server-based customized I/O fencing.

Table 12-2 lists the fields in the response file that are relevant for server-based customized I/O fencing.

Table 12-2 Coordination point server (CP server) based fencing response file definitions

Response file field	Definition
CFG {fencing_config_cpagent}	Enter '1' or '0' depending upon whether you want to configure the Coordination Point agent using the installer or not. Enter "0" if you do not want to configure the Coordination Point agent using the installer. Enter "1" if you want to use the installer to configure the Coordination Point agent.

Table 12-2 Coordination point server (CP server) based fencing response file definitions *(continued)*

Response file field	Definition
CFG {fencing_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_config_cpagent` field is given a value of '0'.
CFG {fencing_cps}	Virtual IP address or Virtual hostname of the CP servers.
CFG {fencing_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 "$CFG{fencing_reusedg}=0" or "$CFG{fencing_reusedg}=1" before proceeding with a silent installation.
CFG {fencing_dgname}	The name of the disk group to be used in the customized fencing, where at least one disk is being used.
CFG {fencing_disks}	The disks being used as coordination points if any.
CFG {fencing_ncp}	Total number of coordination points being used, including both CP servers and disks.
CFG {fencing_ndisks}	The number of disks being used.
CFG {fencing_cps_vips}	The virtual IP addresses or the fully qualified host names of the CP server.
CFG {fencing_ports}	The port that the virtual IP address or the fully qualified host name of the CP server listens on.
CFG {fencing_scsi3_disk_policy}	The disk policy that the customized fencing uses. The value for this field is either "raw" or "dmp"

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_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.200.117.145) ];
$CFG{fencing_cps_vips}{"10.200.117.145"}=[ qw(10.200.117.145) ];
$CFG{fencing_dgname}="vxfencoorddg";
$CFG{fencing_disks}=[ qw(emc_clariion0_37 emc_clariion0_13) ];
$CFG{fencing_scsi3_disk_policy}="raw";
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=2;
$CFG{fencing_ports}{"10.200.117.145"}=14250;
$CFG{fencing_reusedg}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```

Response file variables to configure non-SCSI-3 server-based I/O fencing

Table 12-3 lists the fields in the response file that are relevant for non-SCSI-3 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 27.

Table 12-3 Non-SCSI-3 server-based I/O fencing response file definitions

Response file field	Definition
CFG{non_scsi3_fencing}	Defines whether to configure non-SCSI-3 server-based I/O fencing. Valid values are 1 or 0. Enter 1 to configure non-SCSI-3 server-based I/O fencing.

Table 12-3 Non-SCSI-3 server-based I/O fencing response file definitions *(continued)*

Response file field	Definition
CFG {fencing_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_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_config_cpagent` field is given a value of '0'.
CFG {fencing_cps}	Virtual IP address or Virtual hostname of the CP servers.
CFG {fencing_cps_vips}	The virtual IP addresses or the fully qualified host names of the CP server.
CFG {fencing_ncp}	Total number of coordination points (CP servers only) being used.
CFG {fencing_ports}	The port of the CP server that is denoted by *cps* .

Sample response file for configuring non-SCSI-3 server-based I/O fencing

The following is a sample response file used for non-SCSI-3 server-based I/O fencing :

```
$CFG{fencing_config_cpagent}=0;
$CFG{fencing_cps}=[ qw(10.198.89.251 10.198.89.252 10.198.89.253) ];
$CFG{fencing_cps_vips}{"10.198.89.251"}=[ qw(10.198.89.251) ];
$CFG{fencing_cps_vips}{"10.198.89.252"}=[ qw(10.198.89.252) ];
$CFG{fencing_cps_vips}{"10.198.89.253"}=[ qw(10.198.89.253) ];
$CFG{fencing_ncp}=3;
$CFG{fencing_ndisks}=0;
$CFG{fencing_ports}{"10.198.89.251"}=14250;
```

```
$CFG{fencing_ports}{"10.198.89.252"}=14250;
$CFG{fencing_ports}{"10.198.89.253"}=14250;
$CFG{non_scsi3_fencing}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{fencing}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
$CFG{vcs_clusterid}=1256;
$CFG{vcs_clustername}="clus1";
$CFG{fencing_option}=1;
```

Section 5

Post-installation tasks

Chapter 13

Performing post-installation tasks

This chapter includes the following topics:

- About enabling LDAP authentication for clusters that run in secure mode
- Accessing the VCS documentation
- Removing permissions for communication
- Changing root user into root role

About enabling LDAP authentication for clusters that run in secure mode

Symantec Product Authentication Service (AT) supports LDAP (Lightweight Directory Access Protocol) user authentication through a plug-in for the authentication broker. AT supports all common LDAP distributions such as Oracle Directory Server, Netscape, OpenLDAP, and Windows Active Directory.

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain.

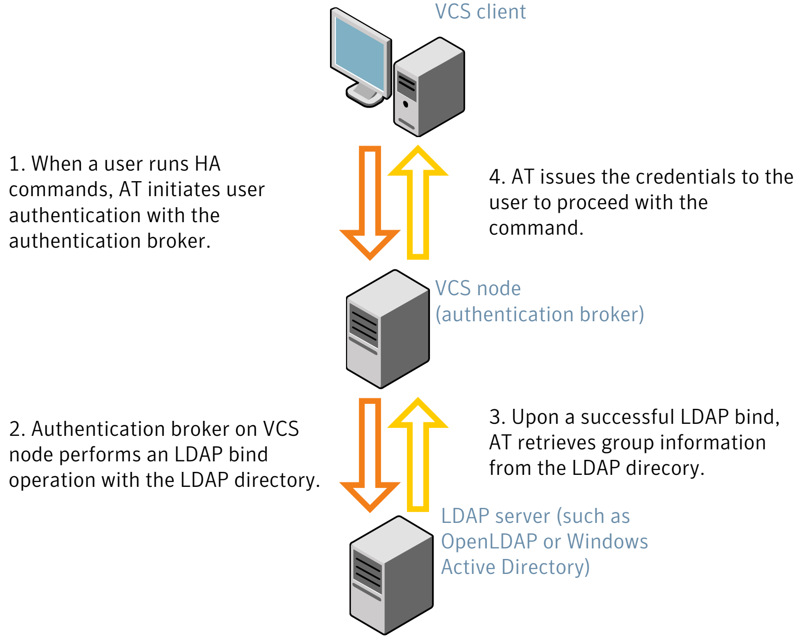
See "Enabling LDAP authentication for clusters that run in secure mode" on page 171.

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 13-1 depicts the VCS cluster communication with the LDAP servers when clusters run in secure mode.

Figure 13-1 Client communication with LDAP servers


VCS client
1. When a user runs HA commands, AT initiates user authentication with the authentication broker.
4. AT issues the credentials to the user to proceed with the command.
VCS node (authentication broker)
2. Authentication broker on VCS node performs an LDAP bind operation with the LDAP directory.
3. Upon a successful LDAP bind, AT retrieves group information from the LDAP direcory.
LDAP server (such as OpenLDAP or Windows Active Directory)

The LDAP schema and syntax for LDAP commands (such as, ldapadd, ldapmodify, and ldapsearch) vary based on your LDAP implementation.

Before adding the LDAP domain in Symantec Product Authentication Service, note the following information about your LDAP environment:

- The type of LDAP schema used (the default is RFC 2307)
  - UserObjectClass (the default is posixAccount)
  - UserObject Attribute (the default is uid)
  - User Group Attribute (the default is gidNumber)
  - Group Object Class (the default is posixGroup)
  - GroupObject Attribute (the default is cn)
  - Group GID Attribute (the default is gidNumber)
  - Group Membership Attribute (the default is memberUid)
- URL to the LDAP Directory

- Distinguished name for the user container (for example, UserBaseDN=ou=people,dc=comp,dc=com)
- Distinguished name for the group container (for example, GroupBaseDN=ou=group,dc=comp,dc=com)

Enabling LDAP authentication for clusters that run in secure mode

The following procedure shows how to enable the plug-in module for LDAP authentication. This section provides examples for OpenLDAP and Windows Active Directory LDAP distributions.

Before you enable the LDAP authentication, complete the following steps:

- Make sure that the cluster runs in secure mode.

  ```
  # haclus -value SecureClus
  ```

  The output must return the value as 1.
- Make sure that the AT version is 6.1.6.0 or later.

  ```
  # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat showversion
  vssat version: 6.1.6.0
  ```

See the `vssat.1m` and the `atldapconf.1m` manual pages.

