# Veritas Cluster Server Installation Guide

Linux for IBM Power

5.0 Release Update 3

symantec™

# Veritas Cluster Server Installation Guide

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

Product version: 5.0 RU3

Document version: 5.0RU3.0

## Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

# Technical Support

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

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

## Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

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

## Licensing and registration

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

www.symantec.com/techsupp/

## Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

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

## Documentation feedback

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

## Maintenance agreement resources

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

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

## Additional enterprise services

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

Enterprise services that are available include the following:

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

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

www.symantec.com

Select your country or language from the site index.

# Contents

Chapter 1

# Introducing Veritas Cluster Server

This chapter includes the following topics:



## About Veritas Cluster Server

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

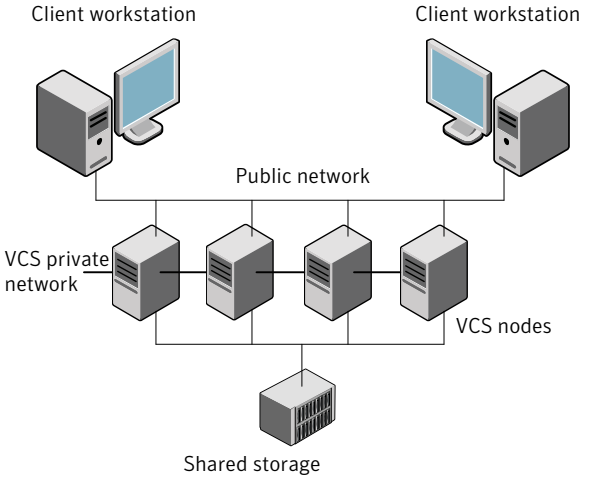
## About VCS basics

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

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

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

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




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

## About multiple nodes

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

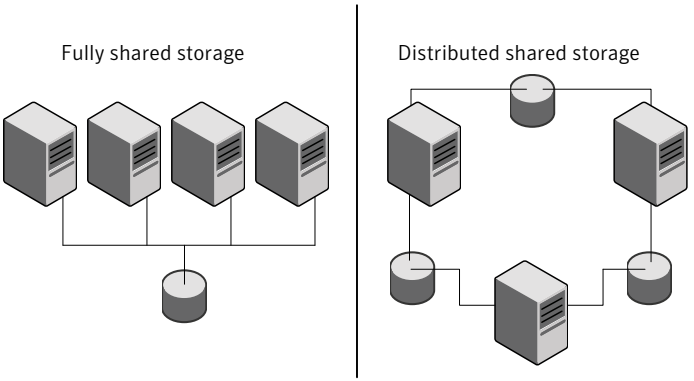
## About shared storage

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

VCS nodes can only access physically-attached storage.

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

**Figure 1-2** Two examples of shared storage configurations




## About LLT and GAB

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

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

LLT configuration files are as follows:

- /etc/llthosts—lists all the nodes in the cluster
- /etc/llttab file—describes the local system's private network links to the other nodes in the cluster

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

See "About the LLT and GAB configuration files" on page 105.

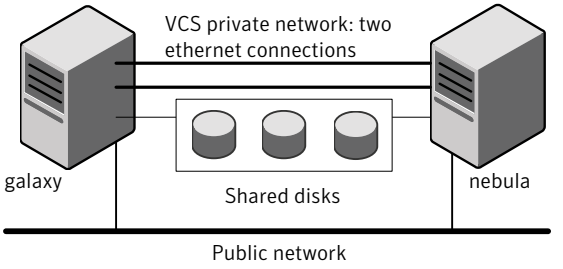
## About network channels for heartbeating

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 Linux for IBM Power 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 User's Guide*.

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

**Figure 1-3** Two Ethernet connections connecting two nodes




## About preexisting network partitions

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

## About VCS seeding

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

GAB automatically seeds nodes under the following conditions:

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

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

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

# About VCS features

You can use the Veritas Installation Assessment Service to assess your setup for VCS installation.

See "Veritas Installation Assessment Service" on page 17.

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

| | |
|---|---|
| VCS notifications | See "About VCS notifications" on page 17. |
| VCS global clusters | See "About global clusters" on page 17. |
| I/O fencing | See "About I/O fencing" on page 18. |

## Veritas Installation Assessment Service

The Veritas Installation Assessment Service (VIAS) utility assists you in getting ready for a Veritas Storage Foundation and High Availability Solutions installation or upgrade. The VIAS utility allows the preinstallation evaluation of a configuration, to validate it prior to starting an installation or upgrade.

https://vias.symantec.com/

## About VCS notifications

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

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

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

## About 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 User'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.

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

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 installvcs program installs the VCS I/O fencing driver, VRTSvxfen. 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.

---

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

---

# About VCS optional components

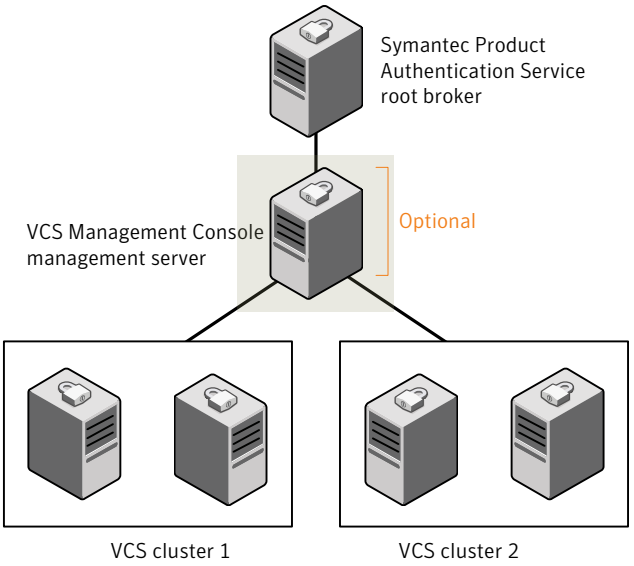
You can add the following optional components to VCS:

| | |
|---|---|
| Symantec Product Authentication Service | See "About Symantec Product Authentication Service (AT)" on page 19. |
| Veritas Cluster Server Management Console | See "About Veritas Cluster Server Management Console" on page 20. |
| Cluster Manager (Java console) | See "About Cluster Manager (Java Console)" on page 20. |
| VCS Simulator | See "About VCS Simulator" on page 20. |

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

Figure 1-4 illustrates a sample VCS deployment with the optional components configured.

**Figure 1-4** Typical VCS setup with optional components




## About Symantec Product Authentication Service (AT)

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

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

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

See Symantec Product Authentication Service documentation for more information.

See "Preparing to configure the clusters in secure mode" on page 29.

## About Cluster Manager (Java Console)

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

You can perform many administrative operations using the Java Console. You can also perform these operations using the command line interface or using the Veritas Cluster Server Management Console.

See "Installing the Java Console" on page 80.

See *Veritas Cluster Server User's Guide*.

## About Veritas Cluster Server Management Console

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

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

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

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

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

## About 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.

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 on a Windows system and test VCS

configurations for Windows, Linux, and Solaris clusters. VCS Simulator also enables creating and testing global clusters.

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

Chapter 2

# Planning to install VCS

This chapter includes the following topics:



## About planning to install VCS

Every node where you want to install VCS must meet the hardware and software requirements.

For the latest information on updates, patches, and software issues, read the following Veritas Technical Support TechNote:

http://entsupport.symantec.com/docs/285834

To find information on supported hardware, see the hardware compatibility list (HCL) in the following TechNote:

http://entsupport.symantec.com/docs/286819

## Hardware requirements

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

**Table 2-1** Hardware requirements for a VCS cluster

| Item | Description |
|---|---|
| VCS nodes | From 1 to 32 Linux PPC systems running the supported Linux PPC operating system version. |
| 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.<br>The VCS I/O fencing feature requires that all data and coordinator disks support SCSI-3 Persistent Reservations (PR).<br>See "About setting up disk-based I/O fencing" on page 89. |
| Disk space | **Note:** VCS may require more temporary disk space during installation than the specified disk space. |
| Network Interface Cards (NICs) | In addition to the built-in public NIC, VCS requires at least one more NIC per system. Symantec recommends two additional NICs.<br>You can also configure aggregated 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 256 megabytes. |

## Required disk space

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

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

**Table 2-2** Disk space requirements and totals

| Packages | / | /opt | /usr | /var | Totals |
|---|---|---|---|---|---|
| Required | 3 MB | 271 MB | 8 MB | 1 MB | 283 MB |
| Optional | 1 MB | 52 MB | 0 MB | 7 MB | 60 MB |
| Required and optional total | 4 MB | 323 MB | 8 MB | 8 MB | 343 MB |

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

# Supported operating systems

VCS operates on the Linux operating systems and kernels distributed by Red Hat and SUSE.

Table 2-3 lists the supported operating system versions for Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES). The table also lists the supported kernel versions and the architecture.

**Table 2-3** Supported Linux operating system and kernel versions

| Operating System | Kernel | Architecture |
|---|---|---|
| RHEL 5 Update 1 | 2.6.18-53.el5 | ppc64 |
| RHEL 5 Update 2 | 2.6.18-92.el5 | ppc64 |
| SLES 10 with SP1 | 2.6.16.46-0.12-default<br>2.6.16.46-0.12-smp | ppc64 |
| SLES 10 with SP2 | 2.6.16.60-0.21-default<br>2.6.16.60-0.21-smp | ppc64 |

**Note:** If your system runs an older version of either Red Hat Enterprise Linux or SUSE Linux Enterprise Server, you must upgrade the operating system before you attempt to install the VCS software. Refer to the Red Hat or SUSE documentation for more information on upgrading your system.

Symantec supports only Red Hat and SUSE distributed kernel binaries.

Symantec products operate on subsequent kernel and patch releases provided the operating systems maintain kernel ABI (application binary interface) compatibility.

Information about the latest supported Red Hat erratas and updates and SUSE service packs is available in the following TechNote. The TechNote also includes any updates to the supported operating systems and software. Read this TechNote before you install Symantec products.

http://entsupport.symantec.com/docs/285834

# Required Linux RPMs for VCS

Make sure you installed the following operating system-specific RPMs on the systems where you want to install or upgrade VCS. VCS will support any updates made to the following RPMs, provided the RPMs maintain the ABI compatibility.

Table 2-4 lists the RPMs that VCS requires for a given Linux operating system.

**Table 2-4** Required RPMs

| Operating system | Required RPMs |
|---|---|
| RHEL 5 | glibc-2.5-34.ppc.rpm<br>glibc-2.5-34.ppc64.rpm<br>glibc-common-2.5-34.ppc.rpm<br>libgcc-4.1.2-44.el5.ppc.rpm<br>libgcc-4.1.2-44.el5.ppc64.rpm<br>compat-libgcc-296-2.96-138.ppc.rpm<br>libstdc++-4.1.2-44.el5.ppc.rpm<br>libstdc++-4.1.2-44.el5.ppc64.rpm<br>compat-libstdc++-296-2.96-138.ppc.rpm<br>compat-libstdc++-33-3.2.3-61.ppc.rpm<br>compat-libstdc++-33-3.2.3-61.ppc64.rpm<br>java-1.4.2-gcj-compat-1.4.2.0-40jpp.115.ppc.rpm |
| SLES 10 | glibc-2.4-31.54.ppc.rpm<br>glibc-64bit-2.4-31.54.ppc.rpm<br>compat-libstdc++-64bit-5.0.7-22.2.ppc.rpm<br>compat-libstdc++-5.0.7-22.2.ppc.rpm<br>compat-2006.1.25-11.2.ppc.rpm<br>libgcc-4.1.2_20070115-0.21.ppc.rpm<br>libgcc-64bit-4.1.2_20070115-0.21.ppc.rpm<br>libstdc++-4.1.2_20070115-0.21.ppc.rpm<br>libstdc++-64bit-4.1.2_20070115-0.21.ppc.rpm |

# Supported software

Veritas Cluster Server supports the previous and next versions of Storage Foundation to facilitate product upgrades, when available.

VCS supports the following volume managers and files systems:

- ext2, ext3, reiserfs, NFS, NFSv4, and bind on LVM2, Veritas Volume Manager (VxVM) 5.0, and raw disks.
- Veritas Volume Manager (VxVM) with Veritas File System (VxFS)
  - VxVM
    VRTSvxvm-common-5.0.33.00-RU3_SLES10
    VRTSvxvm-platform-5.0.33.00-RU3_SLES10
    VRTSvxvm-common-5.0.33.00-RU3_RHEL5
    VRTSvxvm-platform-5.0.33.00-RU3_RHEL5
  - VxFS
    VRTSvxfs-common-5.0.33.00-RU3_SLES10
    VRTSvxfs-platform-5.0.33.00-RU3_SLES10
    VRTSvxfs-common-5.0.33.00-RU3_RHEL5
    VRTSvxfs-platform-5.0.33.00-RU3_RHEL5

Chapter 3

# Preparing to install VCS

This chapter includes the following topics:



## About preparing to install VCS

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

## Preparing to configure the clusters in secure mode

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

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

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

- A system in your enterprise is configured as root broker (RB).
  If a root broker system does not exist, install and configure root broker on a system.
  See "Installing the root broker for the security infrastructure" on page 33.
- An authentication broker (AB) account for each node in the cluster is set up on the root broker system.
  See "Creating authentication broker accounts on root broker system" on page 34.

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

The installvcs program provides the following configuration modes:

| | |
|---|---|
| Automatic mode | The root broker system must allow rsh or ssh passwordless login to use this mode. |
| Semi-automatic mode | This mode requires encrypted files (BLOB files) from the AT administrator to configure a cluster in secure mode.<br>The nodes in the cluster must allow rsh or ssh passwordless login.<br>See "Setting up inter-system communication" on page 44. |
| Manual mode | This mode requires root_hash file and the root broker information from the AT administrator to configure a cluster in secure mode.<br>The nodes in the cluster must allow rsh or ssh passwordless login.<br>See "Setting up inter-system communication" on page 44. |

Figure 3-1 depicts the flow of configuring VCS cluster in secure mode.

**Figure 3-1** Workflow to configure VCS cluster in secure mode

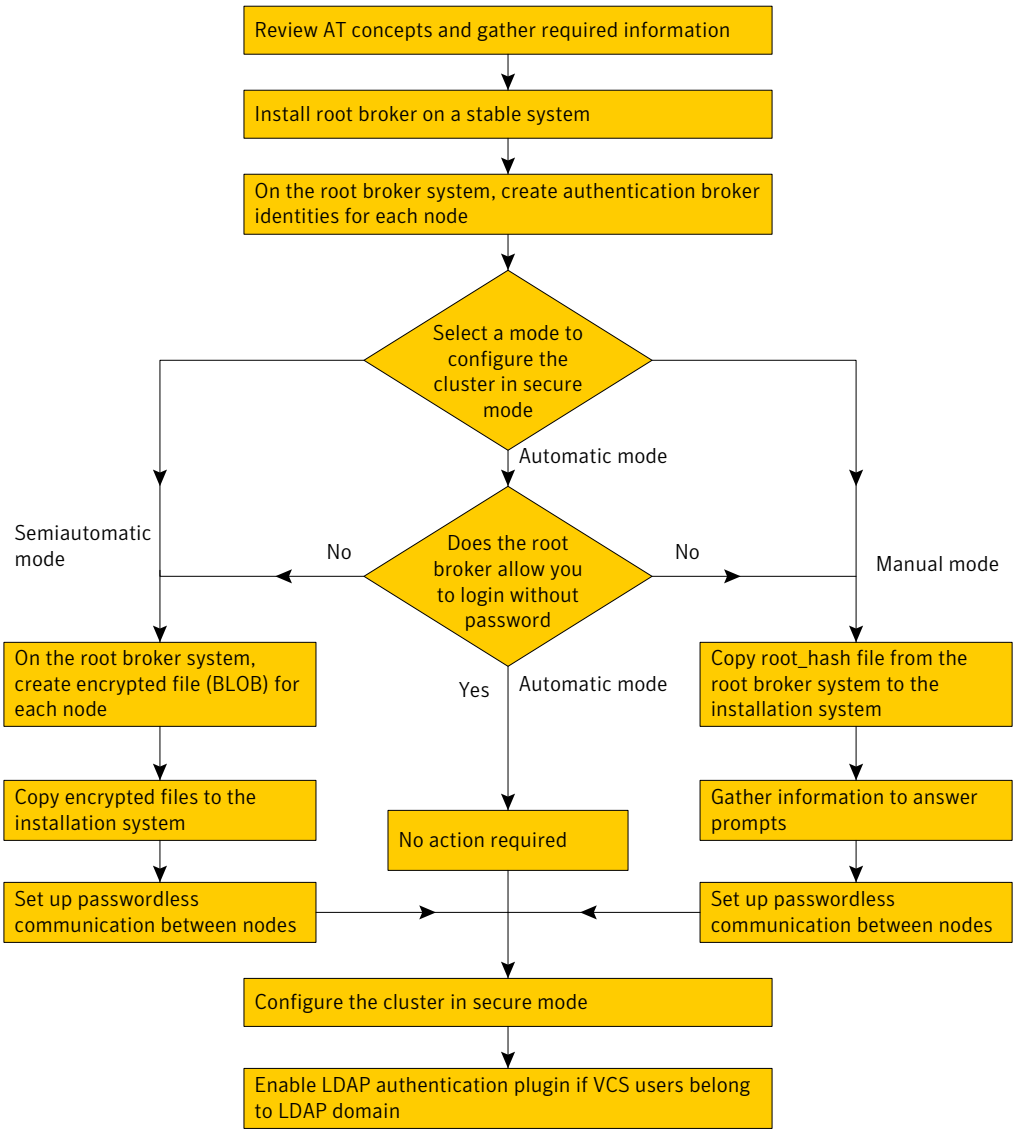



Table 3-1 lists the preparatory tasks in the order which the AT and VCS administrators must perform.