To enable OpenLDAP authentication for clusters that run in secure mode

1 Add the LDAP domain to the AT configuration using the `vssat` command.

The following example adds the LDAP domain, MYENTERPRISE:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat addldapdomain \
--domainname "MYENTERPRISE.symantecdomain.com"\
--server_url "ldap://my_openldap_host.symantecexample.com"\
--user_base_dn "ou=people,dc=symantecdomain,dc=myenterprise,dc=com"\
--user_attribute "cn" --user_object_class "account"\
--user_gid_attribute "gidNumber"\
--group_base_dn "ou=group,dc=symantecdomain,dc=myenterprise,dc=com"\
--group_attribute "cn" --group_object_class "posixGroup"\
--group_gid_attribute "member"\
--admin_user "cn=manager,dc=symantecdomain,dc=myenterprise,dc=com"\
--admin_user_password "password" --auth_type "FLAT"
```

2 Verify that you can successfully authenticate an LDAP user on the 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/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat authenticate
--domain ldap:MYENTERPRISE.symantecdomain.com
--prplname vcsadmin1 --broker galaxy:14149

Enter password for vcsadmin1: ##########

authenticate
----------------------
----------------------

Authenticated User vcsadmin1
----------------------
```

3. Add the LDAP user to the main.cf file.

   ```
   # haconf makerw
   # hauser -add "CN=vcsadmin1/CN=people/\
   DC=symantecdomain/DC=myenterprise/\
   DC=com@myenterprise.symantecdomain.com" -priv Administrator
   # haconf -dump -makero
   ```

   If you want to enable group-level authentication, you must run the following command:

   ```
   # hauser -addpriv \
   ldap_group@ldap_domain AdministratorGroup
   ```

4. Verify that the main.cf file has the following lines:

   ```
   # cat /etc/VRTSvcs/conf/config/main.cf
   ...
   ...
   cluster 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 the Korn shell (ksh), run the following commands:

   ```
   # export VCS_DOMAIN=myenterprise.symantecdomain.com
   # export VCS_DOMAINTYPE=ldap
   ```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
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/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -d \
-s domain_controller_name_or_ipaddress \
-u domain_user -g domain_group
```

For example:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-d -s 192.168.20.32 -u Administrator -g "Domain Admins"
Search User provided is invalid or Authentication is required to
proceed further.
Please provide authentication information for LDAP server.

Username/Common Name: symantecdomain\administrator
Password:

Attribute file created.
```

2 Run the LDAP configuration tool atldapconf using the -c option. The -c option creates a CLI file to add the LDAP domain.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-c -d windows_domain_name
```

For example:

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf \
-c -d symantecdomain.com
Attribute list file not provided, using default AttributeList.txt.
CLI file name not provided, using default CLI.txt.

CLI for addldapdomain generated.
```

3 Run the LDAP configuration tool atldapconf using the -x option. The -x option reads the CLI file and executes the commands to add a domain to the AT.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/atldapconf -x
```

4 List the LDAP domains to verify that the Windows Active Directory server integration is complete.

```
# /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vssat listldapdomains

Domain Name :          symantecdomain.com
Server URL :           ldap://192.168.20.32:389
SSL Enabled :          No
User Base DN :         CN=people,DC=symantecdomain,DC=com
User Object Class :    account
User Attribute :       cn
User GID Attribute :   gidNumber
Group Base DN :        CN=group,DC=symantecdomain,DC=com
Group Object Class :   group
Group Attribute :      cn
Group GID Attribute :  cn
Auth Type :            FLAT
Admin User :
Admin User Password :
Search Scope :         SUB
```

5 Set the VCS_DOMAIN and VCS_DOMAINTYPE environment variables as follows:

- VCS_DOMAIN=symantecdomain.com
- VCS_DOMAINTYPE=ldap

For example, for the Bourne Shell (sh) or the Korn shell (ksh), run the following commands:

```
# export VCS_DOMAIN=symantecdomain.com
# export VCS_DOMAINTYPE=ldap
```

6 Verify that you can log on to VCS. For example

```
# halogin vcsadmin1 password
# hasys -state
VCS NOTICE V-16-1-52563 VCS Login:vcsadmin1
#System    Attribute    Value
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 `rsh`, remove the temporary `rsh` access permissions that you set for the nodes and restore the connections to the public network.

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

Changing root user into root role

On Oracle Solaris 11, to perform installation, you need to create root user. This means that a local user cannot assume the root role. After installation, you may want to turn root user into root role for a local user, who can log in as root.

1. Log in as root user.

2. Change the root account into role.

   ```
   # rolemod -K type=role root
   ```

   ```
   # getent user_attr root
   ```

   ```
   root::::type=role;auths=solaris.*;profiles=All;audit_flags=lo\
   :no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
   ```

3. Assign the root role to a local user who was unassigned the role.

   ```
   # usermod -R root admin
   ```

For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

Chapter 14

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 cat command.

```
cat /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.

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 63.
3. Verify LLT operation.

   See "Verifying LLT" on page 180.
4. Verify GAB operation.

   See "Verifying GAB" on page 183.
5. Verify the cluster operation.

   See "Verifying the cluster" on page 185.

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 the following:

- For Solaris SPARC:

```
Node          State      Link    Status      Address
*0 galaxy      OPEN
                         qfe:0 UP     08:00:20:93:0E:34
                         qfe:1 UP     08:00:20:93:0E:38
1 nebula       OPEN
                         qfe:0 UP     08:00:20:8F:D1:F2
                         qfe:1 DOWN
```

- For Solaris x64:

```
Node          State      Link    Status      Address
*0 galaxy      OPEN
                         e1000g:1 UP     08:00:20:93:0E:34
                         e1000g:2 UP     08:00:20:93:0E:38
1 nebula       OPEN
                         e1000g:1 UP     08:00:20:8F:D1:F2
                         e1000g:2 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
- An address for each link

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

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

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

```
lltstat -p
```

The output resembles:

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

Verifying GAB

Verify the GAB operation using the `gabconfig -a` command. This command returns the GAB port membership information.

The 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
   ```

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.

Note: The example in the following procedure is for SPARC. x64 clusters have different command output.

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       130

galaxy     ConfigCheckSum         46688

galaxy     ConfigDiskState        CURRENT

galaxy     ConfigFile             /etc/VRTSvcs/conf/config

galaxy     ConfigInfoCnt          0

galaxy     ConfigModDate          Thu Sep 22 07:14:23 CDT 2011

galaxy     ConnectorState         Down

galaxy     CurrentLimits

galaxy     DiskHbStatus
galaxy    DynamicLoad           0

galaxy    EngineRestarted       0

galaxy    EngineVersion         6.0.00.0

galaxy    FencingWeight         0

galaxy    Frozen                0

galaxy    GUIIPAddr

galaxy    HostUtilization       CPU 7 Swap 0

galaxy    LLTNodeId             0

galaxy    LicenseType           PERMANENT_SITE

galaxy    Limits

galaxy    LinkHbStatus          qfe:0 UP qfe:1 UP

galaxy    LoadTimeCounter       0

galaxy    LoadTimeThreshold     600

galaxy    LoadWarningLevel      80

galaxy    NoAutoDisable         0

galaxy    NodeId                0

galaxy    OnGrpCnt              1

galaxy    PhysicalServer

galaxy    ShutdownTimeout       600

galaxy    SourceFile            ./main.cf

galaxy    SwapThresholdLevel    Critical 90 Warning 80 Note 70
                                Info 60

galaxy    SysInfo               Solaris:galaxy,Generic_
                                118558-11,5.9,sun4u

galaxy    SysName               galaxy

galaxy    SysState              RUNNING

galaxy    SystemLocation
galaxy    SystemOwner

galaxy    SystemRecipients

galaxy    TFrozen               0

galaxy    TRSE                  0

galaxy    UpDownState           Up

galaxy    UserInt               0

galaxy    UserStr

galaxy    VCSFeatures           NONE

galaxy    VCSMode               VCS
```

Performing a postcheck on a node

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

See "About using the postcheck option" on page 188.

To run the postcheck command on a node

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

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

2 Review the output for installation-related information.

About using the postcheck option

You can use the installer's post-check to determine installation-related problems and to aid in troubleshooting.

Note: This command option requires downtime for the node.

When you use the `postcheck` option, it can help you troubleshoot the following VCS-related issues:

- The heartbeat link does not exist.
- The heartbeat link cannot communicate.

- The heartbeat link is a part of a bonded or aggregated NIC.
- A duplicated cluster ID exists.
- The VRTSllt pkg version is not consistent on the nodes.
- The llt-linkinstall value is incorrect.
- The llthosts(4) or llttab(4) configuration is incorrect.
- the `/etc/gabtab` file is incorrect.
- The incorrect GAB linkinstall value exists.
- The VRTSgab pkg version is not consistent on the nodes.
- The `main.cf` file or the `types.cf` file is invalid.
- The `/etc/VRTSvcs/conf/sysname` file is not consistent with the hostname.
- The cluster UUID does not exist.
- The `uuidconfig.pl` file is missing.
- The VRTSvcs pkg version is not consistent on the nodes.
- The `/etc/vxfenmode` file is missing or incorrect.
- The `/etc/vxfendg file` is invalid.
- The vxfen link-install value is incorrect.
- The VRTSvxfen pkg version is not consistent.

The `postcheck` option can help you troubleshoot the following SFHA or SFCFSHA issues:

- Volume Manager cannot start because the `/etc/vx/reconfig.d/state.d/install-db` file has not been removed.
- Volume Manager cannot start because the `Volboot` file is not loaded.
- Volume Manager cannot start because no license exists.
- Cluster Volume Manager cannot start because the CVM configuration is incorrect in the `main.cf` file. For example, the Autostartlist value is missing on the nodes.
- Cluster Volume Manager cannot come online because the node ID in the `/etc/llthosts` file is not consistent.
- Cluster Volume Manager cannot come online because Vxfen is not started.
- Cluster Volume Manager cannot start because gab is not configured.

- Cluster Volume Manager cannot come online because of a CVM protocol mismatch.
- Cluster Volume Manager group name has changed from "cvm", which causes CVM to go offline.

See “Performing a postcheck on a node” on page 188.

Section 6

Uninstalling VCS

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 215.
- 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 67.

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 `rsh` commands as superuser on all nodes in the cluster.
- Make sure that the `ssh` or `rsh` 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 packages and VCS language packages.

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 6.0 PR1 packages

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 packages to be uninstalled.

6 Review the output as the uninstaller stops processes, unloads kernel modules, and removes the packages.

7 Note the location of summary, response, and log files that the uninstaller creates after removing all the packages.

Running uninstallvcs from the VCS 6.0 PR1 disc

You may need to use the uninstallvcs program on the VCS 6.0 PR1 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
```

Removing language packages using the uninstaller program

The uninstallvcs program removes all VCS packages and language packages.

Removing the CP server configuration using the removal script

This section describes how to remove the CP server configuration from a node or a cluster that hosts the CP server.

Warning: Ensure that no VCS cluster (application cluster) uses the CP server that you want to unconfigure.

You can use the CP server configuration utility (`configure_cps.pl`) to remove the CP server configuration. This utility performs the following tasks when you choose to unconfigure the CP server:

- Removes all CP server configuration files
- Removes the VCS configuration for CP server

After you run this utility, you can uninstall VCS from the node or the cluster.

Note: You must run the configuration utility only once per CP server (which can be on a single-node VCS cluster or an SFHA cluster), when you want 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. Select option 3 from the menu to unconfigure the CP server.

   ```
   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. Review the warning message and confirm that you want to unconfigure the CP server.

   ```
   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
   ```

4. Review the screen output as the script performs the following steps to remove the CP server configuration:

   - Stops the CP server
   - Removes the CP server from VCS configuration

- Removes resource dependencies
- Takes the the CP server service group (CPSSG) offline, if it is online
- Removes the CPSSG service group from the VCS configuration

5 Answer **y** to delete the CP server database.

```
Do you want to delete the CP Server database? (y/n) (Default:n) :
```

6 Answer **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) :
```

7 Answer **y**to delete the CP server configuration file and log files.

```
Do you want to delete the CP Server configuration file
(/etc/vxcps.conf) and log files (in /var/VRTScps)? (y/n)
(Default:n) : y
```

8 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 16

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 thesystem where you want to uninstall VCS.

   See "Sample response file for uninstalling VCS" on page 201.
3. Edit the values of the response file variables as necessary.

   See "Response file variables to uninstall VCS" on page 200.
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 16-1 lists the response file variables that you can define to uninstall VCS.

Table 16-1 Response file variables specific to uninstalling VCS

Variable	List or Scalar	Description
CFG{opt}{uninstall}	Scalar	Uninstalls VCS packages. (Required)
CFG{systems}	List	List of systems on which the product is to be uninstalled. (Required)
CFG{prod}	Scalar	Defines the product to be uninstalled. 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 *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for uninstalling VCS

Review the response file variables and their definitions.

See “Response file variables to uninstall VCS” on page 200.

```
#
# Configuration Values:
#
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="VCS60";
$CFG{systems}=[ qw(galaxy nebula) ];
1;
```

Chapter 17

Manually uninstalling VCS packages from non-global zones

This chapter includes the following topics:

- Manually uninstalling VCS packages on non-global zones

Manually uninstalling VCS packages on non-global zones

1. Log on to the non-global zone as a super user.
2. Uninstall VCS packages from Solaris brand zones.

   ```
   # pkg uninstall VRTSperl VRTSvlic VRTSvcs VRTSvcsag VRTSvcsea
   ```

3. Uninstall VCS packages from solaris10 brand zones.

   ```
   # pkgrm VRTSperl VRTSvlic VRTSvcs VRTSvcsag VRTSvcsea
   ```

Section 7

Adding and removing nodes

Adding a node to a single-node cluster

This chapter includes the following topics:

- Adding a node to a single-node cluster

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 18-1 specifies the activities that you need to perform to add nodes to a single-node cluster.

Table 18-1 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 208.
■ 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 209.
Connect both nodes to shared storage.	See "Configuring the shared storage" on page 210.

Table 18-1 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 210.
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 211.
Edit the configuration files on Node B.	
Start LLT and GAB on Node B.	See "Starting LLT and GAB" on page 211.
■ Start LLT and GAB on Node A. ■ Copy UUID from Node A to Node B. ■ Restart VCS on Node A. ■ Modify service groups for two nodes.	See "Reconfiguring VCS on the existing node" on page 211.
■ Start VCS on Node B. ■ Verify the two-node cluster.	See "Verifying configuration on both nodes" on page 213.

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 packages and configuration files.
  See "Removing a node from a cluster" on page 218.
- 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.

2 If necessary, install VxVM and VxFS.

See "Installing VxVM or VxFS if necessary" on page 209.

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 54.

To install and configure Ethernet cards for private network

1 Shut down VCS on Node A.

```
# hastop -local
```

2 Shut down the node to get to the OK prompt:

```
# sync;sync;init 0
```

3 Install the Ethernet card on Node A.

If you want to use aggregated interface to set up private network, configure aggregated interface.

4 Install the Ethernet card on Node B.

If you want to use aggregated interface to set up private network, configure aggregated interface.

5 Configure the Ethernet card on both nodes.

6 Make the two Ethernet cable connections from Node A to Node B for the private networks.

7 Restart the nodes.

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 58.

Bringing up the existing node

Bring up the node.

To bring up the node

1 Start the operating system. On a SPARC node (Node A) enter the command:

```
ok boot -r
```

2 Log in as superuser.

3 Make the VCS configuration writable.

```
# haconf -makerw
```

4 Display the service groups currently configured.

```
# hagrp -list
```

5 Freeze the service groups.

```
# hagrp -freeze group -persistent
```

Repeat this command for each service group in step 4.

6 Make the configuration read-only.

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

7 Stop VCS on Node A.

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

8 If you have configured I/O Fencing, GAB, and LLT on the node, stop them.

```
# /usr/sbin/svcadm disable -t gab

# /usr/sbin/svcadm disable -t llt
```

Installing the VCS software manually when adding a node to a single node cluster

Install the VCS 6.0 PR1 packages manually and install the license key.

Refer to the following sections:

-
-

Creating configuration files

Create the configuration files for your cluster.

To create the configuration files

1. Create the file /etc/llttab for a two-node cluster
2. Create the file /etc/llthosts that list both the nodes.
3. Create the file /etc/gabtab.

Starting LLT and GAB

On the new node, start LLT and GAB.

To start LLT and GAB

1. Start LLT on Node B.
   - On Solaris 10:

     ```
     # /usr/sbin/svcadm enable llt
     ```

2. Start GAB on Node B
   - On Solaris 10:

     ```
     # /usr/sbin/svcadm enable gab
     ```

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.

   - Solaris 10:

     ```
     # /usr/sbin/svcadm enable llt
     ```

3. Start GAB on Node A.

   - Solaris 10:

     ```
     # /usr/sbin/svcadm enable gab
     ```

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
   ```

   To start VCS using SMF service, use the following command:

   ```
   # svcadm enable vcs
   ```

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
```

Chapter 19

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.

See "Important preinstallation information for VCS" on page 31.

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
  /etc/default/llt
  /etc/default/gab
  /etc/default/vxfen
- 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 106.

```
Enter the NIC for the first private heartbeat
link on saturn: [b,q,?] qfe:0
```

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,?] qfe:1
```

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: qfe:2
```

Removing a node from a cluster

Table 19-1 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 19-1 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 219.
■ 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 219.
Modify the llthosts(4) and gabtab(4) files to reflect the change.	See "Modifying configuration files on each remaining node" on page 222.
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 223.
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 224.
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 packages.	See "Unloading LLT and GAB and removing VCS on the departing node" on page 224.

Verifying the status of nodes and service groups

Start by issuing the following commands from one of the nodes to remain in the cluster node galaxy or node nebula in our example.

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
   ```

   To stop VCS using SMF, run the following command:

   ```
   # svcadm disable vcs
   ```

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 /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 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. Stop the AT process.

   ```
   # /opt/VRTSvcs/bin/vcsauth/vcsauthserver/bin/vcsauthserver.sh \
   stop
   ```

2. Remove the credentials.

   ```
   # rm -rf /var/VRTSvcs/vcsauth/data/
   ```

Unloading LLT and GAB and removing VCS on the departing node

Perform the tasks on the node that is departing the cluster.

If you have configured VCS as part of the Storage Foundation and High Availability products, you may have to delete other dependent packages before you can delete all of the following ones.

To unconfigure and unload LLT and GAB and remove VCS

1. If you had configured I/O fencing in enabled mode, then stop I/O fencing.

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

2. Unconfigure GAB and LLT:

   ```
   # /sbin/gabconfig -U
   # /sbin/lltconfig -U
   ```

3. Unload the GAB and LLT modules from the kernel.

   - Determine the kernel module IDs:

     ```
     # modinfo | grep gab
     # modinfo | grep llt
     ```

     The module IDs are in the left-hand column of the output.

   - Unload the module from the kernel:

     ```
     # modunload -i gab_id
     # modunload -i llt_id
     ```

4. Disable the startup files to prevent LLT, GAB, or VCS from starting up:

   ```
   # /usr/sbin/svcadm disable -t llt
   # /usr/sbin/svcadm disable -t gab
   # /usr/sbin/svcadm disable -t vcs
   ```

5. To determine the packages to remove, enter:

   ```
   # pkginfo | grep VRTS
   ```

6 To permanently remove the VCS packages from the system, use the `pkgrm` command. Start by removing the following packages, which may have been optionally installed, in the order shown:

```
# pkgrm VRTSvcsea
# pkgrm VRTSat
# pkgrm VRTSvcsag
# pkgrm VRTScps
# pkgrm VRTSvcs
# pkgrm VRTSamf
# pkgrm VRTSvxfen
# pkgrm VRTSgab
# pkgrm VRTSllt
# pkgrm VRTSspt
# rpm -e VRTSsfcpi60
# pkgrm VRTSperl
# pkgrm VRTSvlic
```

7 Remove the LLT and GAB configuration files.