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

| Tasks | Who performs this task |
|---|---|
| Decide one of the following configuration modes to set up a cluster in secure mode:<br>■ Automatic mode<br>■ Semi-automatic mode<br>■ Manual mode | VCS administrator |
| Install the root broker on a stable system in the enterprise.<br>See "Installing the root broker for the security infrastructure" on page 33. | AT administrator |
| On the root broker system, create authentication broker accounts for each node in the cluster.<br>See "Creating authentication broker accounts on root broker system" on page 34.<br>AT administrator requires the following information from the VCS administrator:<br>■ Node names that are designated to serve as authentication brokers<br>■ Password for each authentication broker | AT administrator |
| To use the semi-automatic mode, create the encrypted files (BLOB files) for each node and provide the files to the VCS administrator.<br>See "Creating encrypted files for the security infrastructure" on page 35.<br>AT administrator requires the following additional information from the VCS administrator:<br>■ Administrator password for each authentication broker<br>Typically, the password is the same for all nodes. | AT administrator |
| To use the manual mode, provide the root_hash file (/opt/VRTSat/bin/root_hash) from the root broker system to the VCS administrator. | AT administrator |
| Copy the files that are required to configure a cluster in secure mode to the system from where you plan to install and configure VCS.<br>See "Preparing the installation system for the security infrastructure" on page 37. | VCS administrator |

# Installing the root broker for the security infrastructure

Install the root broker only if you plan to use AT to configure the cluster in secure mode. The root broker administrator must install and configure the root broker before you configure the Authentication Service for VCS. Symantec recommends that you install the root broker on a stable system that is outside the cluster.

You can install the root broker on an AIX, HP-UX, Linux, or Solaris system.

See Symantec Product Authentication Service documentation for more information.

See "About Symantec Product Authentication Service (AT)" on page 19.

**To install the root broker**

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

```
# ./installer
```

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

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

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

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

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

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

   The installer lists the RPMs that the program is about to install on the system. Press Enter to continue.
8. Review the output as the installer installs the root broker on the system.

9 Enter **y** when the installer prompts you to configure the Symantec Product Authentication Service.

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

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

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

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

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

## Creating authentication broker accounts on root broker system

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

**To create authentication broker accounts on root broker system**

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

```
venus> # vssat showalltrustedcreds
```

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

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

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

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

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

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

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

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

  Proceed to step 3.

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

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

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

## Creating encrypted files for the security infrastructure

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

### To create encrypted files

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

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

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

| | |
|---|---|
| identity | The value for the authentication broker identity, which you provided to create authentication broker principal on the root broker system.<br>This is the value for the **--prplname** option of the `addprpl` command.<br>See "Creating authentication broker accounts on root broker system" on page 34. |
| password | The value for the authentication broker password, which you provided to create authentication broker principal on the root broker system.<br>This is the value for the **--password** option of the `addprpl` command.<br>See "Creating authentication broker accounts on root broker system" on page 34. |
| broker_admin_password | The value for the authentication broker password for Administrator account on the node. This password must be at least five characters. |

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

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

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

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

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

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

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

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

For example:

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

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

6 After you complete creating the output files for the encrypted file, you must copy these files to the installer node.

## Preparing the installation system for the security infrastructure

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

**To prepare the installation system for the security infrastructure**

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

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

Manual mode

Do the following:

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

# Performing preinstallation tasks

Table 3-2 lists the tasks you must perform before proceeding to install VCS.

**Table 3-2** Preinstallation tasks

| Task | Reference |
|---|---|
| Obtain license keys. | See "Obtaining VCS license keys" on page 39. |
| Set up the private network. | See "Setting up the private network" on page 40. |
| Configure SuSE network interfaces | See "Configuring SuSE network interfaces" on page 42. |
| Enable communication between systems. | See "Setting up inter-system communication" on page 44. |
| Set up ssh on cluster systems. | See "Setting up ssh on cluster systems" on page 45. |
| Set up shared storage for I/O fencing (optional) | See "Setting up shared storage" on page 46. |
| Set the PATH and the MANPATH variables. | See "Setting the PATH variable" on page 47.<br>See "Setting the MANPATH variable" on page 47. |
| Set the kerne.panic tunable | See "Setting the kernel.panic tunable" on page 48. |

**Table 3-2** Preinstallation tasks *(continued)*

| Task | Reference |
|---|---|
| Review basic instructions to optimize LLT media speeds. | See "Optimizing LLT media speed settings on private NICs" on page 48. |
| Review guidelines to help you set the LLT interconnects. | See "Guidelines for setting the media speed of the LLT interconnects" on page 48. |
| Mount the product disc | See "Mounting the product disc" on page 49. |
| Verify the systems before installation | See "Performing automated pre-installation check" on page 49. |

## Obtaining VCS license keys

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. 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 the features and their descriptions that are encoded in a license key |

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.

## Setting up the private network

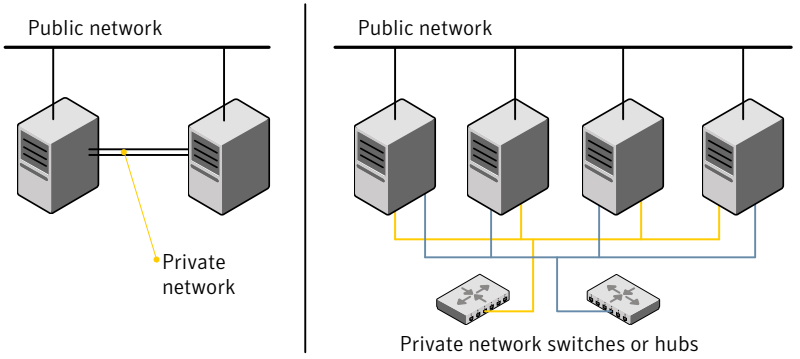
VCS requires you to set up a private network between the systems that form a cluster. You can use either NICs or aggregated interfaces to set up private network.

You can use network switches instead of hubs.

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

Figure 3-2 shows two private networks for use with VCS.

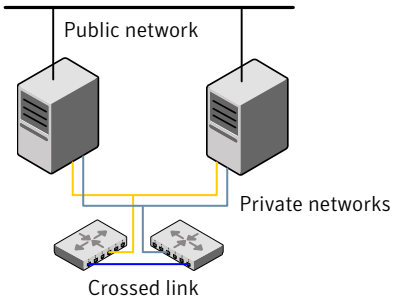
**Figure 3-2** Private network setups: two-node and four-node clusters




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

Figure 3-3 shows a private network configuration with crossed links between the network switches.

**Figure 3-3** Private network setup with crossed links




### To set up the private network

1 Install the required network interface cards (NICs).

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

2 Connect the VCS private NICs on each system.

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

Ensure that you meet the following requirements:

- The power to the switches or hubs must come from separate sources.
- On each system, you must use two independent network cards to provide redundancy.
- The network interface card to set up private interface is not part of any aggregated interface.

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

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

- The systems still run, and

- The systems can access the shared storage.

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

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

The installvcs program configures the private network in the cluster during installation.

See "About installing and configuring VCS" on page 51.

## Configuring SuSE network interfaces

You must perform additional network configuration on SuSE. You need not perform this procedure for the systems that run SLES 10 or later. By default, SLES 10 uses udev to achieve persistent interface names. Refer to the OS documentation for information on configuring persistent interfaces on SLES 10.

In rare cases where RedHat does not automatically configure the network interfaces, RedHat users may also have to perform the network configuration.

Review the following tasks that allow VCS to function properly:

- VCS must be able to find the same network interface names across reboots.
- VCS must have network interfaces up before LLT starts to run.

Symantec suggests the following steps for configuring network interfaces on SUSE.

---

**Note:** You must not reboot the system between configuring the persistent interface names and configuring the interfaces to be up before starting LLT.

---

---

**Note:** The MAC address in the ifcfg-eth-id-mac file can be in uppercase or lowercase. SUSE, and therefore the Veritas product installer, ignores the file with lowercase MAC address if the file with uppercase MAC address is present.

---

**To configure persistent interface names for network devices**

1 Navigate to the hotplug file in the /etc/sysconfig directory:

```
# cd /etc/sysconfig
```

2 Open the hotplug file in an editor.

3 Set HOTPLUG_PCI_QUEUE_NIC_EVENTS to yes:

```
HOTPLUG_PCI_QUEUE_NIC_EVENTS=yes
```

4 Run the command:

```
ifconfig -a
```

5 Make sure that the interface name to MAC address mapping remains same across the reboots.

Symantec recommends adding the PERSISTENT_NAME entries to the configuration files for all the network interfaces (including the network interfaces that are not used).

For each ethernet interface displayed, do the following:

- If a file named /etc/sysconfig/network/ifcfg-eth-id-mac, where mac is the hardware address of that interface, does not exist, then do the following:
  Create the file.
  If a file exists for the same network interface with the name /etc/sysconfig/network/ifcfg-*ethX*, then copy the contents of that file into the newly created file. The variable *ethX* represents the interface name.
- Add the following line at the end of the file /etc/sysconfig/network/ifcfg-eth-id-mac.

  ```
  PERSISTENT_NAME=ethX
  ```

  where *ethX* is the interface name.

For example:

```
# ifconfig -a
eth0    Link encap:Ethernet  HWaddr 00:02:B3:DB:38:FE
        inet addr:10.212.99.30  Bcast:10.212.99.255
        Mask:255.255.254.0
        inet6 addr: fe80::202:b3ff:fedb:38fe/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:453500 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8131 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:1000
RX bytes:35401016 (33.7 Mb)  TX bytes:999899 (976.4 Kb)
Base address:0xdce0 Memory:fcf20000-fcf40000
```

If a file named etc/sysconfig/network/ifcfg-eth-id-00:02:B3:DB:38:FE does not exist, do the following task:

- Create the file.
- If the file /etc/sysconfig/network/ifcfg-eth0 exists, then copy the contents of this file into etc/sysconfig/network/ifcfg-eth-id-00:02:B3:DB:38:FE.

Add the following to the end of the file named etc/sysconfig/network/ifcfg-eth-id-00:02:B3:DB:38:FE,

```
PERSISTENT_NAME=eth0
```

Perform the procedure for all the interfaces that the `ifconfig -a` command displays.

**To configure interfaces to be up before starting LLT**

1. For each network interface that you want LLT to use, find its MAC address by running the `ifconfig` command:

   ```
   # ifconfig eth0
   eth0    Link encap:Ethernet  HWaddr 00:0C:0D:08:C4:32
   ```

   Where `eth0` is the sample network interface name. The output displays 00:0C:0D:08:C4:32 as the interface's MAC address.

2. Navigate to the config file in the /etc/sysconfig/network directory:

   ```
   # cd /etc/sysconfig/network
   ```

3. Open the config file in an editor.
4. Append the string eth-id-macaddress to the MANDATORY_DEVICES list in the config file. Separate each address with a space, for example:

   ```
   MANDATORY_DEVICES="eth-id-00:0C:0D:08:C4:31
   eth-id-00:0C:0D:08:C4:32"
   ```

## Setting up inter-system communication

When you install VCS using the installvcs program, to install and configure the entire cluster at one time, make sure that communication between systems exists. By default the installer uses ssh. You must grant root privileges for the system

where you run installvcs program. This privilege facilitates to issue ssh or rsh commands on all systems in the cluster. If ssh is used to communicate between systems, it must be configured in a way such that it operates without requests for passwords or passphrases. Similarly, rsh must be configured in such a way to not prompt for passwords.

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

---

**Warning:** The rsh and ssh commands to the remote systems, where VCS is to be installed, must not print any extraneous characters.

---

## 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.

The Remote Shell (rsh) is disabled by default to provide better security. Use ssh for remote command execution.

### Configuring ssh

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

---

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

---

#### To configure ssh

1. Log on to the system from which you want to install VCS.
2. Generate a DSA key pair on this system by running the following command:

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

3. Accept the default location of ~/.ssh/id_dsa.

4 When the command prompts, enter a passphrase and confirm it.

5 Change the permissions of the .ssh directory by typing:

```
# chmod 755 ~/.ssh
```

6 The file ~/.ssh/id_dsa.pub contains a line that begins with ssh_dss and ends with the name of the system on which it was created. Copy this line to the /root/.ssh/authorized_keys2 file on all systems where you plan to install VCS.

If the local system is part of the cluster, make sure to edit the authorized_keys2 file on that system.

7 Run the following commands on the system where you are installing:

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

This step is shell-specific and is valid for the duration the shell is alive.

8 When the command prompts, enter your DSA passphrase.

You are ready to install VCS on several systems in one of the following ways:

- Run the installvcs program on any one of the systems
- Run the installvcs program on an independent system outside the cluster

To avoid running the ssh-agent on each shell, run the X-Window system and configure it so that you are not prompted for the passphrase. Refer to the Red Hat documentation for more information.

9 To verify that you can connect to the systems where you plan to install VCS, type:

```
# ssh -x -l root north ls
# ssh -x -l root south ifconfig

# ssh-copy-id -i ~/.ssh/id_dsa.pub  root@north
```

The commands should execute on the remote system without having to enter a passphrase or password.

## Setting up shared storage

For VCS 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 setting up disk-based I/O fencing" on page 89.

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

## Setting the PATH variable

Installation commands as well as other commands reside in the /sbin, /usr/sbin, /opt/VRTS/bin, and /opt/VRTSvcs/bin directories. Add these directories to your PATH environment variable.

**To set the PATH variable**

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

```
$ PATH=/usr/sbin:/sbin:/opt/VRTS/bin:/opt/VRTSvcs/bin:\
$PATH; export PATH
```

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

```
% setenv PATH /usr/sbin:/sbin:/opt/VRTS/bin:\
/opt/VRTSvcs/bin:$PATH
```

## Setting the MANPATH variable

Set the MANPATH variable to view the manual pages.

**To set the MANPATH variable**

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

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

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

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

If you use the `man` command to access manual pages, set LC_ALL to "C" in your shell for correct page display.

```
# export LC_ALL=C
```

See incident 82099 on the Red Hat support web site for more information.

## Setting the kernel.panic tunable

By default, the kernel.panic tunable is set to zero. Therefore the kernel does not reboot automatically if a node panics. To ensure that the node reboots automatically after it panics, this tunable must be set to a non zero value.

**To set the kernel.panic tunable**

1. Set the kernel.panic tunable to a desired value in the /etc/sysctl.conf file.

   For example, kernel.panic = 10, will assign a value 10 seconds to the kernel.panic tunable. This step makes the change persistent across reboots.

2. Run the command:

   ```
   sysctl -w kernel.panic=10
   ```

   In case of a panic, the node will reboot after 10 seconds.

## 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.

## 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 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), set the media speed to the highest value common to both cards, typically 100_Full_Duplex.
- Symantec does not recommend using dissimilar network cards for private links.

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

## Mounting the product disc

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

**To mount the product disc**

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

   The system from which you install VCS need not be part of the cluster. The systems must be in the same subnet.

2. Insert the product disc with the VCS software into a drive that is connected to the system.

   The disc is automatically mounted.

3. If the disc does not automatically mount, then enter:

   ```
   # mount -o ro /dev/cdrom /mnt/cdrom
   ```

4. Navigate to the location of the RPMs.

   Depending on the OS distribution, type the following appropriate command:

   | | |
   |---|---|
   | RHEL 5 | `# cd /mnt/cdrom/rhel5_ppc64/cluster_server` |
   | SLES 10 | `# cd /mnt/cdrom/sles10_ppc64/cluster_server` |

## Performing automated pre-installation 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 pre-installation check is:

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

You can also use the Veritas Installation Assessment Service utility for a detailed assessment of your setup.

See "Veritas Installation Assessment Service" on page 17.

### To check the systems

1 Navigate to the folder that contains the installvcs program.

See "Mounting the product disc" on page 49.

2 Start the pre-installation check:

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

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

Chapter 4

# Installing and configuring VCS

This chapter includes the following topics:



## About installing and configuring VCS

You can install Veritas Cluster Server on clusters of up to 32 systems. You can install VCS using one of the following:

| | |
|---|---|
| Veritas product installer | Use the product installer to install multiple Veritas products. |
| installvcs program | Use this to install just VCS. |

The Veritas product installer and the installvcs program use ssh to install by default. Refer to the *Getting Started Guide* for more information.