```
# rm /etc/llttab
# rm /etc/gabtab
# rm /etc/llthosts
```

8 Remove the language packages and patches.

Section 8

Installation reference

VCS installation packages

This appendix includes the following topics:

- Veritas Cluster Server installation packages

Veritas Cluster Server installation packages

Table A-1 shows the package name and contents for each Veritas Cluster Server package.

Table A-1 Veritas Cluster Server packages

Package	Contents	Required/Optional
VRTSamf	Contains the binaries for the Veritas Asynchronous Monitoring Framework kernel driver functionality for the Process and Mount based agents.	Required
VRTScps	Contains the binaries for the Veritas Coordination Point Server.	Optional. Required to Coordination Point Server (CPS).
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 binaries for Veritas.	Required

Table A-1 Veritas Cluster Server packages *(continued)*

Package	Contents	Required/Optional
VRTSsfcpi60	Veritas Storage Foundation Common Product Installer The Storage Foundation Common Product installer package contains the scripts that perform the following: ■ installation ■ configuration ■ upgrade ■ uninstallation ■ adding nodes ■ removing nodes ■ etc. You can use this script to simplify the native operating system installations, configurations, and upgrades.	Required
VRTSspt	Contains the binaries for Veritas Software Support Tools.	Recommended package, 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 and VRTSvlic.
VRTSvcsag	Contains the binaries for Veritas Cluster Server bundled agents.	Required Depends on VRTSvcs.

Table A-1 Veritas Cluster Server packages *(continued)*

Package	Contents	Required/Optional
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
VRTSvxfen	Contains the binaries for Veritas I/O Fencing .	Required to use fencing. Depends on VRTSgab.
VRTSsfmh	Veritas Storage Foundation Managed Recommended Host Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at: http://www.symantec.com/business/storage-foundation-manager	Recommended
VRTSvbs	Enables fault management and VBS command line operations on VCS nodes managed by Veritas Operations Manager. For more information, see the *Virtual Business Service–Availability User's Guide*.	Recommended Depends on VRTSsfmh. VRTSsfmh version must be 4.1 or later for VRTSvbs to get installed.
VRTSvcsnr	Network reconfiguration service for Oracle VM Server logical domains	Optional You must install VRTSvcsnr manually inside a Oracle VM Server logical domain if the domain is to be configured for disaster recovery.

Appendix B

Installation command options

This appendix includes the following topics:

- Command options for installvcs program
- Command options for uninstallvcs program

Command options for installvcs program

The `installvcs` command usage takes the following form:

```
installvcs [ system1
   system2... ]
        [ -install | -configure | -uninstall | -license
        | -upgrade | -precheck | -requirements | -start | -stop
        | -postcheck ]
        [ -responsefile response_file ]
        [ -logpath log_path ]
        [ -tmppath tmp_path ]
        [ -tunablesfile tunables_file ]
        [ -timeout timeout_value ]
        [ -keyfile ssh_key_file ]
        [ -hostfile hostfile_path ]
        [ -rootpath root_path ]
        [ -flash_archive flash_archive_path ]
        [ -serial | -rsh | -redirect | -installminpkgs
        | -installrecpkgs | -installallpkgs | -minpkgs
        | -recpkgs | -allpkgs | -pkgset | -pkgtable | -pkginfo
        | -makeresponsefile | -comcleanup  | -version | -nolic
        | -ignorepatchreqs | -settunables | -security | -securityonenode
        | -securitytrust | -addnode | -fencing | -upgrade_kernelpkgs
        | -upgrade_nonkernelpkgs | -rolling_upgrade
        | -rollingupgrade_phase1        | -rollingupgrade_phase2 ]
```

Table B-1 provides a consolidated list of the options used with the `installvcs` command and `uninstallvcs` command.

Table B-1 installvcs and uninstallvcs 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 packages. The installvcs program lists the packages 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 ssh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.
`-configure`	Configure VCS after using `-install` option to install VCS.

Table B-1 installvcs and 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 6.0 PR1 release, the *release_name* is UXRT60.
`-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.
`-install`	Install product packages on systems without configuring VCS.
`-installallpkgs`	Select all the packages for installation. See the `-allpkgs` option.
`-installminpkgs`	Select the minimum packages for installation. See the `-minpkgs` option.

Table B-1 installvcs and uninstallvcs options *(continued)*

Option and Syntax	Description
`-installrecpkgs`	Select the recommended packages 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.
`-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`	Generate a response file. No actual software installation occurs when you use this option. Create a response file or to verify that your system configuration is ready for uninstalling VCS.
`-minpkgs`	View a list of the minimal packages for VCS. The installvcs program lists the packages in the correct installation order. The list does not include the optional packages. 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 packages on systems without licensing or configuration. License-based features or variants are not installed when you use this option.
`-pkginfo`	Display a list of packages 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 packages are displayed.
`-pkgpath` *`pkg_path`*	Specify that *pkg_path* contains all packages that the installvcs program is about to install on all systems. The *pkg_path* is the complete path of a directory, usually NFS mounted.

Table B-1 installvcs and uninstallvcs options *(continued)*

Option and Syntax	Description
`-pkgset`	Discover and lists the 6.0 PR1 packages installed on the systems that you specify.
`-pkgtable`	Display the VCS 6.0 PR1 packages 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 66.
`-recpkgs`	View a list of the recommended packages for VCS. The installvcs program lists the packages in the correct installation order. The list does not include the optional packages. 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.
`-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 141. See "Configuring VCS using response files" on page 147.
`-rootpath` *`root_path`*	Specify that root_path is the root location for the installation of all packages. On Solaris, `-rootpath` passes `-R` *`root_path`* to pkgadd command.

Table B-1 installvcs and uninstallvcs options *(continued)*

Option and Syntax	Description
`-redirect`	Specify that the installer need not display the progress bar details during the installation.
`-rsh`	Specify that *rsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *rsh* commands between systems execute without prompting for passwords or confirmations
`-security`	Enable or disable secure mode in a VCS cluster. See the *Veritas Cluster Server Administrator's Guide* for instructions.
`-securityonenode`	Form a secure cluster node by node in environments that do not support passwordless ssh or passwordless rsh. See "Configuring a secure cluster node by node" on page 113.
`-securitytrust`	Set up a trust relationship between your VCS cluster and a broker. See "Setting up trust relationships for your VCS cluster" on page 112.
`-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.
`-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 288.
`-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 288.

Table B-1 installvcs and uninstallvcs options *(continued)*

Option and Syntax	Description
`-timeout`	Specifies the timeout value (in seconds) for each command that the installer issues during the installation. The default timeout value is set to 600 seconds.
`-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 packages on remote systems before installation.
`-uninstall`	Uninstall VCS from the systems that you specify.
`-upgrade`	Upgrade the installed packages on the systems that you specify.
`-rollingupgrade_phase1`	Upgrade the product kernel packages to the latest version during rolling upgrade Phase 1.
`-rollingupgrade_phase2`	Upgrade the VCS and other agent packages to the latest version during rolling upgrade Phase 2. 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 packages for the product. Provide a summary that includes the count of the installed and any missing packages. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.
`-settunables`	Set tunable parameters after a product is installed and configured. Processes of the installed product may need to be restarted for the tunable parameter values to take effect. This option must be used together with `-tunablesfile` option.
`-tunablesfile`	Specify a tunables file including tunable parameters to be set.
`-upgrade_kernelpkgs`	Has been renamed to `-rollingupgrade_phase1`
`-upgrade_nonkernelpkgs`	Has been renamed to `-rollingupgrade_phase2`

Command options for uninstallvcs program

The `uninstallvcs` command usage takes the following form:

```
uninstallvcs [ system1
   system2... ]
        [ -uninstall ]
        [ -responsefile response_file ]
        [ -logpath log_path ]
        [ -tmppath tmp_path ]
        [ -tunablesfile tunables_file ]
        [ -timeout timeout_value ]
        [ -keyfile ssh_key_file ]
        [ -hostfile hostfile_path ]
        [ -rootpath root_path ]
        [ -flash_archive flash_archive_path ]
        [ -serial | -rsh | -redirect | -makeresponsefile
        | -comcleanup | -version | -nolic | -ignorepatchreqs
        | -settunables | -security | -securityonenode
        | -securitytrust | -addnode | -fencing | -upgrade_kernelpkgs
        | -upgrade_nonkernelpkgs | -rolling_upgrade
       | -rollingupgrade_phase1
        | -rollingupgrade_phase2 ]
```

For description of the `uninstallvcs` command options:

See Table B-1 on page 234.

Configuration files

This appendix includes the following topics:

- About the LLT and GAB configuration files
- About the AMF configuration files
- About the VCS configuration files
- About I/O fencing configuration files
- Sample configuration files for CP server

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 C-1 lists the LLT configuration files and the information that these files contain.

Table C-1 LLT configuration files

File	Description
/etc/default/llt	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`

Table C-1 LLT configuration files *(continued)*

File	Description

/etc/llttab	The file `llttab` contains the information that is derived during installation and used by the utility `lltconfig(1M)`. After installation, this file lists the private network links that correspond to the specific system. For example, the file /etc/llttab contains the entries that resemble the following:
	- For Solaris SPARC:
	`set-node galaxy`
	`set-cluster 2`
	`link net1 /dev/net/net1 - ether - -`
	`link net2 /dev/net/net2 - ether - -`
	- For Solaris x64:
	`set-node galaxy`
	`set-cluster 2`
	`link net1 /dev/net/net1 - ether - -`
	`link net2 /dev/net/net2 - ether - -`
	The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.
	If you configured a low priority link under LLT, the file also includes a "link-lowpri" line.
	Refer to the `llttab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `llttab` file.

Table C-2 lists the GAB configuration files and the information that these files contain.

Table C-2 GAB configuration files

File	Description
/etc/default/gab	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 C-3 lists the AMF configuration files.

Table C-3 AMF configuration files

File	Description
/etc/default/amf	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. (default) 0—Indicates that AMF is disabled to start up. ■ 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 247.
  See "Sample main.cf file for global clusters" on page 248.

- 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/default/vcs

  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.

  - ONENODE—Option for VCS to form a single node cluster. Valid values include:

    Yes—Indicates that VCS is started as a single node cluster.

    No—Indicates that VCS is not set to form a single node cluster.

  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 "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 Solaris systems.

Sample main.cf file for VCS clusters

The following sample main.cf file is for a three-node cluster in secure mode.

```
include "types.cf"
include "OracleTypes.cf"
include "OracleASMTypes.cf"



cluster vcs02 (
    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
    )

NIC csgnic (
    Device = hme0
    NetworkHosts = { "10.182.13.1" }
    )
```

```
NotifierMngr ntfr (
   SnmpConsoles = { jupiter" = SevereError }
   SmtpServer = "smtp.example.com"
   SmtpRecipients =  { "ozzie@example.com" = SevereError }
   )

ntfr requires csgnic

// resource dependency tree
//
//     group ClusterService
//     {
//     NotifierMngr ntfr
//         {
//         NIC csgnic
//         }
// }
```

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.

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 = hme0
    Address = "10.182.13.50"
    NetMask = "255.255.240.0"
    )

NIC csgnic (
    Device = hme0
    NetworkHosts = { "10.182.13.1" }
    )

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
//              }
//          }
//      }
```

About I/O fencing configuration files

Table C-4 lists the I/O fencing configuration files.

Table C-4 I/O fencing configuration files

File	Description
/etc/default/vxfen	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 C-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 ■ dmp—Configure the vxfen module to use DMP devices The disk policy is dmp by default. If you use iSCSI devices, you must set the disk policy as dmp. ■ raw—Configure the vxfen module to use the underlying raw character devices **Note:** You must use the same SCSI-3 disk policy on all the nodes. ■ security This parameter is applicable only for server-based fencing. 1—Indicates that communication with the CP server is in secure mode. This setting is the default. 0—Indicates that communication with the CP server is in non-secure mode. ■ 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 and multiple IP addresses for each CP server. ■ single_cp This parameter is applicable for server-based fencing which uses a single highly available CP server as its coordination point. Also applicable for when you use a coordinator disk group with single disk. ■ autoseed_gab_timeout This parameter enables GAB automatic seeding of the cluster even when some cluster nodes are unavailable. This feature requires that I/O fencing is enabled. 0—Turns the GAB auto-seed feature on. Any value greater than 0 indicates the number of seconds that GAB must delay before it automatically seeds the cluster. -1—Turns the GAB auto-seed feature off. This setting is the default.

Table C-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.
	For disk-based I/O fencing, the /etc/vxfentab file on each node contains a list of all paths to each coordinator disk. An example of the /etc/vxfentab file in a disk-based fencing configuration on one node resembles as follows:
	■ Raw disk:
	`/dev/rdsk/c1t1d0s2`
	`/dev/rdsk/c2t1d0s2`
	`/dev/rdsk/c3t1d2s2`
	■ DMP disk:
	`/dev/vx/rdmp/c1t1d0s2`
	`/dev/vx/rdmp/c2t1d0s2`
	`/dev/vx/rdmp/c3t1d0s2`
	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

The `/etc/vxcps.conf` file determines the configuration of the coordination point server (CP server.)

See "Sample CP server configuration (/etc/vxcps.conf) file output" on page 258.

The 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 253.
- 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 255.

Note: The CP server supports Internet Protocol version 4 or version 6 (IPv4 or IPv6 addresses) when communicating with VCS clusters (application clusters). The 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"
include "/opt/VRTScps/bin/Quorum/QuorumTypes.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 cpsvip1 (
            Critical = 0
            Device @mycps1 = hme0
            Address = "10.209.3.1"
            NetMask = "255.255.252.0"
            )

      IP cpsvip2 (
            Critical = 0
            Device @mycps1 = qfe:0
            Address = "10.209.3.2"
            NetMask = "255.255.252.0"
            )

      NIC cpsnic1 (
           Critical = 0
           Device @mycps1 = hme0
           PingOptimize = 0
           NetworkHosts @mycps1 = { "10.209.3.10 }
           )

      NIC cpsnic2 (
           Critical = 0
           Device @mycps1 = qfe:0
           PingOptimize = 0
           )

      Process vxcpserv (
           PathName = "/opt/VRTScps/bin/vxcpserv"
           ConfInterval = 30
           RestartLimit = 3
           )

      Quorum quorum (
            QuorumResources = { cpsvip1, cpsvip2 }
            )

cpsvip1 requires cpsnic1
cpsvip2 requires cpsnic2
vxcpserv requires quorum


// resource dependency tree
//
// group CPSSG
// {
// IP cpsvip1
```

```
 //     {
 //     NIC cpsnic1
 //     }
 // IP cpsvip2
 //     {
 //     NIC cpsnic2
 //     }
 // Process vxcpserv
 //     {
 //     Quorum quorum
 //     }
 // }
```

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"
include "/opt/VRTScps/bin/Quorum/QuorumTypes.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 cpsvip1 (
            Critical = 0
            Device @mycps1 = hme0
            Device @mycps2 = hme0
            Address = "10.209.81.88"
            NetMask = "255.255.252.0"
            )

      IP cpsvip2 (
            Critical = 0
            Device @mycps1 = qfe:0
            Device @mycps2 = qfe:0
            Address = "10.209.81.89"
            NetMask = "255.255.252.0"
            )

      Mount cpsmount (
            MountPoint = "/etc/VRTScps/db"
            BlockDevice = "/dev/vx/dsk/cps_dg/cps_volume"
            FSType = vxfs
            FsckOpt = "-y"
            )

      NIC cpsnic1 (
           Critical = 0
           Device @mycps1 = hme0
           Device @mycps2 = hme0
           PingOptimize = 0
           NetworkHosts @mycps1 = { "10.209.81.10 }
           )
      NIC cpsnic2 (
           Critical = 0
           Device @mycps1 = qfe:0
           Device @mycps2 = qfe:0
           PingOptimize = 0
           )

      Process vxcpserv (
            PathName = "/opt/VRTScps/bin/vxcpserv"
            )

      Quorum quorum (
            QuorumResources = { cpsvip1, cpsvip2 }
            )

      Volume cpsvol (
            Volume = cps_volume
            DiskGroup = cps_dg
            )

 cpsmount requires cpsvol
 cpsvip1 requires cpsnic1
 cpsvip2 requires cpsnic2
 cpsvol requires cpsdg
 vxcpserv requires cpsmount
 vxcpserv requires quorum


 // resource dependency tree
 //
 // group CPSSG
 // {
 // IP cpsvip1
 //     {
 //     NIC cpsnic1
 //     }
 // IP cpsvip2
 //     {
 //     NIC cpsnic2
 //     }
 // Process vxcpserv
 //     {
```

```
//     Quorum quorum
//     Mount cpsmount
//         {
//         Volume cpsvol
//             {
//             DiskGroup cpsdg
//             }
//         }
//     }
// }
```

Sample CP server configuration (/etc/vxcps.conf) file output

The following is an example of a coordination point server (CP server) configuration file `/etc/vxcps.conf` output.

```
##  The vxcps.conf file determines the
## configuration for Veritas CP Server.
cps_name=mycps1
vip=[10.209.81.88]
vip=[10.209.81.89]:56789
port=14250
security=1
db=/etc/VRTScps/db
```

Appendix D

Installing VCS on a single node

This appendix includes the following topics:

- About installing VCS on a single node
- Creating a single-node cluster using the installer program
- Verifying single-node operation

About installing VCS on a single node

You can install VCS 6.0 PR1 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 259.

Creating a single-node cluster using the installer program

Table D-1 specifies the tasks that are involved to install VCS on a single node using the installer program.

Table D-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 260.
Install the VCS software on the system using the installer.	See "Starting the installer for the single node cluster" on page 260.

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, enable 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 21.

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. While you configure, the installer 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.