# Getting your VCS installation and configuration information ready

The VCS installation and configuration program prompts you for information about certain VCS components.

When you perform the installation, prepare the following information:

- To install VCS RPMs you need:

| | |
|---|---|
| The system names where you plan to install VCS | Example: **galaxy**, **nebula** |
| The required license keys | Depending on the type of installation, keys include:<br>■ A valid site license key<br>■ A valid demo license key<br>■ A valid license key for VCS global clusters<br>See "Obtaining VCS license keys" on page 39. |
| To decide whether to install:<br>■ the required VCS RPMs<br>■ all the VCS RPMs | Install only the required RPMs if you do not want to configure any optional components or features.<br>The default option is to install all RPMs.<br>See "Optional VCS RPMs" on page 54. |

- To configure Veritas Cluster Server you need:

| | |
|---|---|
| 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 "_".<br>Example: **vcs_cluster27** |
| A unique ID number for the cluster | A number in the range of 0-65535. Within the site that contains the cluster, each cluster must have a unique ID.<br>Example: **7** |
| The device names of the NICs that the private networks use among systems | A network interface card that is not part of any aggregated interface, or an aggregated interface.<br>Do not use the network interface card that is used for the public network, which is typically eth0.<br>Example: **eth1, eth2** |

- To configure VCS clusters in secure mode (optional), you need:

| | |
|---|---|
| For automatic mode (default) | ■ The name of the Root Broker system<br>Example: `east`<br>See "About Symantec Product Authentication Service (AT)" on page 19.<br>■ Access to the Root Broker system without use of a password. |
| For semiautomatic mode using encrypted files | The path for the encrypted files that you get from the Root Broker administrator.<br>See "Creating encrypted files for the security infrastructure" on page 35. |
| For semiautomatic mode without using encrypted files | ■ The fully-qualified hostname (FQDN) of the Root Broker . (e.g. east.symantecexample.com)<br>The given example puts a system in the (DNS) domain symantecexample.com with the unqualified hostname east, which is designated as the Root Broker.<br>■ The root broker's security domain (e.g. **`root@east.symantecexample.com`**)<br>■ The root broker's port (e.g. **`2821`**)<br>■ The path to the local root hash (e.g. **`/var/tmp/privatedir/root_hash`**)<br>■ The authentication broker's principal name on each cluster node (e.g. **`galaxy.symantecexample.com`** and **`nebula.symantecexample.com`**) |

- To add VCS users, which is not required if you configure your cluster in secure mode, you need:

| | |
|---|---|
| User names | VCS usernames are restricted to 1024 characters.<br>Example: **`smith`** |
| User passwords | VCS passwords are restricted to 255 characters.<br>Enter the password at the prompt. |
| To decide user privileges | Users have three levels of privileges: A=Administrator, O=Operator, or G=Guest.<br>Example: **`A`** |

- To configure SMTP email notification (optional), you need:

| | |
|---|---|
| The domain-based address of the SMTP server | The SMTP server sends notification emails about the events within the cluster.<br>Example: `smtp.symantecexample.com` |
| The email address of each SMTP recipient to be notified | Example: `john@symantecexample.com` |
| To decide the minimum severity of events for SMTP email notification | Events have four levels of severity: I=Information, W=Warning, E=Error, and S=SevereError.<br>Example: `E` |

- To configure SNMP trap notification (optional), you need:

| | |
|---|---|
| The port number for the SNMP trap daemon | The default port number is 162. |
| The system name for each SNMP console | Example: `saturn` |
| To decide the minimum severity of events for SNMP trap notification | Events have four levels of severity: I=Information, W=Warning, E=Error, and S=SevereError.<br>Example: `E` |

- To configure global clusters (optional), you need:

| | |
|---|---|
| The name of the public NIC | You must specify appropriate values for the NIC.<br>Example: `eth0` |
| The virtual IP address of the NIC | You must specify appropriate values for the virtual IP address.<br>Example: `192.168.1.16` |
| The netmask for the virtual IP address | You must specify appropriate values for the netmask.<br>Example: `255.255.240.0` |

## Optional VCS RPMs

The optional VCS RPMs include the following packages:

- VRTScssim — VCS Simulator
- VRTScscm — Veritas Cluster Server Cluster Manager

- VRTSvcsmn — Manual pages for VCS commands

# 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 RPMs on multiple cluster systems
- Configuring VCS, by creating several detailed configuration files on each system
- Starting VCS processes

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

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

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 29.

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

See "About the uninstallvcs program" on page 153.

## Optional features of the installvcs program

Table 4-1 specifies the optional actions that the installvcs program can perform.

**Table 4-1** installvcs optional features

| Optional action | Reference |
|---|---|
| Check the systems to verify that they meet the requirements to install VCS. | See "Performing automated pre-installation check" on page 49. |
| Install VCS RPMs without configuring VCS. | See "Installing VCS using installonly option" on page 59. |
| Configure or reconfigure VCS when VCS RPMs are already installed. | See "Configuring VCS using configure option" on page 59. |

**Table 4-1** installvcs optional features *(continued)*

| Optional action | Reference |
|---|---|
| Perform secure installations using the values that are stored in a configuration file. | See "Installing VCS with a response file where ssh or rsh are disabled" on page 171. |
| Perform automated installations using the values that are stored in a configuration file. | See "Performing automated VCS installations" on page 164. |

## 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 RPMs 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 "About the uninstallvcs program" on page 153.

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

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

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

See "Installing the Java Console" on page 80.

## About installvcs program command options

In addition to the `-precheck`, `-responsefile`, `-installonly`, and `-configure` options, the installvcs program has other useful options.

The `installvcs` command usage takes the following form:

```
installvcs [ system1 system2... ] [ options ]
```

Table 4-2 lists the installvcs command options.

**Table 4-2** installvcs options

| Option and Syntax | Description |
|---|---|
| -configure | Configure VCS after using -installonly option to install VCS.<br>See "Configuring VCS using configure option" on page 59. |
| -enckeyfile *encryption_key_file* | See the -responsefile and the -encrypt options. |
| -encrypt *password* | Encrypt password using the encryption key that is provided with the -enckeyfile option so that the encrypted password can be stored in response files. |
| -hostfile | Specifies the location of a file that contains the system names for the installer. |
| -installonly | Install product RPMs on systems without configuring VCS.<br>See "Installing VCS using installonly option" on page 59. |
| -installpkgs | Display VCS packages in correct installation order. Output can be used to create scripts for command line installs, or for installations over a network. See the requiredpkgs option. |
| -keyfile *ssh_key_file* | Specifies 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. Useful for replacing demo license. |
| -logpath *log_path* | Specifies that log_path, not /opt/VRTS/install/logs, is the location where installvcs log files, summary file, and response file are saved. |
| -noextrapkgs | Specifies that additional product RPMs such as VxVM and VxFS need not be installed.<br>**Note:** VCS product upgrades in the future can be simplified if you do not install additional product RPMs. |
| -nolic | Install product RPMs on systems without licensing or configuration. License-based features or variants are not installed when using this option. |

**Table 4-2** installvcs options *(continued)*

| Option and Syntax | Description |
|---|---|
| `-nooptionalpkgs` | Specifies that the optional product RPMs such as man pages and documentation need not be installed. |
| `-nostart` | Bypass starting VCS after completing installation and configuration. |
| `-pkgpath` *pkg_path* | Specifies that pkg_path contains all RPMs that the installvcs program is about to install on all systems. The pkg_path is the complete path of a directory, usually NFS mounted. |
| `-precheck` | Verify that systems meet the installation requirements before proceeding with VCS installation.<br><br>Symantec recommends doing a precheck before installing VCS.<br><br>See "Performing automated pre-installation check" on page 49. |
| `-requiredpkgs` | Displays all required VCS packages in correct installation order. Optional packages are not listed. Output can be used to create scripts for command line installs, or for installations over a network. See `installpkgs` option. |
| `-responsefile` *response_file* `[-enckeyfile` *encryption_key_file*`]` | Perform automated VCS installation using the system and the configuration information that is stored in a specified file instead of prompting for information.<br><br>The response_file must be a full path name. If not specified, the response file is automatically generated as installerernumber.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.<br><br>The `-enckeyfile` option and encryption_key_file name are required with the `-responsefile` option when the response file contains encrypted passwords.<br><br>See "Installing VCS with a response file where ssh or rsh are disabled" on page 171.<br><br>See "Performing automated VCS installations" on page 164. |

**Table 4-2** installvcs options *(continued)*

| Option and Syntax | Description |
|---|---|
| `-rsh` | Specifies 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 Symantec Product Authentication Service in a VCS cluster that is running. Install and configure Root Broker for Symantec Product Authentication Service.<br>See "About Symantec Product Authentication Service (AT)" on page 19. |
| `-serial` | Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems. |
| `-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* | Specifies that tmp_path is the working directory for installvcs program. This path is different from the /var/tmp path. This destination is where initial logging is performed and where RPMs are copied on remote systems before installation. |
| `-verbose` | Displays the details when the installer installs the RPMs. By default, the installer displays only a progress bar during the RPMs installation. |

## Installing VCS using installonly option

In certain situations, users may choose to install the VCS RPMs on a system before they are ready for cluster configuration. During such situations, the `installvcs -installonly` option can be used. The installation program licenses and installs VCS RPMs on the systems that you enter without creating any VCS configuration files.

## Configuring VCS using configure option

If you installed VCS and did not choose to configure VCS immediately, use the `installvcs -configure` option. You can configure VCS when you are ready for

cluster configuration. The installvcs program prompts for cluster information, and creates VCS configuration files without performing installation.

See "Configuring the basic cluster" on page 67.

The `-configure` option can be used to reconfigure a VCS cluster. VCS must not be running on systems when this reconfiguration is performed.

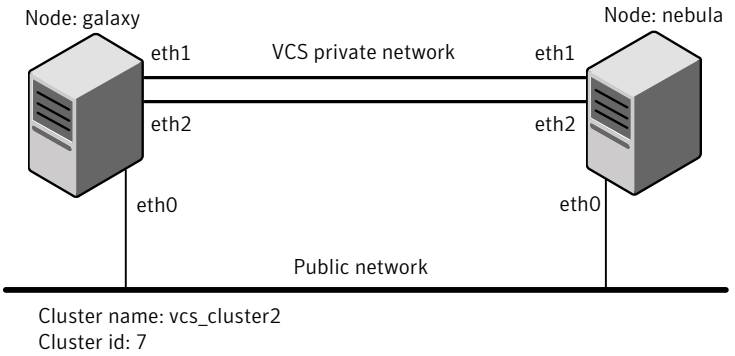
If you manually edited the main.cf file, you need to reformat the main.cf file.

# Installing and configuring VCS 5.0 RU3

The example installation demonstrates how to install VCS on two systems: galaxy and nebula. The example installation chooses to install all VCS RPMs and configures all optional features. For this example, the cluster's name is vcs_cluster2 and the cluster's ID is 7.

Figure 4-1 illustrates the systems on which you would install and run VCS.

**Figure 4-1** An example of a VCS installation on a two-node cluster




## Overview of tasks

Table 4-3 lists the installation and the configuration tasks.

**Table 4-3** Installation and configuration tasks

| Task | Reference |
|---|---|
| License and install VCS | ■ See "Starting the software installation" on page 61.<br>■ See "Specifying systems for installation" on page 62.<br>■ See "Licensing VCS" on page 63.<br>■ See "Choosing VCS RPMs for installation" on page 64.<br>■ See "Choosing to install VCS RPMs or configure VCS" on page 65.<br>■ See "Installing VCS RPMs" on page 75. |
| Configure the cluster and its features | ■ See "Starting the software configuration" on page 66.<br>■ See "Specifying systems for configuration" on page 67.<br>■ See "Configuring the basic cluster" on page 67.<br>■ See "Adding VCS users" on page 71. (optional)<br>■ See "Configuring SMTP email notification" on page 71. (optional)<br>■ See "Configuring SNMP trap notification" on page 73. (optional)<br>■ See "Configuring global clusters" on page 74. (optional) |
| Create configuration files | See "Creating VCS configuration files" on page 76. |
| Start VCS and its components | ■ See "Starting VCS" on page 77.<br>■ See "Completing the installation" on page 77. |
| For clusters that run in secure mode, enable LDAP authentication plug-in if VCS users belong to LDAP domain. | ■ See "About enabling LDAP authentication for clusters that run in secure mode" on page 78. |
| Perform the post-installation tasks | ■ See "About configuring VCS clusters for data integrity" on page 87.<br>■ See "Installing the Java Console" on page 80. |
| Verify the cluster | See "Verifying the cluster after installation" on page 84. |

## Starting the software installation

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

**Note:** The system from where you install VCS must run the same Linux distribution as the target systems.

**To install VCS using the product installer**

1. Confirm that you are logged in as the superuser and 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: I for "Install/Upgrade a Product."
4. From the displayed list of products to install, choose: Veritas Cluster Server.

**To install VCS using the installvcs program**

1. Confirm that you are logged in as the superuser and mounted the product disc.
2. Navigate to the folder that contains the installvcs program.

   ```
   # cd /cluster_server
   ```

3. Start the installvcs program.

   ```
   # ./installvcs [-rsh]
   ```

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

## Specifying systems for installation

The installer prompts for the system names on which you want to install and then performs an initial system check.

### To specify system names for installation

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

```
Enter the system names separated by spaces on which to install
VCS: galaxy nebula
```

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

See "Creating a single-node cluster using the installer program" on page 139.

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

The installer does the following:

- 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 the systems use the proper operating system
- Checks whether VCS is installed

## Licensing VCS

The installer checks whether VCS license keys are currently in place on each system. If license keys are not installed, the installer prompts you for the license keys.

See "Checking licensing information on the system" on page 84.

### To license VCS

1 Review the output as the utility checks system licensing and installs the licensing RPM.

2 Enter the license key for Veritas Cluster Server as the installer prompts for each node.

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

3 Enter keys for additional product features.

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

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

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

4 Review the output as the installer registers the license key on the other nodes. Enter keys for additional product features on the other nodes when the installer prompts you.

```
XXXX-XXXX-XXXX-XXXX-XXX successfully registered on nebula
VCS license registered on nebula

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

## Choosing VCS RPMs for installation

The installer verifies for any previously installed RPMs and then based on your choice installs all the VCS RPMs or only the required RPMs.

**To install VCS RPMs**

1 Review the output as the installer checks the RPMs that are already installed.

2 Choose the VCS RPMs that you want to install.

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

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

1 Installs only the required VCS RPMs.

2 Installs all the VCS RPMs.

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

Note that this option is the default if you already installed the SF HA RPMs.

3 Installs all the VCS and the SF HA RPMs. (default option)

If you already installed the SF HA RPMs, the installer does not list this option.

3 View the list of RPMs that the installer would install on each node.

If the current version of a RPM is on a system, the installer removes it from the RPM installation list for the system.

## Choosing to install VCS RPMs or configure VCS

While you must configure VCS before you can use VCS, you can do one of the following:

- Choose to install and configure VCS now.
  See "Configuring the basic cluster" on page 67.
- Install packages on the systems and leave the cluster configuration steps for later.

**To install VCS packages now and configure VCS later**

1 If you do not want to configure VCS now, enter n at the prompt.

```
Are you ready to configure VCS? [y,n,q] (y) n
```

The utility 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 utility stops and indicates the actions required to proceed with the process.

2 Review the output as the installer uninstalls any previous versions and installs the VCS 5.0 RU3 packages.

3 Configure the cluster later.

See "Configuring VCS using configure option" on page 59.

## Starting the software configuration

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

**To configure VCS using the product installer**

1 Confirm that you are logged in as the superuser and 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: Veritas Cluster Server.

**To configure VCS using the installvcs program**

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

2 Navigate to the folder that contains the installvcs program.

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

3 Start the installvcs program.

```
# ./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 installation**

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

```
Enter the system names separated by spaces on which to configure
VCS: 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 the systems use the proper operating system
- Checks whether VCS is installed
- Exits if VCS 5.0 RU3 is not installed

## Configuring the basic cluster

Enter the cluster information when the installer prompts you.

### To configure the cluster

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

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

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

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

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

   You can choose the network interface cards or the aggregated interfaces that the installer discovers.

   See "Starting VCS" on page 77.

   You must not enter the network interface card that is used for the public network (typically eth0.)