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 the SMF command.

```
# svcadm enable system/vcs-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 E

Configuring LLT over UDP

This appendix includes the following topics:

Using the UDP layer for LLT

VCS 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 separate subnets. Set the broadcast address in /etc/llttab explicitly depending on the subnet for each link.

See “Broadcast address in the /etc/llttab file” on page 264.

- Make sure that each NIC has an IP address that is configured before configuring LLT.
- Make sure the IP addresses in the /etc/llttab 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 266.
- Set the broadcast address correctly for direct-attached (non-routed) links.
  See “Sample configuration: direct-attached links” on page 268.
- For the links that cross an IP router, disable broadcast features and specify the IP address of each link manually in the /etc/llttab file.
  See “Sample configuration: links crossing IP routers” on page 270.

Broadcast address in the /etc/llttab file

The broadcast address is set explicitly for each link in the following example.

- Display the content of the /etc/llttab file on the first node galaxy:

  ```
  galaxy # cat /etc/llttab

  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.
- Display the content of the /etc/llttab file on the second node nebula:

  ```
  nebula # cat /etc/llttab

  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.

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 268.
- See "Sample configuration: links crossing IP routers" on page 270.

Table E-1 describes the fields of the link command that are shown in the /etc/llttab file examples. Note that some of the fields differ from the command for standard LLT links.

Table E-1 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/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 266.
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.
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/llttab file

The `set-addr` command in the /etc/llttab 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 270.

Table E-2 describes the fields of the set-addr command.

Table E-2 Field description for set-addr command in /etc/llttab

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 | more
UDP
   Local Address         Remote Address     State
-------------------- -------------------- -------
      *.sunrpc                              Idle
      *.*                                   Unbound
      *.32771                               Idle
      *.32776                               Idle
      *.32777                               Idle
      *.name                                Idle
      *.biff                                Idle
      *.talk                                Idle
      *.32779                               Idle
.
.
.
      *.55098                               Idle
      *.syslog                              Idle
```

```
     *.58702                                      Idle
     *.*                                          Unbound
```

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:

```
# ifconfig interface_name netmask netmask
```

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.

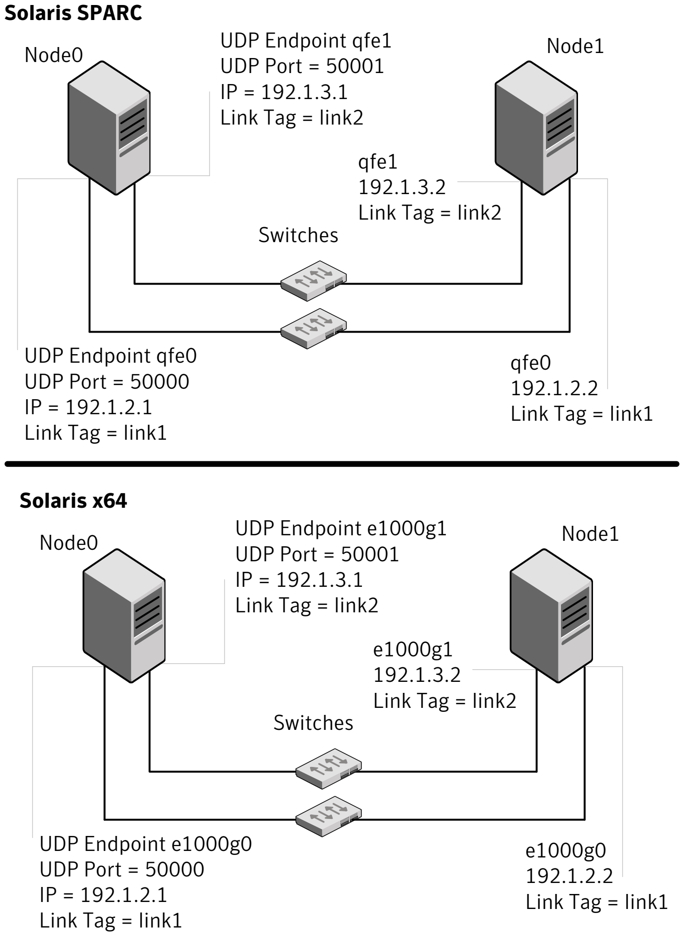
An example of a typical /etc/llttab file when nodes are on different subnets. Note the explicitly set broadcast address for each link.

```
# 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 E-1 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure E-1 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 broadcasts requests peer nodes to discover their addresses. So the addresses of peer nodes do not need to be specified in the /etc/llttab file using the `set-addr` command. For direct attached links, you do need to set the broadcast address of the links in the /etc/llttab file. Verify that the IP addresses and broadcast addresses are set correctly by using the `ifconfig -a` 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
```

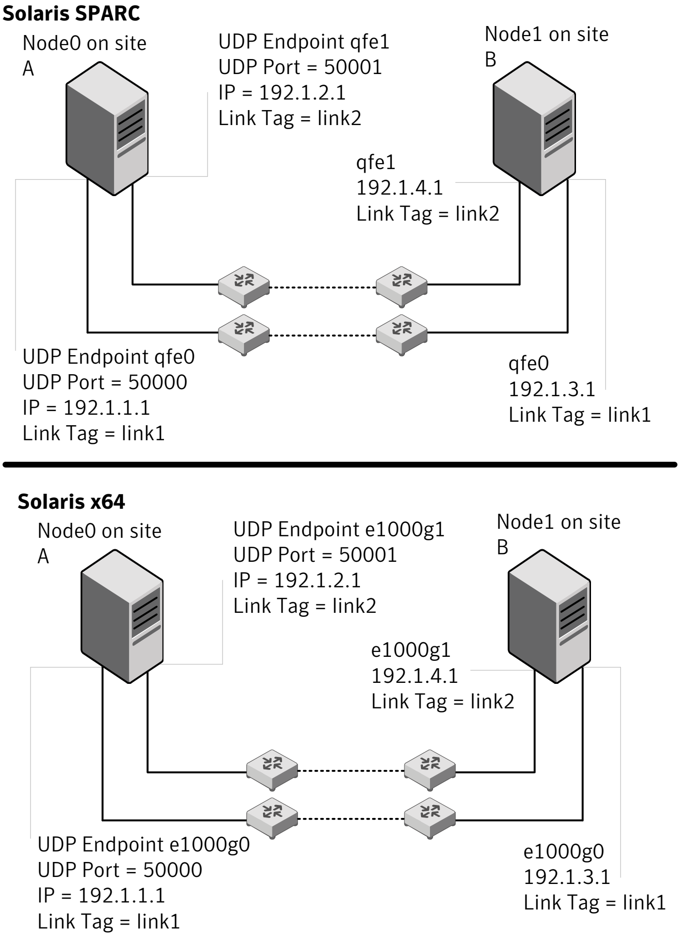
The file for Node 1 resembles:

```
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 E-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 E-2 A typical configuration of links crossing an IP router



The configuration that the following `/etc/llttab` 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/llttab` 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 274.
- 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 277.

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 275.
- See "Sample configuration: links crossing IP routers" on page 277.

Note that some of the fields in Table E-3 differ from the command for standard LLT links.

Table E-3 describes the fields of the link command that are shown in the /etc/llttab file examples.

Table E-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 274.
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.

Table E-3 Field description for link command in /etc/llttab *(continued)*

Field	Description
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 277.

Table E-4 describes the fields of the set-addr command.

Table E-4 Field description for set-addr command in /etc/llttab

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 |  more
```

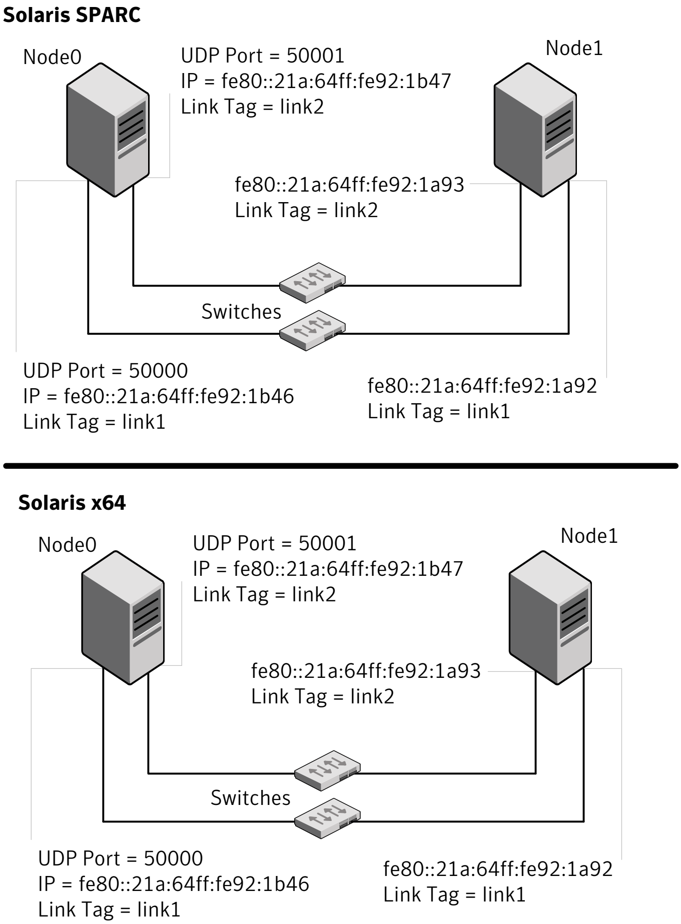
```
UDP: IPv4
   Local Address        Remote Address      State
-------------------- -------------------- ----------
      *.sunrpc                             Idle
      *.*                                 Unbound
      *.32772                             Idle
      *.*                                 Unbound
      *.32773                             Idle
      *.lockd                             Idle
      *.32777                             Idle
      *.32778                             Idle
      *.32779                             Idle
      *.32780                             Idle
      *.servicetag                        Idle
      *.syslog                            Idle
      *.16161                             Idle
      *.32789                             Idle
      *.177                               Idle
      *.32792                             Idle
      *.32798                             Idle
      *.snmpd                             Idle
      *.32802                             Idle
      *.*                                 Unbound
      *.*                                 Unbound
      *.*                                 Unbound

UDP: IPv6
   Local Address             Remote Address           State      If
------------------------- ------------------------- ---------- -----
      *.servicetag                                  Idle
      *.177                                         Idle
```

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 E-3 depicts a typical configuration of direct-attached links employing LLT over UDP.