```
Enter the NIC for the first private heartbeat NIC on galaxy:
[b,?] eth1
Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat NIC on galaxy:
[b,?] eth2
Would you like to configure a third private heartbeat link?
[y,n,q,b,?](n)
Do you want to configure an additional low priority heartbeat
link? [y,n,q,b,?] (n)
```

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

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

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

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

6 Verify and confirm the information that the installer summarizes.

## Configuring the cluster in secure mode

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

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

See "Preparing to configure the clusters in secure mode" on page 29.

**To configure the cluster in secure mode**

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

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

- If you want to configure the cluster in secure mode, make sure you meet the prerequisites and enter **y**.
- If you do not want to configure the cluster in secure mode, enter **n**.
  You must add VCS users when the configuration program prompts.
  See "Adding VCS users" on page 71.

2 Select one of the options to enable security.

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

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

| | |
|---|---|
| `Option 1`. Automatic configuration | Enter the name of the Root Broker system when prompted.<br>Requires a remote access to the Root Broker.<br>Review the output as the installer verifies communication with the Root Broker system, checks vxatd process and version, and checks security domain. |
| `Option 2`. Semiautomatic configuration | Enter the path of the encrypted file (BLOB file) for each node when prompted. |
| `Option 3`. Manual configuration | Enter the following Root Broker information as the installer prompts you:<br>`Enter root Broker name:`<br>**`east.symantecexample.com`**<br>`Enter root broker FQDN: [b]`<br>`(symantecexample.com)`<br>**`symantecexample.com`**<br>`Enter root broker domain: [b]`<br>`(root@east.symantecexample.com)`<br>**`root@east.symantecexample.com`**<br>`Enter root broker port: [b] (2821)` **`2821`**<br>`Enter path to the locally accessible`<br>`root hash [b] (/var/tmp/`<br>`installvcs-1Lcljr/root_hash)`<br>**`/root/root_hash`**<br>Enter the following Authentication Broker information as the installer prompts you for each node:<br>`Enter authentication broker principal name on galaxy [b]`<br>`(galaxy.symantecexample.com)`<br>**`galaxy.symantecexample.com`**<br>`Enter authentication broker password on galaxy:`<br>`Enter authentication broker principal name on nebula [b]`<br>`(nebula.symantecexample.com)`<br>**`nebula.symantecexample.com`**<br>`Enter authentication broker password on nebula:` |

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

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

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

## Adding VCS users

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

**To add VCS users**

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

```
Do you want to set the password for the Admin user
(default password='password')? [y,n,q] (n) y

Enter New Password:******

Enter Again:******
```

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

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

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

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

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

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

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

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

## Configuring SMTP email notification

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

**To configure SMTP email notification**

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

2 Specify whether you want to configure the SMTP notification.

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

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

See "Configuring SNMP trap notification" on page 73.

3 Provide information to configure SMTP notification.

Provide the following information:

- Enter the SMTP server's host name.

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

- Enter the email address of each recipient.

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

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

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

4 Add more SMTP recipients, if necessary.

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

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

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

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

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

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

5 Verify and confirm the SMTP notification information.

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

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

## Configuring SNMP trap notification

You can choose to configure 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 User'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] (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 74.

3 Provide information to configure SNMP trap notification.

Provide the following information:

- Enter the SNMP trap daemon port.

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

- Enter the SNMP console system name.

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

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

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

4 Add more SNMP consoles, if necessary.

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

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

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

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

5 Verify and confirm the SNMP notification information.

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

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

## Configuring global clusters

If you had installed a valid HA/DR license, the installer provides you an option to configure this cluster as global cluster. If not, the installer proceeds 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 *Veritas Cluster Server User'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] (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.

   You can also enter an IPv6 address as a virtual IP address.
4. Verify and confirm the configuration of the global cluster.

   ```
   Global Cluster Option configuration verification:

   NIC: eth0
   IP: 192.168.1.16
   Netmask: 255.255.240.0

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

## Installing VCS RPMs

After the installer gathers all the configuration information, the installer installs the RPMs on the cluster systems. If you already installed the RPMs and chose to configure or reconfigure the cluster, the installer proceeds to create the configuration files.

See "Creating VCS configuration files" on page 76.

The utility 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 utility stops and indicates the actions that are required to proceed with the process. Review the output as the installer uninstalls any previous versions and installs the VCS 5.0 RU3 RPMs.

# Creating VCS configuration files

After you install the RPMs and provide the configuration information, the installer continues to create configuration files and copies them to each system.

```
Creating Cluster Server configuration files ..... Done
Copying configuration files to galaxy..... Done
Copying configuration files to nebula..... Done
Cluster Server configured successfully.
```

If you chose to configure the cluster in secure mode, the installer also configures the Symantec Product Authentication Service.

Depending on the mode you chose to set up Authentication Service, the installer does one of the following:

- Creates the security principal
- Executes the encrypted file to create security principal on each node in the cluster

The installer then does the following before the installer starts VCS in secure mode:

- Creates the VxSS service group
- Creates the Authentication Server credentials on each node in the cluster
- Creates the Web credentials for VCS users
- Sets up trust with the root broker

## Verifying the NIC configuration

The installer verifies on all the nodes if all NICs have PERSISTENT_NAME set correctly.

If the persistent interface names are not configured correctly for the network devices, the installer displays the following warnings:

```
Verifying that all NICs have PERSISTENT_NAME set correctly on
galaxy:

For VCS to run correctly, the names of the NIC cards must be
boot persistent.
```

```
CPI WARNING V-9-122-1021
 No PERSISTENT_NAME set for NIC with MAC address
 00:11:43:33:17:28 (present name eth0), though config file  exists!
CPI WARNING V-9-122-1022
 No config file for NIC with MAC address 00:11:43:33:17:29
 (present name eth1) found!
CPI WARNING V-9-122-1022
 No config file for NIC with MAC address 00:04:23:ac:25:1f
 (present name eth3) found!

PERSISTENT_NAME is not set for all the NICs.
You need to set them manually before the next reboot.
```

Set the PERSISTENT_NAME for all the NICs.

**Warning:** If the installer finds the network interface name to be different from the name in the configuration file, then the installer exits.

## Starting VCS

You can now start VCS and its components on each system. If you chose to configure the cluster in secure mode, the installer also starts the Authentication Service processes on each node in the cluster.

**To start VCS**

- Confirm to start VCS and its components on each node.

  Enter **y** if you want to start VCS.

  ```
  Do you want to start Veritas Cluster Server processes now?
  [y,n,q] (y) n
  ```

## Completing the installation

After VCS 5.0 RU3 installation completes successfully, the installer creates summary, log, and response files. The files provide the useful information that can assist you with the installation and can also assist future installations.

Review the location of the installation log files, summary file, and response file that the installer displays.

Table 4-4 specifies the files that are created at the end of the installation.

**Table 4-4** File description

| File | Description |
|---|---|
| summary file | ■ Lists the RPMs that are installed on each system.<br>■ Describes the cluster and its configured resources.<br>■ Provides the information for managing the cluster. |
| log file | Details the entire installation. |
| response file | Contains the configuration information that can be used to perform secure or unattended installations on other systems.<br>See "Example response file" on page 165. |

## About enabling LDAP authentication for clusters that run in secure mode

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

For a cluster that runs in secure mode, you must enable the LDAP authentication plug-in if the VCS users belong to an LDAP domain. To enable LDAP authentication plug-in, you must verify the LDAP environment, add the LDAP domain in AT, and then verify LDAP authentication. The AT component packaged with VCS requires you to manually edit the VRTSatlocal.conf file to enable LDAP authentication.

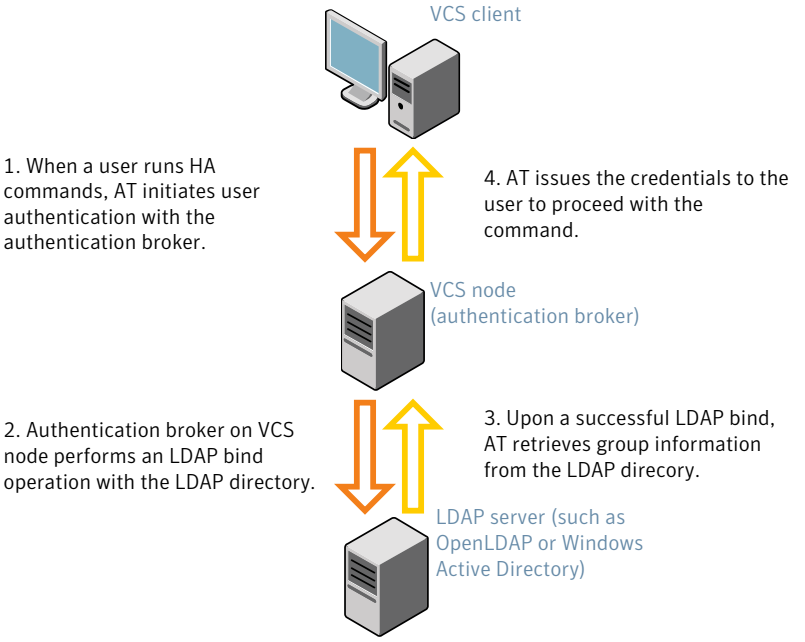
Refer to the *Symantec Product Authentication Service Administrator's Guide* for instructions.

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

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

Figure 4-2 depicts the VCS cluster communication with the LDAP servers when clusters run in secure mode.

**Figure 4-2** Client communication with LDAP servers




See the *Symantec Product Authentication Service Administrator's Guide*.

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

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

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

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

# Installing the Java Console

You can administer VCS using the VCS Java-based graphical user interface, Java Console. After VCS has been installed, install the Java Console on a Windows system or Linux system. Review the software requirements for Java Console.

See "Software requirements for the Java Console" on page 80.

The system from which you run the Java Console can be a system in the cluster or a remote workstation. A remote workstation enables each system in the cluster to be administered remotely.

Review the information about using the Cluster Manager and the Configuration Editor components of the Java Console. For more information, refer to the *Veritas Cluster Server User's Guide*.

## Software requirements for the Java Console

Cluster Manager (Java Console) is supported on:

- RHEL 4 Update 3, RHEL 5, SLES 9 SP3, SLES 10, and SLES 11
- Windows XP, Windows 2003 Server Edition

---

**Note:** Make sure that you are using an operating system version that supports JRE 1.5.

---

## Hardware requirements for the Java Console

The minimum hardware requirements for the Java Console follow:

- Pentium II 300 megahertz
- 256 megabytes of RAM
- 800x600 display resolution
- 8-bit color depth of the monitor
- A graphics card that is capable of 2D images

**Note:** Symantec recommends using Pentium III, 400MHz, 256MB RAM, and 800x600 display resolution.

The version of the Java™ 2 Runtime Environment (JRE) requires 32 megabytes of RAM. This version is supported on the Intel Pentium platforms that run the Linux kernel v 2.2.12 and glibc v2.1.2-11 (or later).

Symantec recommends using the following hardware:

- 48 megabytes of RAM
- 16-bit color mode
- The KDE and the KWM window managers that are used with displays set to local hosts

## Installing the Java Console on Linux for IBM Power

Review the procedure to install the Java console.

### To install Java console on Linux

1. Insert the VCS software disc into a drive on the system.

   The software automatically mounts the disc on /mnt/cdrom.

2. If the disc does not get automatically mounted, then enter:

   ```
   # mount -o ro /dev/cdrom /mnt/cdrom
   ```

3. Navigate to the folder that contains the RPMs.

   ```
   # cd /mnt/cdrom/dist_arch/cluster_server/rpms
   ```

   Where dist is the Linux distribution, rhel5 or sles10 and arch is the architecture, ppc64.

4. Install the RPM using rpm -i command.

   ```
   # rpm -i VRTScscm-5.0.33.00-RU3_GENERIC.noarch.rpm
   ```

## Installing the Java Console on a Windows system

Review the procedure to install the Java console on a Windows system.

### To install the Java Console on a Windows system

1. Insert the software disc with the VCS software into a drive on your Windows system.
2. Using Windows Explorer, select the disc drive.

3 Go to \windows\VCSWindowsInstallers\ClusterManager.

4 Open the language folder of your choice, for example EN.

5 Double-click setup.exe.

6 The Veritas Cluster Manager Install Wizard guides you through the installation process.

# Installing VCS Simulator

You can administer VCS Simulator from the Java Console or from the command line. Review the software requirements for VCS Simulator.

## Software requirements for VCS Simulator

VCS Simulator is supported on:

- RHEL 4 Update 3, RHEL 5, SLES 9 SP3, SLES 10, and SLES 11
- Windows XP, Windows 2003

---

**Note:** Make sure that you are using an operating system version that supports JRE 1.5.

---

## Installing VCS Simulator on UNIX systems

This section describes the procedure to install VCS Simulator on UNIX systems.

### To install VCS Simulator on UNIX systems

1 Insert the VCS installation disc into a drive.

2 Navigate to the following directory and locate VRTScssim.

- Linux—rpms

3 Install the VRTScssim package.

To use Cluster Manager with Simulator, you must also install the VRTScscm package.

## Installing VCS Simulator on Windows systems

This section describes the procedure to install VCS Simulator on Windows systems.

**To install VCS Simulator on Windows systems**

1. Insert the VCS installation disc into a drive.
2. Navigate to the path of the Simulator installer file:

   \your_platform_architecture\cluster_server\windows\VCSWindowsInstallers\Simulator
3. Double-click the installer file.
4. Read the information in the Welcome screen and click **Next**.
5. In the Destination Folders dialog box, click **Next** to accepted the suggested installation path or click **Change** to choose a different location.
6. In the Ready to Install the Program dialog box, click **Back** to make changes to your selections or click **Install** to proceed with the installation.
7. In the Installshield Wizard Completed dialog box, click **Finish**.

## Reviewing the installation

VCS Simulator installs Cluster Manager (Java Console) and Simulator binaries on the system. The Simulator installation creates the following directories:

| Directory | Content |
|---|---|
| attrpool | Information about attributes associated with VCS objects |
| bin | VCS Simulator binaries |
| default_clus | Files for the default cluster configuration |
| sample_clus | A sample cluster configuration, which serves as a template for each new cluster configuration |
| templates | Various templates that are used by the Java Console |
| types | The types.cf files for all supported platforms |
| conf | Contains another directory called types. This directory contains assorted resource type definitions that are useful for the Simulator. The type definition files are present in platform-specific sub directories. |

Additionally, VCS Simulator installs directories for various cluster configurations.

VCS Simulator creates a directory for every new simulated cluster and copies the contents of the sample_clus directory. Simulator also creates a log directory within each cluster directory for logs that are associated with the cluster.

## Verifying the cluster after installation

When you have used installvcs program and chosen to configure and start VCS, VCS and all components are properly configured and can start correctly. You must verify that your cluster operates properly after the installation.

See "About verifying the VCS installation" on page 105.

# 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.

## 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:

```
# cd /opt/VRTS/bin
# ./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                  = 1249
License Type                   = PERMANENT
OEM ID                         = 478

Features :=
Platform                       = Linux for IBM Power
Version                        = 5.0
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 85.

**To update product licenses**

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

```
# cd /opt/VRTS/bin
# ./vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

### Replacing a VCS demo license with a permanent license

When a VCS demonstration 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:

```
# cd /opt/VRTS/bin
# ./vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

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

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

5 Start VCS on each node:

```
# hastart
```

# 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.

Chapter 5

# Configuring VCS clusters for data integrity

This chapter includes the following topics:



## 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.

# 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 88.
- Coordination points—Act as a global lock during membership changes
  See "About coordination points" on page 88.

## About data disks

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

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

## About coordination points

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

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

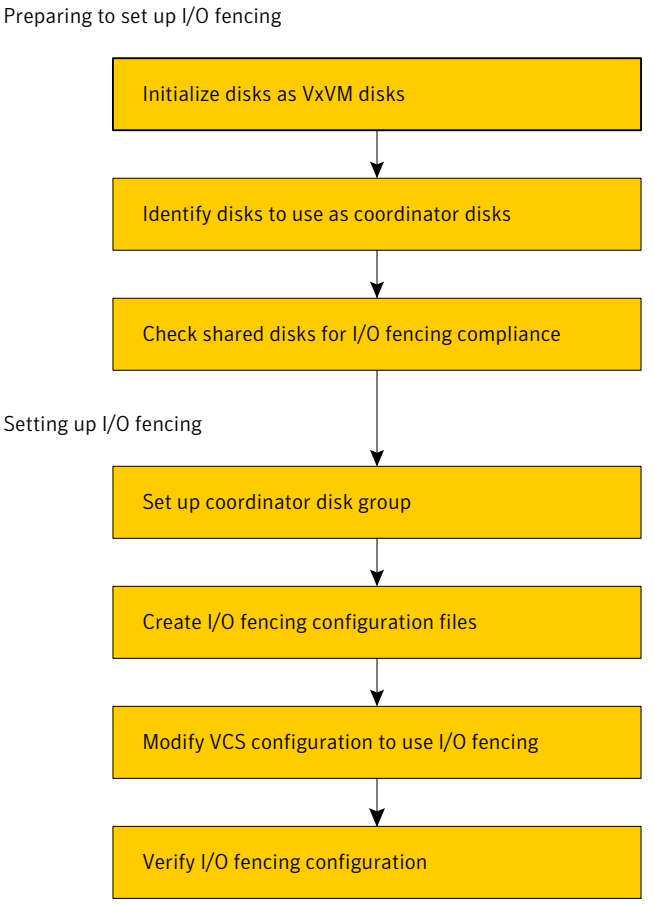
You can configure coordinator disks to use Veritas Volume Manager Dynamic Multipathing (DMP) feature. Dynamic Multipathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. So, you can configure I/O fencing to use either DMP 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 raw by default. Symantec recommends using the DMP disk policy.

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

# About setting up disk-based I/O fencing

Figure 5-1 illustrates the tasks involved to configure I/O fencing.

**Figure 5-1** Workflow to configure disk-based I/O fencing




See "Preparing to configure disk-based I/O fencing" on page 92.

See "Setting up disk-based I/O fencing manually" on page 99.

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

Review the following requirements for coordinator disks:

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

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

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

The I/O fencing configuration files include:

| | |
|---|---|
| /etc/vxfendg | You must create this file to include the coordinator disk group information. |
| /etc/vxfenmode | You must set the I/O fencing mode to SCSI-3.<br>You can configure the vxfen module to use either DMP devices or the underlying raw character devices. Note that you must use the same SCSI-3 disk policy on all the nodes. The SCSI-3 disk policy can either be raw or dmp. The policy is raw by default. If you use iSCSI devices, you must set the disk policy as dmp. |

/etc/vxfentab

When you run the vxfen startup file to start I/O fencing, the script creates this /etc/vxfentab file on each node with a list of all paths to each coordinator disk. The startup script uses the contents of the /etc/vxfendg and /etc/vxfenmode files.

Thus any time a system is rebooted, the fencing driver reinitializes the vxfentab file with the current list of all paths to the coordinator disks.

**Note:** The /etc/vxfentab file is a generated file; do not modify this file.

An example of the /etc/vxfentab file on one node resembles as follows:

- Raw disk:

```
/dev/sdx
/dev/sdy
/dev/sdz
```

- DMP disk:

```
/dev/vx/rdmp/sdx
/dev/vx/rdmp/sdy
/dev/vx/rdmp/sdz
```

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

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

# Preparing to configure disk-based I/O fencing

Make sure you performed the following tasks before configuring I/O fencing for VCS:

- Install the correct operating system.
- Install the VRTSvxfen RPM when you installed VCS.
- Install a version of Veritas Volume Manager (VxVM) that supports SCSI-3 persistent reservations (SCSI-3 PR).

Refer to the installation guide that comes with the Storage Foundation product that you use.

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

| | |
|---|---|
| Initialize disks as VxVM disks | See "Initializing disks as VxVM disks" on page 93. |
| Identify disks to use as coordinator disks | See "Identifying disks to use as coordinator disks" on page 95. |
| Check shared disks for I/O fencing<br>The tasks involved in checking the shared disks for I/O fencing are as follows:<br>■ Verify that the nodes have access to the same disk<br>■ Test the disks using the vxfentsthdw utility | See "Checking shared disks for I/O fencing" on page 95. |

## Initializing disks as VxVM disks

Perform the following procedure to initialize disks as VxVM disks.

**To initialize disks as VxVM disks**

1 Make the new disks recognizable. On each node, enter:

```
# fdisk -l
```

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

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

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

The following output is a sample:

```
# vxddladm listsupport all

LIBNAME             VID                 PID
==============================================================================

libvx3par.so        3PARdata            VV
libvxCLARiiON.so    DGC                 All
libvxcscovrts.so    CSCOVRTS            MDS9
libvxemc.so         EMC                 SYMMETRIX
libvxhds.so         HITACHI             All
libvxhds9980.so     HITACHI             All
libvxhdsalua.so     HITACHI             DF600, DF600-V, DF600F, DF600F-V
libvxhdsusp.so      HITACHI             All
libvxhitachi.so     HITACHI             DF350, DF400, DF400F, DF500, DF500F
libvxhpalua.so      HP, COMPAQ          HSV101, HSV111 (C)COMPAQ, HSV111, H
                                        HSV210
libvxhpmsa.so       HP                  MSA VOLUME
libvxibmds4k.so     IBM                 1722, 1724, 3552, 3542, 1742-900, 1
                                        3526, 1815, 1814
libvxibmds6k.so     IBM                 1750
libvxibmds8k.so     IBM                 2107
libvxpp.so          EMC, DGC            All
libvxpurple.so      SUN                 T300
libvxshark.so       IBM                 2105
libvxveritas.so     VERITAS             All
libvxxiv.so         XIV, IBM            NEXTRA, 2810XIV
libvxxp1281024.so   HP                  All
libvxxp12k.so       HP                  All
libvxxp256.so       HP                  All
```

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

```
# vxdisk scandisks
```

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

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

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

  ```
  vxdisksetup -i device_name
  ```

  The example specifies the CDS format:

  ```
  # vxdisksetup -i sdr
  ```

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

## Identifying disks to use as coordinator disks

After you add and initialize disks, identify disks to use as coordinator disks.

**To identify the coordinator disks**

1 List the disks on each node.

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

```
# vxdisk list
```

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

## Checking shared disks for I/O fencing

Make sure that the shared storage you set up while preparing to configure 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 *Veritas Cluster Server User's Guide*.

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

- Verifying that nodes have access to the same disk
  See "Verifying that the nodes have access to the same disk" on page 96.
- Testing the shared disks for SCSI-3
  See "Testing the disks using vxfentsthdw utility" on page 97.

## 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.

   ```
   /sbin/vxfenadm -i diskpath
   ```

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

   For example, an EMC disk is accessible by the /dev/sdx path on node A and the /dev/sdy path on node B.

   From node A, enter:

   ```
   # /sbin/vxfenadm -i /dev/sdx

   SCSI ID=>Host: 2 Channel: 0 Id: 0 Lun: E

   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/sdy path.

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

```
# /sbin/vxfenadm -i /dev/sdz

SCSI ID=>Host: 2 Channel: 0 Id: 0 Lun: E

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

## Testing the disks using vxfentsthdw utility

This procedure uses the /dev/sdx 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/sdx 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 User'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 44.

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

See "Removing permissions for communication" on page 103.

2 From one node, start the utility.

Do one of the following:

- If you use `ssh` for communication:

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

- If you use `rsh` for communication:

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

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

---

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

---

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

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

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

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

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

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

6 If a disk is ready for I/O fencing on each node, the utility reports success:

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

ALL tests on the disk /dev/sdx 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 disk-based I/O fencing manually

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

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

**Table 5-1** Tasks to set up I/O fencing manually

| Action | Description |
|---|---|
| Setting up coordinator disk groups | See "Setting up coordinator disk groups" on page 99. |
| Creating I/O fencing configuration files | See "Creating I/O fencing configuration files" on page 100. |
| Modifying VCS configuration to use I/O fencing | See "Modifying VCS configuration to use I/O fencing" on page 101. |
| Verifying I/O fencing configuration | See "Verifying I/O fencing configuration" on page 102. |

## Setting up coordinator disk groups

From one node, create a disk group named vxfencoorddg. This group must contain three disks or LUNs. If you use VxVM 5.0 or later, you must also set the coordinator attribute for the coordinator disk group. VxVM uses this attribute to prevent the reassignment of coordinator disks to other disk groups.

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

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

The following example procedure assumes that the disks have the device names sdx, sdy, and sdz.

**To create the vxfencoorddg disk group**

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

```
# vxdg init vxfencoorddg sdx sdy sdz
```

2 If you use VxVM 5.0 or later, set the coordinator attribute value as "on" for the coordinator disk group.

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

3 Deport the coordinator disk group:

```
# vxdg deport vxfencoorddg
```

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

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

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

```
# vxdg deport vxfencoorddg
```

## Creating I/O fencing configuration files

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

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

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

1 On each nodes, type:

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

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

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

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

- For DMP configuration:

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

- For raw device configuration:

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

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

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

## Modifying VCS configuration to use I/O fencing

After you add coordinator disks and configure I/O fencing, add the UseFence = SCSI3 cluster attribute to the VCS configuration file /etc/VRTSvcs/conf/config/main.cf. If you reset this attribute to UseFence = None, VCS does not make use of I/O fencing abilities while failing over service groups. However, I/O fencing needs to be disabled separately.

**To modify VCS configuration to enable I/O fencing**

1 Save the existing configuration:

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

2 Stop VCS on all nodes:

```
# hastop -all
```

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

```
# /etc/init.d/vxfen stop
```

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

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

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

```
cluster clus1(
UserNames = { admin = "cDRpdxPmHpzS." }
Administrators = { admin }
HacliUserLevel = COMMANDROOT
CounterInterval = 5
UseFence = SCSI3
)
```

6 Save and close the file.

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

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

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

For example, on each remaining node, enter:

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

9 Start the I/O fencing driver and VCS. Perform the following steps on each node:

- Start the I/O fencing driver.
  The vxfen startup script also invokes the `vxfenconfig` command, which configures the vxfen driver to start and use the coordinator disks that are listed in /etc/vxfentab.

  ```
  # /etc/init.d/vxfen start
  ```

- Start VCS.

  ```
  # /opt/VRTS/bin/hastart
  ```

## Verifying I/O fencing configuration

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

**To verify I/O fencing configuration**

- On one of the nodes, type:

```
# vxfenadm -d

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

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

   * 0 (galaxy)
   1 (nebula)

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

## Removing permissions for communication

Make sure you completed the installation of 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.

Chapter 6

# 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 LLT and GAB configuration files

Low Latency Transport (LLT) and Group Membership and Atomic Broadcast (GAB) are VCS communication services. LLT requires /etc/llthosts and /etc/llttab files. GAB requires /etc/gabtab file.

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

- The /etc/llthosts file

The file `llthosts` is a database that contains one entry per system. This file links the LLT system ID (in the first column) with the LLT host name. This file is identical on each node in the cluster.
For example, the file /etc/llthosts contains the entries that resemble:

```
0       galaxy
1       nebula
```

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

```
set-node galaxy
set-cluster 2
link eth1 eth1 - ether - -
link eth2 eth2 - ether - -
```

  If you use MAC address for the network interface, the file /etc/llttab contains the entries that resemble:

```
set-node galaxy
set-cluster 2
link eth1 eth-00:04:23:AC:12:C4 - ether - -
link eth2 eth-00:04:23:AC:12:C5 - ether - -
```

  The first line identifies the system. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines begin with the `link` command. These lines identify the two network cards that the LLT protocol uses.
  Refer to the `lltttab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `llttab` file.

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

**Note:** The use of the `-c -x` option for `/sbin/gabconfig` is not recommended.

# About the VCS configuration file main.cf

The VCS configuration file /etc/VRTSvcs/conf/config/main.cf is created during the installation process.

See "Sample main.cf file for VCS clusters" on page 108.

See "Sample main.cf file for global clusters" on page 110.

The main.cf file contains the minimum information that defines the cluster and its nodes. In addition, the file types.cf, which is listed in the include statement, defines the VCS bundled types for VCS resources. The file types.cf is also located in the directory /etc/VRTSvcs/conf/config after installation.

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 that you added is present.
- If you configured the cluster in secure mode, the main.cf includes the VxSS service group and "SecureClus = 1" cluster attribute.
- The installvcs program creates the ClusterService service group. The group includes the IP, NIC, and VRTSWebApp resources.

  The service group also has the following characteristics:

  - 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 User's Guide* for information about managing VCS global clusters.

Refer to the *Veritas Cluster Server User's Guide* to review the configuration concepts, and descriptions of main.cf and types.cf files for Linux for IBM Power systems.

## Sample main.cf file for VCS clusters

The following sample main.cf file is for a secure cluster that is managed locally by the Cluster Management Console.

```
include "types.cf"

cluster vcs_cluster2 (
    UserNames = { admin = cDRpdxPmHpzS, smith = dKLhKJkHLh }
    ClusterAddress = "192.168.1.16"
    Administrators = { admin, smith }
    CounterInterval = 5
    SecureClus = 1
)

    system galaxy (
   )

    system nebula (
   )

    group ClusterService (
       SystemList = { galaxy = 0, nebula = 1 )
       UserStrGlobal = "LocalCluster@https://10.182.2.76:8443;"
       AutoStartList = { galaxy, nebula )
       OnlineRetryLimit = 3
       OnlineRetryInterval = 120
       )

    IP webip (
       Device = eth0
       Address = "192.168.1.16"
       NetMask = "255.255.240.0"
       )

NIC csgnic (
       Device = eth0
       )
```

```
NIC csgnic (
        Device = eth0
        NetworkHosts = { "192.168.1.17", "192.168.1.18" }
        )

NotifierMngr ntfr (
    SnmpConsoles = { "saturn" = Error, "jupiter" = SevereError }
    SmtpServer = "smtp.example.com"
    SmtpRecipients =  { "ozzie@example.com" = Warning,
                    "harriet@example.com" = Error }
    )


VRTSWebApp VCSweb (
    Critical = 0
    InstallDir = "/opt/VRTSweb/VERITAS"
    TimeForOnline = 5
    RestartLimit = 3
    )

    VCSweb requires webip
    ntfr requires csgnic
    webip requires csgnic

// resource dependency tree
    //
    // group ClusterService
    // {
    //       VRTSWebApp VCSweb
    //       {
    //          IP webip
    //          {
    //             NIC csgnic
    //          }
    //       }
    //       NotifierMngr ntfr
    //       {
    //          NIC csgnic
    //       }
    // }



group VxSS (
```

```
    SystemList = { galaxy = 0, nebula = 1 }
    Parallel = 1
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Phantom phantom_vxss (
       )

    ProcessOnOnly vxatd (
       IgnoreArgs = 1
       PathName = "/opt/VRTSat/bin/vxatd"
       )



// resource dependency tree
    //
    // group VxSS
    // {
    // Phantom phantom_vxss
    // ProcessOnOnly vxatd
    // }
```

## Sample main.cf file for global clusters

If you installed VCS with the Global Cluster option, note that the ClusterService group also contains the Application resource, wac. The wac resource is required to control the cluster in a global cluster environment.

```
    UserStrGlobal = "LocalCluster@https://10.182.2.78:8443;"

    AutoStartList = { galaxy, nebula }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Application wac (
       StartProgram = "/opt/VRTSvcs/bin/wacstart"
       StopProgram = "/opt/VRTSvcs/bin/wacstop"
       MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
       RestartLimit = 3
       )
```

```
    .
    .
```

In the following main.cf file example, bold text highlights global cluster specific entries.

```
include "types.cf"

cluster vcs03 (
    ClusterAddress = "10.182.13.50"
    SecureClus = 1
    )

system sysA (
    )

system sysB (
    )

system sysC (
    )

group ClusterService (
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

Application wac (
    StartProgram = "/opt/VRTSvcs/bin/wacstart"
    StopProgram = "/opt/VRTSvcs/bin/wacstop"
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
    RestartLimit = 3
    )

IP gcoip (
    Device = eth0
    Address = "10.182.13.50"
    NetMask = "255.255.240.0"
    )

NIC csgnic (
```

```
    Device = eth0
    )

NotifierMngr ntfr (
    SnmpConsoles = { vcslab4079 = SevereError }
    SmtpServer = "smtp.veritas.com"
    SmtpRecipients = { "johndoe@veritas.com" = SevereError }
    )

gcoip requires csgnic
ntfr requires csgnic
wac requires gcoip

// resource dependency tree
//
//     group ClusterService
//     {
//     NotifierMngr ntfr
//         {
//         NIC csgnic
//         }
//     Application wac
//         {
//         IP gcoip
//             {
//             NIC csgnic
//             }
//         }
//     }

group VxSS (
    SystemList = { sysA = 0, sysB = 1, sysC = 2 }
    Parallel = 1
    AutoStartList = { sysA, sysB, sysC }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

Phantom phantom_vxss (
    )

ProcessOnOnly vxatd (
    IgnoreArgs = 1
```

```
    PathName = "/opt/VRTSat/bin/vxatd"
    )

// resource dependency tree
//
//     group VxSS
//     {
//     Phantom phantom_vxss
//     ProcessOnOnly vxatd
//     }
```

# 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/lltab
- GAB
  /etc/gabtab
- VCS
  /etc/VRTSvcs/conf/config/main.cf

2 Verify the content of the configuration files.

See "About the LLT and GAB configuration files" on page 105.

See "About the VCS configuration file main.cf" on page 107.

# 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 47.

3 Verify LLT operation.

See "Verifying LLT" on page 114.

4 Verify GAB operation.

See "Verifying GAB" on page 116.

5 Verify the cluster operation.

See "Verifying the cluster" on page 117.

## Verifying LLT

Use the `lltstat` command to verify that links are active for LLT. If LLT is configured correctly, this command shows all the nodes in the cluster. The command also returns information about the links for LLT for the node on which you typed the command.

Refer to the `lltstat(1M)` manual page for more information.