Figure E-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 -a` command to verify that the IPv6 address is set correctly.

```
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 -
```

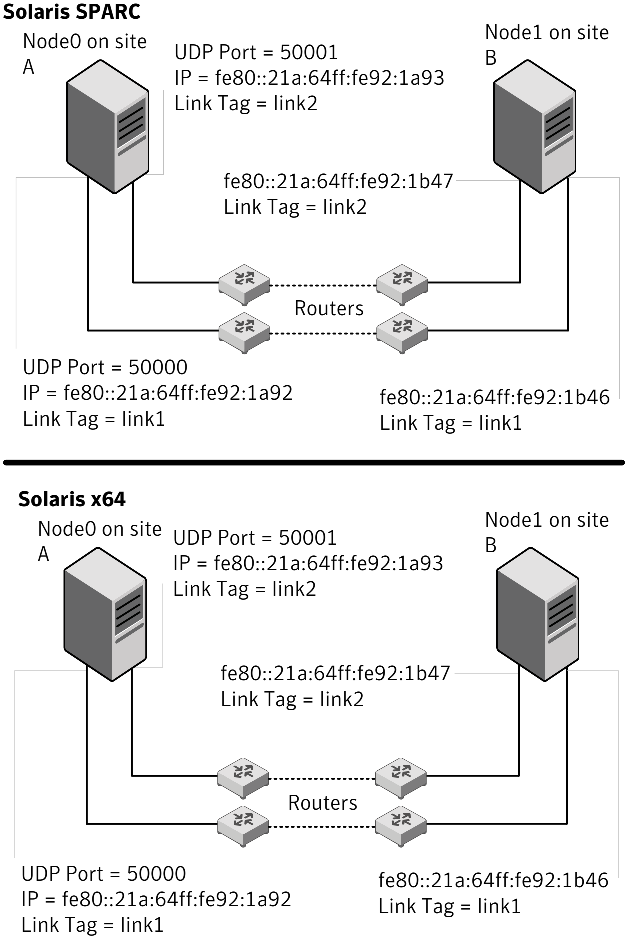
The file for Node 1 resembles:

```
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 E-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 E-4 A typical configuration of links crossing an IP router



The configuration that the following `/etc/llttab` 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/llttab` 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 e1000g1 /dev/udp - udp 50000 - 192.168.10.1 -
link e1000g2 /dev/udp - udp 50001 - 192.168.11.1 -
link-lowpri e1000g0 /dev/udp - udp 50004 - 10.200.58.205 -
set-addr 1 e1000g1 192.168.10.2
```

```
set-addr 1 e1000g2 192.168.11.2
set-addr 1 e1000g0 10.200.58.206
set-bcasthb 0
set-arp 0
```

Appendix F

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

- Setting up inter-system communication

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 rsh commands on all systems in the cluster. If ssh is used to communicate between systems, it must be configured in a way such that it operates without requests for passwords or passphrases. Similarly, rsh must be configured in such a way to not prompt for passwords.

If system communication is not possible between systems using ssh or rsh, 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, rsh, and rcp.

Configuring ssh

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

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

To configure ssh

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

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

   System output similar to the following is displayed:

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

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

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

4. Do not enter a passphrase. Press **Enter**. Enter same passphrase again. Press **Enter** again.
5. Make sure the /.ssh directory is on all the target installation systems. If that directory is absent, create it on the target system and set the write permission to root only:

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

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

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

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

```
# svcadm restart ssh
```

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

```
# sftp target_sys
```

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

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

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

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

10 Enter the root password.

11 At the sftp prompt, type the following command:

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

The following output is displayed:

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

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

```
sftp> quit
```

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

```
 # ssh target_sys
```

14 Enter the root password at the prompt:

```
password:
```

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

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

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

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

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

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

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

```
# exit
```

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

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

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

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

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

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

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

Appendix G

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:

  ```
  # /opt/VRTS/bin/vxkeyless
  ```

- 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.

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.

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
```

Check the log files that get generated in the `/var/svc/log` directory for any errors.

Recommended action: Ensure that all systems on the network have unique clusterid-nodeid pair. You can use the `lltdump -f` *`device`* `-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 G-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 G-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.
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 different root brokers, and trust is not established between the authentication brokers:

Appendix H

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

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:

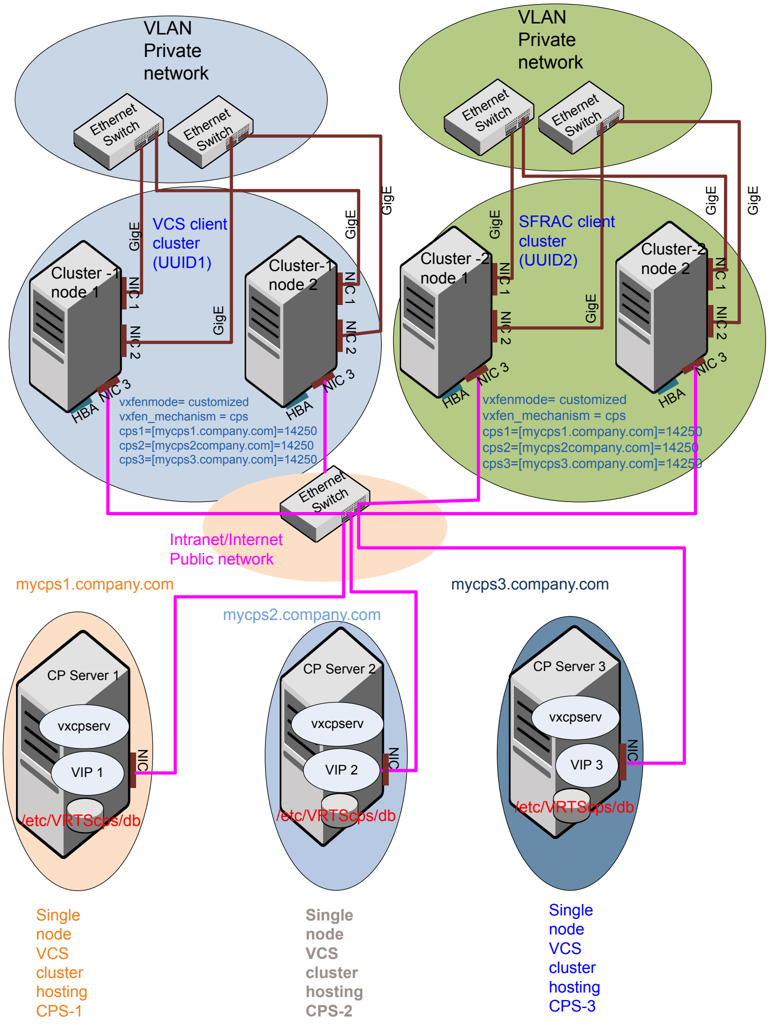
- Two unique client clusters that are served by 3 CP servers:
  See Figure H-1 on page 294.
- Client cluster that is served by highly available CP server and 2 SCSI-3 disks:
  Figure H-2
- Two node campus cluster that is served be remote CP server and 2 SCSI-3 disks:
  Figure H-3
- Multiple client clusters that are served by highly available CP server and 2 SCSI-3 disks:
  Figure H-4

Two unique client clusters served by 3 CP servers

Figure H-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 H-1 Two unique client clusters served by 3 CP servers



```
vxfenmode= customized
vxfen_mechanism = cps
cps1=[mycps1.company.com]=14250
cps2=[mycps2company.com]=14250
cps3=[mycps3.company.com]=14250
```

```
vxfenmode= customized
vxfen_mechanism = cps
cps1=[mycps1.company.com]=14250
cps2=[mycps2company.com]=14250
cps3=[mycps3.company.com]=14250
```

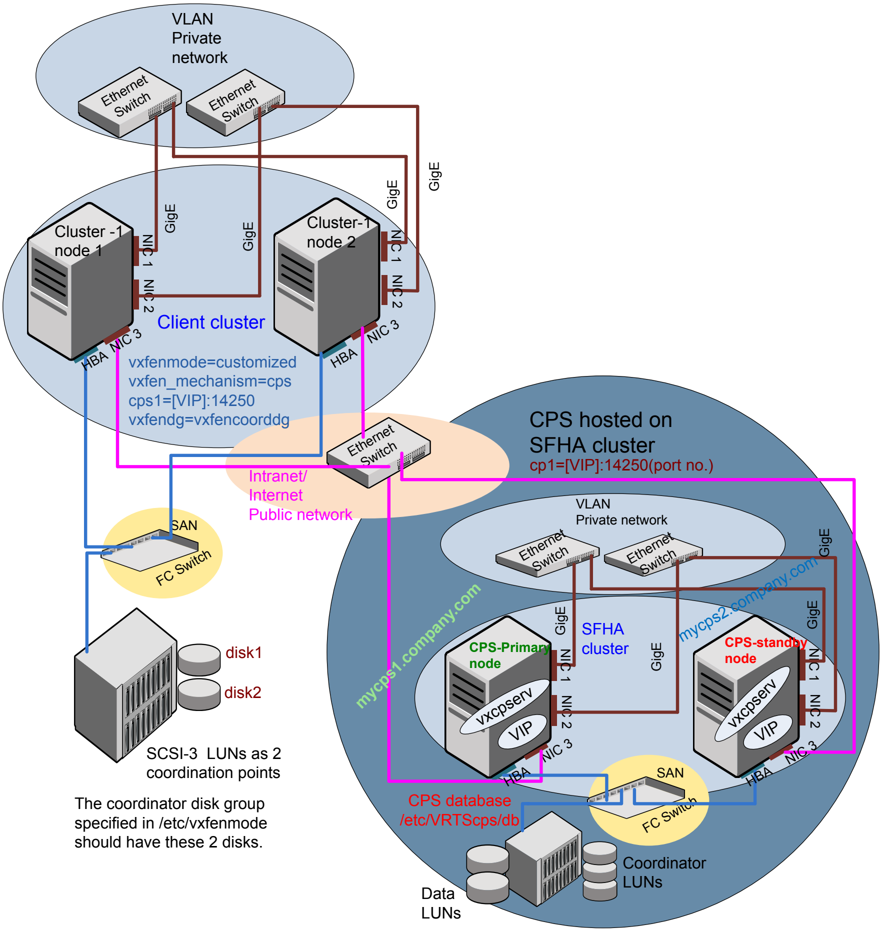
Client cluster served by highly available CPS and 2 SCSI-3 disks

Figure H-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 H-2 Client cluster served by highly available CP server and 2 SCSI-3 disks



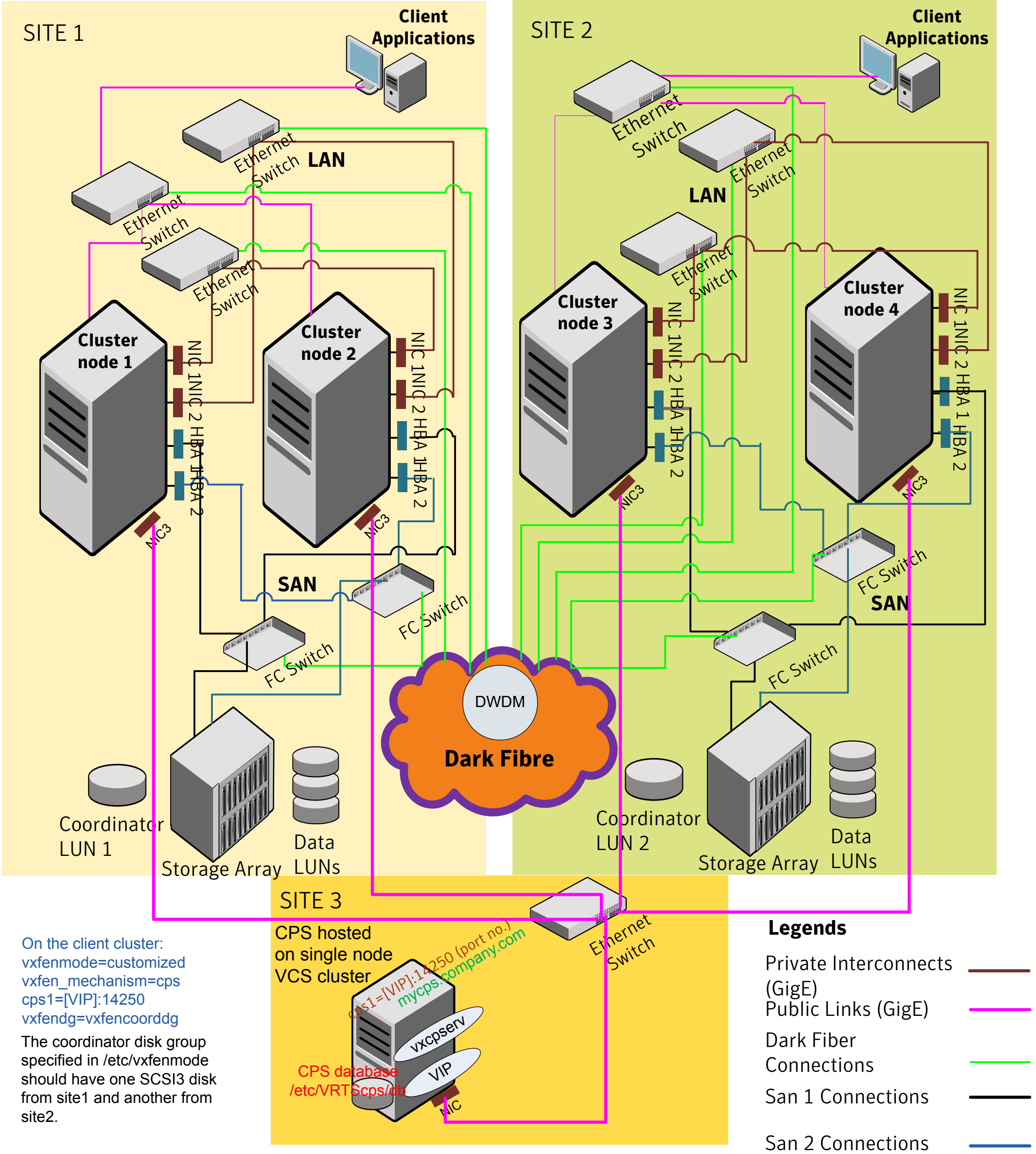
Two node campus cluster served by remote CP server and 2 SCSI-3 disks

Figure H-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 H-3 Two node campus cluster served by remote CP server and 2 SCSI-3



On the client cluster:
vxfenmode=customized
vxfen_mechanism=cps
cps1=[VIP]:14250
vxfendg=vxfencoorddg

The coordinator disk group specified in /etc/vxfenmode should have one SCSI3 disk from site1 and another from site2.

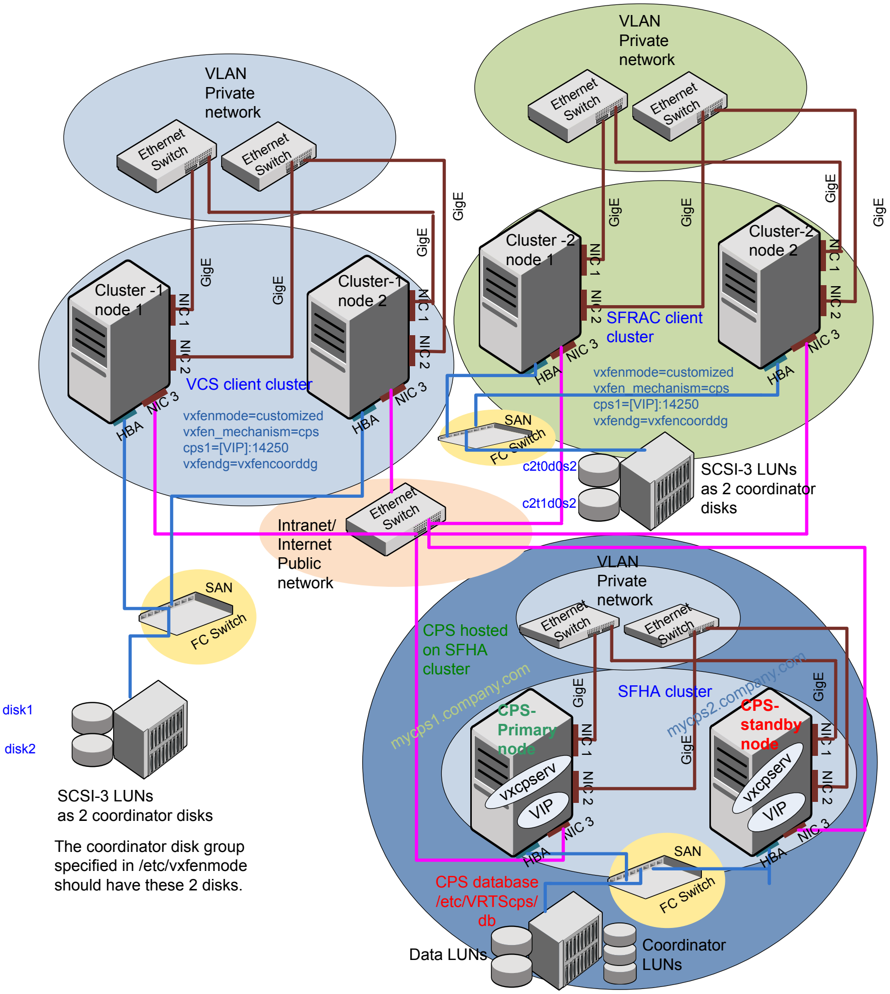
Multiple client clusters served by highly available CP server and 2 SCSI-3 disks

Figure H-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 H-4 Multiple client clusters served by highly available CP server and 2 SCSI-3 disks



Reconciling major/minor numbers for NFS shared disks

This appendix includes the following topics:

- Reconciling major/minor numbers for NFS shared disks

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/c1t1d0s2`.

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 Solaris 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/c1t1d0s2
```

Output on Node A resembles:

```
crw-r-----  1 root  sys  32,1 Dec 3 11:50 /dev/dsk/c1t1d0s2
```

Output on Node B resembles:

```
crw-r-----  1 root  sys  32,1 Dec 3 11:55 /dev/dsk/c1t1d0s2
```

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/c1t1d0s2
   ```

   Output on Node B:

   ```
   crw-r-----  1 root  sys  36,1 Dec 3 11:55 /dev/dsk/c1t1d0s2
   ```

2. Place the VCS command directory in your path.

   ```
   # 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/c1t1d0s2
```

Output from this command resembles the following on Node A:

```
    lrwxrwxrwx  1 root  root  83 Dec 3 11:50
     /dev/dsk/c1t1d0s2         -> ../../
     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.

Appendix J

Compatability issues when installing Veritas Cluster Server with other products

This appendix includes the following topics:

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx, VRTSicsco, and VRTSat.

Index