**To verify LLT**

1 Log in as superuser on the node galaxy.

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

```
lltstat -n
```

The output on galaxy resembles:

```
LLT node information:
    Node             State            Links
    *0 galaxy          OPEN            2
     1 nebula          OPEN            2
```

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

3 Log in as superuser on the node nebula.

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

```
lltstat -n
```

The output on nebula resembles:

```
LLT node information:
    Node             State            Links
     0 galaxy          OPEN            2
    *1 nebula          OPEN            2
```

5 To view additional information about LLT, run the `lltstat -nvv` command on each node.

For example, run the following command on the node galaxy in a two-node cluster:

```
lltstat -nvv | more
```

The output on galaxy resembles:

```
Node          State      Link    Status      Address
*0 galaxy      OPEN
                         eth1 UP     08:00:20:93:0E:34
                         eth2 UP     08:00:20:93:0E:34
1 nebula       OPEN
                         eth1 UP     08:00:20:8F:D1:F2
                         eth2 DOWN
2             CONNWAIT
                         eth1 DOWN
                         eth2 DOWN
3             CONNWAIT
                         eth1 DOWN
                         eth2 DOWN
.
.
.

31            CONNWAIT
                         eth1 DOWN
                         eth2 DOWN
```

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

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

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

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

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

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

```
lltstat -p
```

The output resembles:

```
LLT port information:
  Port  Usage       Cookie
  0     gab          0x0
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 28 29 30 31
        connects:    0 1
  7     gab          0x7
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 28 29 30 31
        connects:    0 1
  31    gab          0x1F
        opens:       0 2 3 4 5 6 7 8 9 10 11 ... 28 29 30 31
        connects:    0 1
```

## Verifying GAB

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

The 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 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 User'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:

```
GAB Port Memberships
===================================
Port a gen a36e0003 membership 01
Port h gen fd570002 membership 01
```

- 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 User's Guide* for a description of system states and the transitions between them.

**To verify the cluster**

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

```
hastatus -summary
```

The output resembles:

```
-- SYSTEM STATE
-- System               State                Frozen

A  galaxy                RUNNING               0
A  nebula                RUNNING               0

-- GROUP STATE
-- Group           System        Probed  AutoDisabled   State


B  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 User's Guide* for information about the system attributes for VCS.

**To verify the cluster nodes**

- On one of the nodes, type the `hasys -display` command:

```
hasys -display
```

The example shows the output when the command is run on the node galaxy. The list continues with similar information for nebula (not shown) and any other nodes in the cluster.

```
#System    Attribute             Value

galaxy     AgentsStopped         0

galaxy     AvailableCapacity     100

galaxy     CPUUsage              0

galaxy     CPUUsageMonitoring    Enabled 0 ActionThreshold 0
                                 ActionTimeLimit 0 Action NONE
                                 NotifyThreshold 0 NotifyTimeLimit 0

galaxy     Capacity              100

galaxy     ConfigBlockCount      142

galaxy     ConfigCheckSum        4085

galaxy     ConfigDiskState       CURRENT

galaxy     ConfigFile            /etc/VRTSvcs/conf/config

galaxy     ConfigInfoCnt         0

galaxy     ConfigModDate         Fri May 22 17:22:48 2009

galaxy     ConnectorState        Down

galaxy     CurrentLimits

galaxy     DiskHbStatus

galaxy     DynamicLoad           0

galaxy     EngineRestarted       0

galaxy     EngineVersion         5.1.00.0

galaxy     Frozen                0

galaxy     GUIIPAddr

galaxy     LLTNodeId             0

galaxy     LicenseType           DEMO
```

```
#System    Attribute             Value

galaxy     Limits

galaxy     LinkHbStatus          eth1 UP eth2 UP

galaxy     LoadTimeCounter       0

galaxy     LoadTimeThreshold     600

galaxy     LoadWarningLevel      80

galaxy     NoAutoDisable         0

galaxy     NodeId                0

galaxy     OnGrpCnt              1

galaxy     ShutdownTimeout       120

galaxy     SourceFile            ./main.cf

galaxy     SysInfo               Linux:galaxy,#1 SMP Mon Dec 12
                                 18:32:25 UTC
                                 2005,2.6.5-7.244-pseries64,ppc64

galaxy     SysName               galaxy

galaxy     SysState              RUNNING

galaxy     SystemLocation

galaxy     SystemOwner

galaxy     TFrozen               0

galaxy     TRSE                  0

galaxy     UpDownState           Up

galaxy     UserInt               0

galaxy     UserStr

galaxy     VCSFeatures           DR

galaxy     VCSMode               VCS
```

Chapter 7

# 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 32 nodes.

## Adding a node to a cluster

The system you add to the cluster must meet the hardware and software requirements.

Table 7-1 specifies the tasks that are involved in adding a cluster. The example demonstrates how to add a node saturn to already existing nodes, galaxy and nebula.

**Table 7-1** Tasks that are involved in adding a node to a cluster

| Task | Reference |
| --- | --- |
| Set up the hardware. | See "Setting up the hardware" on page 122. |

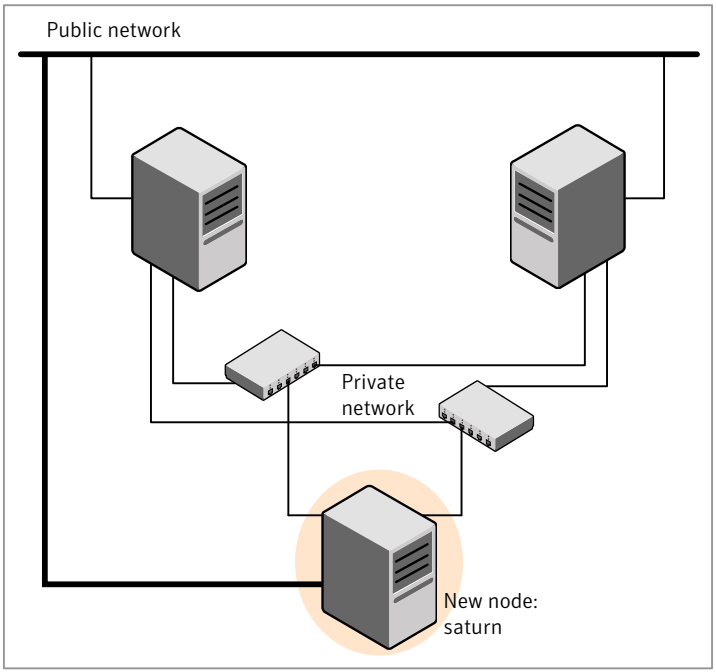
**Table 7-1** Tasks that are involved in adding a node to a cluster *(continued)*

| Task | Reference |
|---|---|
| Install the software manually. | See "Preparing for a manual installation when adding a node" on page 123.<br>See "Installing VCS RPMs for a manual installation" on page 124. |
| Add a license key. | See "Adding a license key" on page 125. |
| For a cluster that is running in secure mode, verify the existing security setup on the node. | See "Setting up the node to run in secure mode" on page 126. |
| Configure LLT and GAB. | See "Configuring LLT and GAB" on page 128. |
| Add the node to the existing cluster. | See "Adding the node to the existing cluster" on page 130. |
| Start VCS and verify the cluster. | See "Starting VCS and verifying the cluster" on page 131. |

## Setting up the hardware

Figure 7-1 shows that before you configure a new system on an existing cluster, you must physically add the system to the cluster.

**Figure 7-1** Adding a node to a two-node cluster using two switches




**To set up the hardware**

1 Connect the VCS private Ethernet controllers.

Perform the following tasks as necessary:

- When you add nodes to a two-node cluster, use independent switches or hubs for the private network connections. You can only use crossover cables for a two-node cluster, so you might have to swap out the cable for a switch or hub.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 7-1 illustrates a new node being added to an existing two-node cluster using two independent hubs.

2 Connect the system to the shared storage, if required.

## Preparing for a manual installation when adding a node

Before you install, log in as the superuser. You then mount the disc and put the files in a temporary folder for installation.

See "Mounting the product disc" on page 49.

**To prepare for installation**

- Depending on the OS distribution, replace the dist in the command with rhel5 or sles10. Replace the arch in the command with ppc64.

```
# cd  /mnt/cdrom/dist_arch/cluster_server/rpms
```

## Installing VCS RPMs for a manual installation

VCS has both required and optional RPMs. Install the required RPMs first. All RPMs are installed in the /opt directory.

When you select the optional RPMs, review the following information:

- Symantec recommends that you install the RPMs for VCS manual pages (VRTSvcsmn).
- The I/O fencing RPM (VRTSvxfen) can be used only with the shared disks that support SCSI-3 Persistent Reservations (PR). See the *Veritas Cluster Server User's Guide* for a conceptual description of I/O fencing. You need to test shared storage for SCSI-3 PR and to implement I/O fencing.
  See "About setting up disk-based I/O fencing" on page 89.

Use this procedure if you install VCS for the first time. Make sure the system does not have any of the VCS RPMs already installed. If VCS is already installed, either remove the RPMs before you perform this procedure or upgrade VCS on the new node.

Perform the steps to install VCS RPMs on each node in the cluster.

**To install VCS RPMs on a node**

- Install the required VCS RPMs in the order shown. Do not install any RPMs already installed on the system. Pay special attention to operating system distribution and architecture.
  - RHEL5/ppc64, required RPMS

```
# rpm -i VRTSvlic-3.02.33.4-0.ppc64.rpm
# rpm -i VRTSperl-5.10.0.1-RHEL5.2.ppc64.rpm
# rpm -i VRTSspt-5.5.00.0-GA.noarch.rpm
# rpm -i VRTSllt-5.0.33.00-RU3_RHEL5.ppc64.rpm
# rpm -i VRTSgab-5.0.33.00-RU3_RHEL5.ppc64.rpm
# rpm -i VRTSvxfen-5.0.33.00-RU3_RHEL5.ppc64.rpm
# rpm -i VRTSvcs-5.0.33.00-RU3_RHEL5.ppc64.rpm
# rpm -i VRTSvcsag-5.0.33.00-RU3_RHEL5.ppc64.rpm
# rpm -i VRTSvcsdr-5.0.33.00-RU3_RHEL5.ppc64.rpm
```

```
# rpm -i VRTScutil-5.0.33.00-RU3_GENERIC.noarch.rpm
# rpm -i VRTSatClient-4.3.28.0-0.ppc.rpm
# rpm -i VRTSatServer-4.3.28.0-0.ppc.rpm
```

- SLES10/ppc64, required RPMS

```
# rpm -i VRTSvlic-3.02.33.4-0.ppc64.rpm
# rpm -i VRTSperl-5.10.0.1-SLES10.ppc64.rpm
# rpm -i VRTSspt-5.5.00.0-GA.noarch.rpm
# rpm -i VRTSllt-5.0.33.00-RU3_SLES10.ppc64.rpm
# rpm -i VRTSgab-5.0.33.00-RU3_SLES10.ppc64.rpm
# rpm -i VRTSvxfen-5.0.33.00-RU3_SLES10.ppc64.rpm
# rpm -i VRTSvcs-5.0.33.00-RU3_SLES10.ppc64.rpm
# rpm -i VRTSvcsag-5.0.33.00-RU3_SLES10.ppc64.rpm
# rpm -i VRTSvcsdr-5.0.33.00-RU3_SLES10.ppc64.rpm
# rpm -i VRTScutil-5.0.33.00-RU3_GENERIC.noarch.rpm
# rpm -i VRTSatClient-4.3.28.0-0.ppc.rpm
# rpm -i VRTSatServer-4.3.28.0-0.ppc.rpm
```

## Adding a license key

After you have installed all RPMs on each cluster node, use the `vxlicinst` command to add the VCS license key on each system:

```
# cd /opt/VRTS/bin
# ./vxlicinst -k XXXX-XXXX-XXXX-XXXX-XXXX-XXX
```

### Checking licensing information on the system

Use the `vxlicrep` utility to display information about all Veritas licenses on a system. For example, enter:

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

From the output, you can determine the license key, the type of license, the product for which it applies, and its expiration date, if any. Demo keys have expiration dates, while permanent keys and site keys do not.

## Setting up the node to run in secure mode

You must follow this procedure only if you are adding a node to a cluster that is running in secure mode. If you are adding a node to a cluster that is not running in a secure mode, proceed with configuring LLT and GAB.

See "Configuring LLT and GAB" on page 128.

Table 7-2 uses the following information for the following command examples.

**Table 7-2** The command examples definitions

| Name | Fully-qualified host name (FQHN) | Function |
|---|---|---|
| saturn | saturn.nodes.example.com | The new node that you are adding to the cluster. |
| RB1 | RB1.brokers.example.com | The root broker for the cluster |
| RB2 | RB2.brokers.example.com | Another root broker, not the cluster's RB |

**To verify the existing security setup on the node**

1. If node saturn is configured as an authentication broker (AB) belonging to a root broker, perform the following steps. Else, proceed to configuring the authentication broker on node saturn.

   See "Configuring the authentication broker on node saturn" on page 127.

2. Find out the root broker to which the node saturn belongs using the following command.

   ```
   # vssregctl -l -q -b \
   "Security\Authentication\Authentication Broker" \
    -k "BrokerName"
   ```

3. If the node saturn already belongs to root broker RB1, it is configured as part of the cluster. Proceed to setting up VCS related security configuration.

   See "Setting up VCS related security configuration" on page 128.

4. If the node saturn belongs to a different root broker (for example RB2), perform the following steps to remove the security credentials from node saturn.

   - Kill /opt/VRTSat/bin/vxatd process.
   - Remove the credential that RB2 has given to AB on node saturn.

```
# vssat deletecred --domain type:domainname \
--prplname prplname
```

For example:

```
# vssat deletecred --domain vx:root@RB2.brokers.example.com \
--prplname saturn.nodes.example.com
```

## Configuring the authentication broker on node saturn

Configure a new authentication broker (AB) on node saturn. This AB belongs to root broker RB1.

**To configure the authentication broker on node saturn**

1 Create a principal for node saturn on root broker RB1. Execute the following command on root broker RB1.

```
# vssat addprpl --pdrtype root --domain domainname \
 --prplname prplname --password password \
 --prpltype service
```

For example:

```
# vssat addprpl --pdrtype root \
--domain root@RB1.brokers.example.com \
--prplname saturn.nodes.example.com \
--password flurbdicate --prpltype service
```

2 Ensure that there is no clock skew between the times on node saturn and RB1.

3 Copy the /opt/VRTSat/bin/root_hash file from RB1 to node saturn.

4 Configure AB on node saturn to talk to RB1.

```
# vxatd -o -a -n prplname -p password -x vx -y domainname -q \
rootbroker -z 2821 -h roothash_file_path
```

For example:

```
# vxatd -o -a -n saturn.nodes.example.com -p flurbdicate \
-x vx -y root@RB1.brokers.example.com -q RB1 \
-z 2821 -h roothash_file_path
```

5 Verify that AB is configured properly.

```
# vssat showbrokermode
```

The command should return 1, indicating the mode to be AB.

### Setting up VCS related security configuration

Perform the following steps to configure VCS related security settings.

**Setting up VCS related security configuration**

1 Start /opt/VRTSat/bin/vxatd process.

2 Create HA_SERVICES domain for VCS.

```
# vssat createpd --pdrtype ab --domain HA_SERVICES
```

3 Add VCS and webserver principal to AB on node saturn.

```
# vssat addprpl --pdrtype ab --domain HA_SERVICES --prplname
webserver_VCS_prplname --password new_password --prpltype
service --can_proxy
```

4 Create /etc/VRTSvcs/conf/config/.secure file.

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

## Configuring LLT and GAB

Create the LLT and GAB configuration files on the new node and update the files on the existing nodes.

**To configure LLT**

1 Create the file /etc/llthosts on the new node. You must also update it on each of the current nodes in the cluster.

For example, suppose you add saturn to a cluster consisting of galaxy and nebula:

- If the file on one of the existing nodes resembles:

```
0 galaxy
1 nebula
```

- Update the file for all nodes, including the new one, resembling:

```
0 galaxy
1 nebula
2 saturn
```

2 Create the file /etc/llttab on the new node, making sure that line beginning "`set-node`" specifies the new node.

The file /etc/llttab on an existing node can serve as a guide.

The following example describes a system where node saturn is the new node on cluster number 2:

```
set-node saturn
set-cluster 2
link eth1 eth1 - ether - -
link eth2 eth2 - ether - -
```

3 On the new system, run the command:

```
# /sbin/lltconfig -c
```

### To configure GAB

1 Create the file /etc/gabtab on the new system.

- If the /etc/gabtab file on the existing nodes resembles:

```
/sbin/gabconfig -c
```

The file on the new node should be the same. Symantec recommends that you use the `-c -n`*N* option, where *N* is the number of cluster nodes.

- If the /etc/gabtab file on the existing nodes resembles:

```
/sbin/gabconfig -c -n2
```

The file on all nodes, including the new node, should change to reflect the change in the number of cluster nodes. For example, the new file on each node should resemble:

```
/sbin/gabconfig -c -n3
```

The -n flag indicates to VCS the number of nodes that must be ready to form a cluster before VCS starts.

2 On the new node, run the command, to configure GAB:

```
# /sbin/gabconfig -c
```

**To verify GAB**

1 On the new node, run the command:

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

The output should indicate that port a membership shows all nodes including the new node. The output should resemble:

```
GAB Port Memberships
===================================
Port a gen a3640003 membership 012
```

See "Verifying GAB" on page 116.

2 Run the same command on the other nodes (galaxy and nebula) to verify that the port a membership includes the new node:

```
# /sbin/gabconfig -a
GAB Port Memberships
===================================
Port a gen a3640003 membership 012
Port h gen fd570002 membership 01
Port h gen fd570002    visible ; 2
```

## Adding the node to the existing cluster

Perform the tasks on one of the existing nodes in the cluster.

**To add the new node to the existing cluster**

1 Enter the command:

```
# haconf -makerw
```

2 Add the new system to the cluster:

```
# hasys -add saturn
```

3 Stop VCS on the new node:

```
# hastop -sys saturn
```

4 Copy the main.cf file from an existing node to your new node:

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

5 Start VCS on the new node:

```
# hastart
```

6 If necessary, modify any new system attributes.

7 Enter the command:

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

## Starting VCS and verifying the cluster

Start VCS after adding the new node to the cluster and verify the cluster.

**To start VCS and verify the cluster**

1 From the new system, start VCS with the new system added to the cluster:

```
# hastart
```

2 Run the GAB configuration command on each node to verify that port a and port h include the new node in the membership:

```
# /sbin/gabconfig -a
  GAB Port Memberships
  ===================================
  Port a gen a3640003 membership 012
  Port h gen fd570002 membership 012
```

# Removing a node from a cluster

Table 7-3 specifies the tasks that are involved in removing a node from a cluster. In the example procedure, the cluster consists of nodes galaxy, nebula, and saturn; node saturn is to leave the cluster.

**Table 7-3** Tasks that are involved in removing a node

| Task | Reference |
|---|---|
| ■ Back up the configuration file.<br>■ Check the status of the nodes and the service groups. | See "Verifying the status of nodes and service groups" on page 132. |
| ■ Switch or remove any VCS service groups on the node departing the cluster.<br>■ Delete the node from VCS configuration. | See "Deleting the departing node from VCS configuration" on page 133. |
| Modify the llthosts and gabtab files to reflect the change. | See "Modifying configuration files on each remaining node" on page 136. |
| 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 136. |
| On the node departing the cluster:<br>■ Modify startup scripts for LLT, GAB, and VCS to allow reboot of the node without affecting the cluster.<br>■ Unconfigure and unload the LLT and GAB utilities.<br>■ Remove the VCS RPMs. | See "Unloading LLT and GAB and removing VCS on the departing node" on page 137. |

## Verifying the status of nodes and service groups

Start by issuing the following commands from one of the nodes to remain, node galaxy or node nebula.

**To verify the status of the nodes and the service groups**

1 Make a backup copy of the current configuration file, main.cf.

```
# cp -p /etc/VRTSvcs/conf/config/main.cf\
/etc/VRTSvcs/conf/config/main.cf.goodcopy
```

2 Check the status of the systems and the service groups.

```
# hastatus -summary

-- SYSTEM STATE
-- System      State          Frozen
A  galaxy      RUNNING        0
A  nebula      RUNNING        0
A  saturn      RUNNING        0

-- GROUP STATE
-- Group    System      Probed   AutoDisabled   State
B  grp1     galaxy      Y        N              ONLINE
B  grp1     nebula      Y        N              OFFLINE
B  grp2     galaxy      Y        N              ONLINE
B  grp3     nebula      Y        N              OFFLINE
B  grp3     saturn      Y        N              ONLINE
B  grp4     saturn      Y        N              ONLINE
```

The example output from the `hastatus` command shows that nodes galaxy, nebula, and saturn are the nodes in the cluster. Also, service group grp3 is configured to run on node nebula and node saturn, the departing node. Service group grp4 runs only on node saturn. Service groups grp1 and grp2 do not run on node saturn.

## Deleting the departing node from VCS configuration

Before you remove a node from the cluster you need to identify the service groups that run on the node.

You then need to perform the following actions:

- Remove the service groups that other service groups depend on, or
- Switch the service groups to another node that other service groups depend on.

### To remove or switch service groups from the departing node

1 Switch failover service groups from the departing node. You can switch grp3 from node saturn to node nebula.

```
# hagrp -switch grp3 -to nebula
```

2 Check for any dependencies involving any service groups that run on the departing node; for example, grp4 runs only on the departing node.

```
# hagrp -dep
```

3 If the service group on the departing node requires other service groups—if it is a parent to service groups on other nodes—unlink the service groups.

```
# haconf -makerw
# hagrp -unlink grp4 grp1
```

These commands enable you to edit the configuration and to remove the requirement grp4 has for grp1.

4 Stop VCS on the departing node:

```
# hastop -sys saturn
```

5 Check the status again. The state of the departing node should be EXITED. Make sure that any service group that you want to fail over is online on other nodes.

```
# hastatus -summary

    -- SYSTEM STATE
    -- System      State          Frozen
    A  galaxy      RUNNING        0
    A  nebula      RUNNING        0
    A  saturn      EXITED         0

    -- GROUP STATE
    -- Group    System      Probed   AutoDisabled   State
    B  grp1     galaxy      Y        N              ONLINE
    B  grp1     nebula      Y        N              OFFLINE
    B  grp2     galaxy      Y        N              ONLINE
    B  grp3     nebula      Y        N              ONLINE
    B  grp3     saturn      Y        Y              OFFLINE
    B  grp4     saturn      Y        N              OFFLINE
```

6 Delete the departing node from the SystemList of service groups grp3 and grp4.

```
# hagrp -modify grp3 SystemList -delete saturn
# hagrp -modify grp4 SystemList -delete saturn
```

7 For the service groups that run only on the departing node, delete the resources from the group before you delete the group.

```
# hagrp -resources grp4
    processx_grp4
    processy_grp4
# hares -delete processx_grp4
# hares -delete processy_grp4
```

8 Delete the service group that is configured to run on the departing node.

```
# hagrp -delete grp4
```

9 Check the status.

```
# hastatus -summary
    -- SYSTEM STATE
    -- System      State          Frozen
    A  galaxy      RUNNING        0
    A  nebula      RUNNING        0
    A  saturn      EXITED         0

    -- GROUP STATE
    -- Group    System      Probed   AutoDisabled   State
    B  grp1     galaxy      Y        N              ONLINE
    B  grp1     nebula      Y        N              OFFLINE
    B  grp2     galaxy      Y        N              ONLINE
    B  grp3     nebula      Y        N              ONLINE
```

10 Delete the node from the cluster.

```
# hasys -delete saturn
```

11 Save the configuration, making it read only.

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

## Modifying configuration files on each remaining node

Perform the following tasks on each of the remaining nodes of the cluster.

**To modify the configuration files on a remaining node**

1 If necessary, modify the /etc/gabtab file.

No change is required to this file if the `/sbin/gabconfig` command has only the argument `-c`. Symantec recommends using the `-n`*N* option, where *N* is the number of cluster systems.

If the command has the form `/sbin/gabconfig -c -n`*N*, 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.

---

**Note:** 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 security credentials from the leaving node

If the leaving node is part of a cluster that is running in a secure mode, you must remove the security credentials from node saturn. Perform the following steps.

**To remove the security credentials**

1 Kill /opt/VRTSat/bin/vxatd process.

2 Remove the root credentials on node saturn.

```
# vssat deletecred --domain type:domainname --prplname prplname
```

# Unloading LLT and GAB and removing VCS on the departing node

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 RPMs before you can delete all of the following ones.

### To stop LLT and GAB and remove VCS

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

```
# /etc/init.d/vxfen stop
```

2. Stop GAB and LLT:

```
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

3. To determine the RPMs to remove, enter:

```
# rpm -qa | grep VRTS
```

4. To permanently remove the VCS RPMs from the system, use the `rpm -e` command. Start by removing the following RPMs, which may have been optionally installed, in the order shown:

```
# rpm -e VRTScmccc
# rpm -e VRTScmcs
# rpm -e VRTScssim
# rpm -e VRTScscm
# rpm -e VRTSvcsmn
# rpm -e VRTScutil
# rpm -e VRTSweb
# rpm -e VRTScscw
# rpm -e VRTSjre15
# rpm -e VRTSjre
# rpm -e VRTSvcsdr
# rpm -e VRTSvcsag
# rpm -e VRTSacclib
# rpm -e VRTSvcsmg
# rpm -e VRTSvcs
# rpm -e VRTSvxfen
# rpm -e VRTSgab
# rpm -e VRTSllt
```

```
# rpm -e VRTSvlic
# rpm -e VRTSperl
# rpm -e VRTSpbx
# rpm -e VRTSicsco
# rpm -e VRTSatServer
# rpm -e VRTSatClient
```

5 Remove the LLT and GAB configuration files.

```
# rm /etc/lltab
# rm /etc/gabtab
# rm /etc/llthosts
```

Chapter 8

# Installing VCS on a single node

This chapter includes the following topics:



## About installing VCS on a single node

You can install VCS 5.0 RU3 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 139.

See "Creating a single-node cluster manually" on page 141.

## Creating a single-node cluster using the installer program

Table 8-1 specifies the tasks that are involved to install VCS on a single node using the installer program.

**Table 8-1** Tasks to create a single-node cluster using the installer

| Task | Reference |
|---|---|
| Prepare for installation. | See "Preparing for a single node installation" on page 140. |
| Install the VCS software on the system using the installer. | See "Starting the installer for the single node cluster" on page 140. |

## Preparing for a single node installation

You can use the installer program to install a cluster on a single system for either of the two following purposes:

- To prepare the single node cluster to join a larger cluster
- To prepare the single node cluster to be a stand-alone single node cluster

When you prepare it to join a larger cluster, install it with LLT and GAB. For a stand-alone cluster, you do not need to enable LLT and GAB.

For more information about LLT and GAB:

See "About LLT and GAB" on page 15.

## 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.

See "Starting the software installation" on page 61.

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:
```

Enter a single system name. The installer now asks if you want to enable LLT and GAB:

```
If you plan to run VCS on a single node without any need for
adding cluster node online, you have an option to proceed
without starting GAB and LLT.
Starting GAB and LLT is recommended.
Do you want to start GAB and LLT? [y,n,q,?] (y)
```

Answer `n` if you want to use the single node cluster as a stand-alone cluster.

Answer y if you plan to incorporate the single node cluster into a multi-node cluster in the future.

Continue with the installation.

See "Licensing VCS" on page 63.

# Creating a single-node cluster manually

Table 8-2 specifies the tasks that you need to perform to install VCS on a single node.

**Table 8-2** Tasks to create a single-node cluster manually

| Task | Reference |
|---|---|
| Set the PATH variable | See "Setting the path variable for a manual single node installation" on page 141. |
| Install the VCS software manually and add a license key | See "Installing the VCS software manually on a single node" on page 141. |
| Remove any LLT or GAB configuration files and rename LLT and GAB startup files.<br><br>A single-node cluster does not require the node-to-node communication service, LLT, or the membership communication service, GAB. | See "Renaming the LLT and GAB startup files" on page 142. |
| Modify the VCS startup file for single-node operation. | See "Modifying the startup files" on page 142. |
| Create and modify the VCS configuration files. | |
| Start VCS and verify single-node operation. | See "Verifying single-node operation" on page 142. |

## Setting the path variable for a manual single node installation

Set the path variable.

See "Setting the PATH variable" on page 47.

## Installing the VCS software manually on a single node

Install the VCS 5.0 RU3 RPMs manually and install the license key.

Refer to the following sections:

- See "Preparing for a manual installation when adding a node" on page 123.
- See "Installing VCS RPMs for a manual installation" on page 124.
- See "Adding a license key" on page 125.

## Renaming the LLT and GAB startup files

You may need the LLT and GAB startup files to upgrade the single-node cluster to a multiple-node cluster at a later time.

**To rename the LLT and GAB startup files**

- Rename the LLT and GAB startup files.

```
# mv /etc/init.d/llt /etc/init.d/llt.old
# mv /etc/init.d/gab /etc/init.d/gab.old
```

## Modifying the startup files

Modify the VCS startup file /etc/sysconfig/vcs to include the `-onenode` option as follows:

Change the line:

```
ONENODE=no
```

To:

```
ONENODE=yes
```

## Verifying single-node operation

After successfully creating a single-node cluster, start VCS and verify the cluster.

**To verify single-node cluster**

1. Bring up VCS manually as a single-node cluster using `hastart` with the `-onenode` option:

```
# hastart -onenode
```

2. Verify that the `had` and `hashadow` daemons are running in single-node mode:

```
# ps -ef | grep ha
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
```

# 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 8-3 specifies the activities that you need to perform to add nodes to a single-node cluster.

**Table 8-3** 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 144. |
| ■ Add Ethernet cards for private heartbeat network for Node B.<br>■ If necessary, add Ethernet cards for private heartbeat network for Node A.<br>■ Make the Ethernet cable connections between the two nodes. | See "Installing and configuring Ethernet cards for private network" on page 144. |
| Connect both nodes to shared storage. | See "Configuring the shared storage" on page 145. |
| ■ Bring up VCS on Node A.<br>■ Edit the configuration file.<br>■ Edit the startup scripts. | See "Bringing up the existing node" on page 145. |
| If necessary, install VCS on Node B and add a license key.<br>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 146. |
| Edit the configuration files on Node B. | See "Configuring LLT and GAB" on page 128. |
| Start LLT and GAB on Node B. | See "Starting LLT and GAB" on page 149. |
| ■ Start LLT and GAB on Node A.<br>■ Restart VCS on Node A.<br>■ Modify service groups for two nodes. | See "Reconfiguring VCS on the existing node" on page 149. |
| ■ Start VCS on Node B.<br>■ Verify the two-node cluster. | See "Verifying configuration on both nodes" on page 150. |

# Setting up a node to join the single-node cluster

The new node to join the existing single node running VCS must run the same version of operating system and patch level.

**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 RPMs and configuration files.
     See "Removing a node from a cluster" on page 131.
   - If the node you plan to add as Node B is also currently a single VCS node, uninstall VCS.
     See "Uninstalling VCS 5.0 RU3" on page 154.
   - If you renamed the LLT and GAB startup files, remove them.
     See "Renaming the LLT and GAB startup files" on page 142.
2. If necessary, install VxVM and VxFS.

   See "Installing VxVM or VxFS if necessary" on page 144.

## 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 40.

**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:

   ```
   # shutdown -r now
   ```

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 46.

## Bringing up the existing node

Bring up the node.

**To bring up the node**

1. Restart Node A.
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 Edit the VCS system configuration file /etc/sysconfig/vcs, and remove the "-onenode" option.

Change the line:

```
ONENODE=yes
```

To:

```
ONENODE=no
```

9 Rename the GAB and LLT startup files so they can be used.

```
# mv /etc/init.d/gab.old /etc/init.d/gab
# mv /etc/init.d/llt.old /etc/init.d/llt
```

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

Install the VCS 5.0 RU3 RPMs manually and install the license key.

Refer to the following sections:

- See "Preparing for a manual installation when adding a node" on page 123.
- See "Installing VCS RPMs for a manual installation" on page 124.
- See "Adding a license key" on page 125.

## Configuring LLT

VCS uses the Low Latency Transport (LLT) protocol for all cluster communications as a high-performance, low-latency replacement for the IP stack. LLT has two major functions.

It handles the following tasks:

- Traffic distribution
- Heartbeat traffic

Configured as described in the following sections.

## Setting up /etc/llthosts

The file llthosts(4M) is a database. This file contains one entry per system that links the LLT system ID (in the first column) with the LLT host name. You must create an identical file on each node in the cluster.

Use vi, or another editor, to create the file /etc/llthosts that contains the entries that resemble:

```
0 north
1 south
```

## Setting up /etc/lltab

The /etc/lltab file must specify the system's ID number (or, its node name), and the network links that correspond to the system. In addition, the file can contain other directives. Refer also to the sample lltab file in /opt/VRTSllt.

See "LLT directives" on page 147.

Use vi or another editor, to create the file /etc/lltab that contains the entries that resemble:

```
set-node north
set-cluster 2
link eth1 eth1 - ether - -
link eth2 eth2 - ether - -
```

The first line must identify the system where the file exists. In the preceeding example, the value for `set-node` can be: north, 0, or the file name /etc/nodename. The file needs to contain the name of the system (north in this example) to use these choices. The next two lines, beginning with the link command, identify the two private network cards that the LLT protocol uses. The order of directives must be the same as in the sample file /opt/VRTSllt/sample-lltab.

## LLT directives

For more information about LLT directives, refer to the `lltab`(4) manual page.

Table 8-4 describes the LLT directives for LLT setup.

**Table 8-4** LLT directives

| Directive | Description |
|---|---|
| `set-node` | Assigns the system ID or symbolic name. The system ID number must be unique for each system in the cluster, and must be in the range 0-31. The symbolic name corresponds to the system ID in the /etc/llthosts file.Note that LLT fails to operate if any systems share the same ID. |
| `link` | Attaches LLT to a network interface. At least one link is required, and up to eight are supported. The first argument to link is a user-defined tag shown in the `lltstat(1M)` output to identify the link. It may also be used in `llttab` to set optional static MAC addresses.<br><br>The second argument to link is the device name of the network interface. Its format is device_name:device_instance_number. The remaining four arguments to link are defaults; these arguments should be modified only in advanced configurations. There should be one link directive for each network interface. LLT uses an unregistered Ethernet SAP of 0xCAFE. If the SAP is unacceptable, refer to the `llttab(4)` manual page for information on how to customize SAP. Note that IP addresses do not need to be assigned to the network device; LLT does not use IP addresses. |
| `set-cluster` | Assigns a unique cluster number. Use this directive when more than one cluster is configured on the same physical network connection. LLT uses a default cluster number of zero. |
| `link-lowpri` | Use this directive in place of `link` for public network interfaces. This directive prevents VCS communication on the public network until the network is the last link, and reduces the rate of heartbeat broadcasts. Note that LLT distributes network traffic evenly across all available network connections. It also enables VCS communication, and broadcasts heartbeats to monitor each network connection. |

For more information about LLT directives, refer to the `llttab`(4) manual page.

## Additional considerations for LLT

You must attach each network interface that is configured for LLT to a separate and distinct physical network.

## Configuring GAB when adding a node to a single node cluster

VCS uses the Group Membership Services/Atomic Broadcast (GAB) protocol for cluster membership and reliable cluster communications. GAB has two major functions.

It handles the following tasks:

- Cluster membership
- Cluster communications

To configure GAB, use vi or another editor to set up an /etc/gabtab configuration file on each node in the cluster. The following example shows an /etc/gabtab file:

```
/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* systems are ready to form the cluster. By default, *N* is the number of systems in the cluster.

---

**Note:** Symantec does not recommend the use of the `-c -x` option for `/sbin/gabconfig`. Using `-c -x` dramatically increases configuration time for the Gigabit Ethernet controller and can lead to a split-brain condition.

---

## Starting LLT and GAB

On the new node, start LLT and GAB.

**To start LLT and GAB**

1 Start LLT on Node B.

```
# /etc/init.d/llt start
```

2 Start GAB on Node B.

```
# /etc/init.d/gab start
```

## Reconfiguring VCS on the existing node

Reconfigure VCS on the existing nodes.

**To reconfigure VCS on existing nodes**

1. On Node A, create the files /etc/llttab, /etc/llthosts, and /etc/gabtab. Use the files that are created on Node B as a guide, customizing the /etc/llttab for Node A.
2. Start LLT on Node A.

   ```
   # /etc/init.d/llt start
   ```

3. Start GAB on Node A.

   ```
   # /etc/init.d/gab start
   ```

4. Check the membership of the cluster.

   ```
   # gabconfig -a
   ```

5. Start VCS on Node A.

   ```
   # hastart
   ```

6. Make the VCS configuration writable.

   ```
   # haconf -makerw
   ```

7. Add Node B to the cluster.

   ```
   # hasys -add sysB
   ```

8. 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 9

# Uninstalling VCS

This chapter includes the following topics:



## About the uninstallvcs program

You can uninstall VCS from all nodes in the cluster or from specific nodes in the cluster using the uninstallvcs program. The uninstallvcs program does not automatically uninstall VCS enterprise agents, but offers uninstallation if proper RPMs dependencies on VRTSvcs are found.

If uninstallvcs program does not remove an enterprise agent, see the documentation for the specific enterprise agent for instructions on how to remove it.

## 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 121.

- If you have manually edited any of the VCS configuration files, you need to reformat them.

# Uninstalling VCS 5.0 RU3

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 example demonstrates how to uninstall VCS using the uninstallvcs program. The uninstallvcs program uninstalls VCS on two nodes: galaxy nebula. The example procedure uninstalls VCS from all nodes in the cluster.

## Removing VCS 5.0 RU3 RPMs

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:

```
VCS configuration files exist on this system with the following
information:

      Cluster Name: VCS_cluster2
      Cluster ID Number: 7
      Systems: galaxy nebula
      Service Groups: ClusterService groupA groupB
```

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 proceeds with uninstalling the software.

5 Answer the prompt to proceed with uninstalling the software.

Select one of the following:

- To uninstall VCS on all nodes, press `Enter`.
- To uninstall VCS only on specific nodes, enter `n`.

```
Do you want to uninstall VCS from these systems? [y,n,q] (y)
```

6 If the uninstallvcs program prompts, enter a list of nodes from which you want to uninstall VCS.

The uninstallvcs program prompts this information in one of the following conditions:

- You enter `n` .
- The program finds no VCS configuration files on the local node.

7 If RPMs, such as enterprise agents, are found to be dependent on a VCS RPM, the uninstaller prompt you on whether you want them removed. Enter `y` to remove the designated RPMs.

8 Review the uninstaller report after the verification.

9 Press Enter to uninstall the VCS RPMs.

```
Are you sure you want to uninstall VCS rpms? [y,n,q] (y)
```

10 Review the output as the uninstaller stops processes, unloads kernel modules, and removes the RPMs.

11 Note the location of summary and log files that the uninstaller creates after removing all the RPMs.

## Running uninstallvcs from the VCS 5.0 RU3 disc

You may need to use the uninstallvcs program on the VCS 5.0 RU3 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.

Appendix A

# Advanced VCS installation topics

This appendix includes the following topics:



## Using the UDP layer for LLT

VCS 5.0 RU3 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.

**Note:** LLT over UDP is not supported on IPv6.

### 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.

### Configuring LLT over UDP

The following checklist is to configure LLT over UDP:

- Make sure that the LLT private links are on different physical networks.
  If the LLT private links are not on different physical networks, then make sure that the links are on separate subnets. Set the broadcast address in /etc/llttab explicitly depending on the subnet for each link.
  See "Broadcast address in the /etc/llttab file" on page 158.
- 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 160.
- Set the broadcast address correctly for direct-attached (non-routed) links.
  See "Sample configuration: direct-attached links" on page 161.
- 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 163.

## 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:

```
# cat /etc/llttab
set-node Node0
set-cluster 1
link link1 udp - udp  50000  -  10.20.30.1  10.20.30.255
link link2 udp - udp  50001  -  10.20.31.1  10.20.31.255
```

- Verify the subnet mask using the ifconfig command to ensure that the two links are on separate subnets.

```
# ifconfig
eth2 Link encap:Ethernet HWaddr 00:04:23:AC:2B:E4
 inet addr:10.20.30.1 Bcast:10.20.30.255 Mask:255.255.255.0
eth3 Link encap:Ethernet HWaddr 00:04:23:AC:2B:E5
 inet addr:10.20.31.1 Bcast:10.20.31.255 Mask:255.255.255.0
```

## 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 161.
- See “Sample configuration: links crossing IP routers” on page 163.

Table A-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 A-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 udp.<br>A place holder string. On other unix platforms like Solaris or HP, this entry points to a device file (for example, /dev/udp). Linux does not have devices for protocols. So this field is ignored. |
| *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.<br>See “Selecting UDP ports” on page 160. |
| *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.<br>■ "-" 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 163.

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

**Table A-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 -au | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address         State
udp         0      0 *:32768                 *:*
udp         0      0 *:956                   *:*
udp         0      0 *:tftp                  *:*
udp         0      0 *:sunrpc                *:*
udp         0      0 *:ipp                   *:*
```

Look in the UDP section of the output; the UDP ports that are listed under Local Address are already in use. If a port is listed in the /etc/services file, its associated name is displayed rather than the port number in the output.

## Configuring the netmask for LLT

For nodes on different subnets, set the netmask so that the nodes can access the subnets in use. Run the following command and answer the prompt to set the netmask:

```
# set_parms ip_address
```

For example, with the following interfaces:

- For first network interface

```
IP address=192.168.30.1, Broadcast address=192.168.30.255,
Netmask=255.255.255.0
```

- For second network interface

```
IP address=192.168.31.1, Broadcast address=192.168.31.255,
 Netmask=Mask: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.

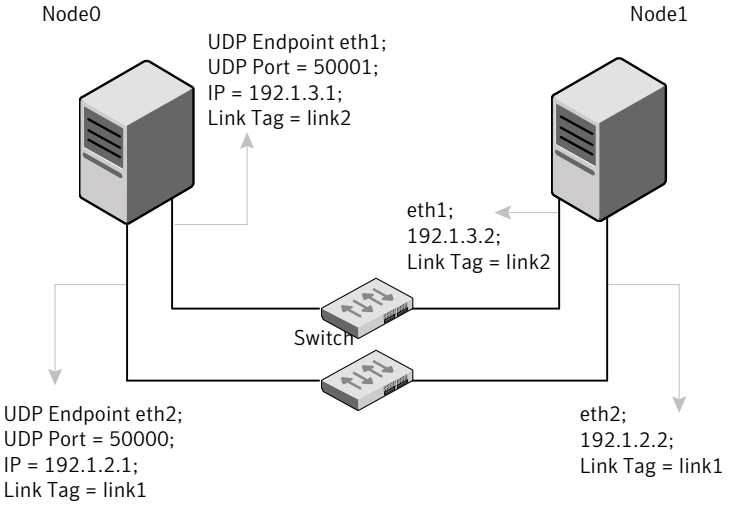
```
# cat /etc/llttab
set-node nodexyz
set-cluster 100

link link1 udp - udp 50000 - 192.168.30.1 192.168.30.255
link link2 udp - udp 50001 - 192.168.31.1 192.168.31.255
```

## Sample configuration: direct-attached links

Figure A-1 depicts a typical configuration of direct-attached links employing LLT over UDP.

**Figure A-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 udp - udp 50000 - 192.1.2.1 192.1.2.255
link link2 udp - udp 50001 - 192.1.3.1 192.1.3.255
```

The file for Node 1 resembles:

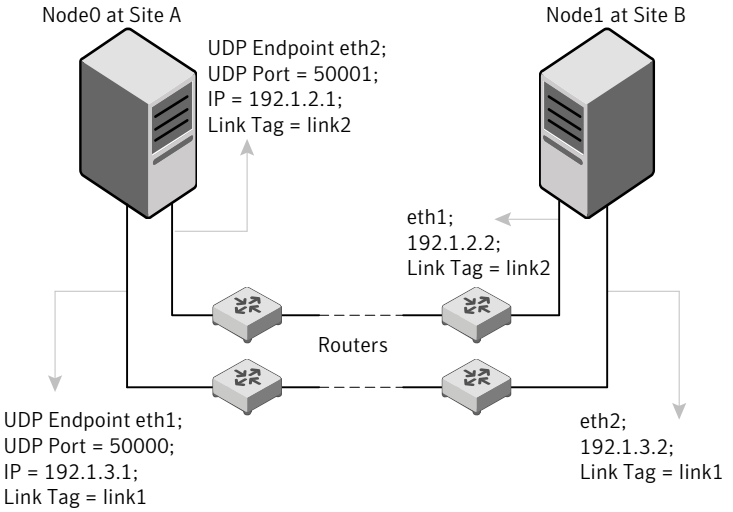
```
set-node Node1
set-cluster 1
#configure Links
#link tag-name device node-range link-type udp port MTU \
IP-address bcast-address
```

```
link link1 udp - udp 50000 - 192.1.2.2 192.1.2.255
link link2 udp - udp 50001 - 192.1.3.2 192.1.3.255
```

## Sample configuration: links crossing IP routers

Figure A-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 A-2** A typical configuration of links crossing an IP router




The configuration that the following `/etc/lltab` file represents for Node 1 has links crossing IP routers. Notice that IP addresses are shown for each link on each peer node. In this configuration broadcasts are disabled. Hence, the broadcast address does not need to be set in the `link` command of the `/etc/lltab` file.

```
set-node Node1
set-cluster 1

link link1 udp - udp 50000 - 192.1.3.1 -
link link2 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 udp - udp 50000 - 192.1.1.1 -
link link2 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
```

# Performing automated VCS installations

Using installvcs program with the `-responsefile` option is useful not only for installing and configuring VCS within a secure environment. This option is also useful for conducting unattended installations to other clusters as well. Typically, you can use the response file generated during the installation of VCS on one cluster to install VCS on other clusters. You can copy the file to a system in another cluster and manually edit the file to contain appropriate values.

When the systems are set up and meet the requirements for installation, you can perform an unattended installation. You perform the installation from one of the cluster systems where you have copied the response file.

**To perform automated installation**

1 Navigate to the folder containing the installvcs program.

```
# cd /mnt/cdrom/cluster_server
```

2 Start the installation from one of the cluster systems where you have copied the response file.

```
# ./installvcs -responsefile /tmp/response_file
```

Where /tmp/response_file is the response file's full path name.

## Syntax in the response file

The syntax of the Perl statements that are included in the response file 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"];
```

## Example response file

The example response file resembles the file that installvcs creates after the example VCS installation. The file is a modified version of the response file generated on vcs_cluster2 that you can use to install VCS on vcs_cluster3. Review the variables that are required for installation.

See "Response file variable definitions" on page 166.

```
#
# installvcs configuration values:
#
$CPI::CFG{AT_ROOTDOMAIN}="root\@east.symantecexample.com";
$CPI::CFG{CMC_CC_CONFIGURED}=1;
$CPI::CFG{CMC_CLUSTERID}{east}=1146235600;
$CPI::CFG{CMC_MSADDR}{east}="mgmtserver1";
$CPI::CFG{CMC_MSADDR}{west}="mgmtserver1";
$CPI::CFG{CMC_MS_ROOT_HASH}="758a33dbd6fae716...3deb54e562fe98";
```

```
$CPI::CFG{CMC_SERVICE_PASSWORD}="U2FsdVkX18v...n0hTSWwodThc+rX";
$CPI::CFG{ENCRYPTED}="U2FsdGVkX1+k2DHcnW7b6...ghdh+zW4G0WFIJA=";
$CPI::CFG{KEYS}{east}=[ qw(XXXX-XXXX-XXXX-XXXX-XXXX-XXX) ];
$CPI::CFG{KEYS}{west}=[ qw(XXXX-XXXX-XXXX-XXXX-XXXX-XXX) ];
$CPI::CFG{OBC_IGNOREWARNINGS}=0;
$CPI::CFG{OBC_MODE}="STANDALONE";
$CPI::CFG{OPT}{INSTALL}=1;
$CPI::CFG{OPT}{NOEXTRAPKGS}=1;
$CPI::CFG{OPT}{RSH}=1;
$CPI::CFG{SYSTEMS}=[ qw(east west) ];
$CPI::CFG{UPI}="VCS";
$CPI::CFG{VCS_ALLOWCOMMS}="Y";
$CPI::CFG{VCS_CLUSTERID}=13221;
$CPI::CFG{VCS_CLUSTERNAME}="vcs_cluster3";
$CPI::CFG{VCS_CSGNETMASK}="255.255.240.0";
$CPI::CFG{VCS_CSGNIC}{ALL}="eth0";
$CPI::CFG{VCS_CSGVIP}="10.10.12.1";
$CPI::CFG{VCS_LLTLINK1}{east}="eth1";
$CPI::CFG{VCS_LLTLINK1}{west}="eth1";
$CPI::CFG{VCS_LLTLINK2}{east}="eth2";
$CPI::CFG{VCS_LLTLINK2}{west}="eth2";

$CPI::CFG{VCS_SMTPRECP}=[ qw(earnie@symantecexample.com) ];
$CPI::CFG{VCS_SMTPRSEV}=[ qw(SevereError) ];
$CPI::CFG{VCS_SMTPSERVER}="smtp.symantecexample.com";
$CPI::CFG{VCS_SNMPCONS}=[ qw(neptune) ];
$CPI::CFG{VCS_SNMPCSEV}=[ qw(SevereError) ];
$CPI::CFG{VCS_SNMPPORT}=162;
```

## Response file variable definitions

**Table A-3** Response file variables

| Variable | Description |
|---|---|
| $CPI::CFG{OPT}{INSTALL} | Installs and configures VCS.<br>List or scalar: scalar<br>Optional or required: required |
| $CPI::CFG{OPT}{INSTALLONLY} | Installs VCS RPMs. Configuration can be performed at a later time using the `-configure` option.<br>List or scalar: scalar<br>Optional or required: optional |

**Table A-3** Response file variables *(continued)*

| Variable | Description |
|---|---|
| $CPI::CFG{SYSTEMS} | List of systems on which the product is to be installed, uninstalled, or configured.<br>List or scalar: list<br>Optional or required: required |
| $CPI::CFG{SYSTEMSCFG} | List of systems to be recognized in configuration if secure environment prevents all systems from being installed at once.<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{UPI} | Defines the product to be installed, uninstalled, or configured.<br>List or scalar: scalar<br>Optional or required: required |
| $CPI::CFG{OPT}{KEYFILE} | Defines the location of an ssh keyfile that is used to communicate with all remote systems.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{OPT}{LICENSE} | Licenses VCS only.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{OPT}{NOLIC} | Installs the product without any license.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{AT_ROOTDOMAIN} | Defines the name of the system where the root broker is installed.<br>List or scalar: list<br>Optional or required: optional |

**Table A-3** Response file variables *(continued)*

| Variable | Description |
|---|---|
| $CPI::CFG{OPT}{PKGPATH} | Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{OPT}{TMPPATH} | Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{OPT}{RSH} | Defines that *rsh* must be used instead of ssh as the communication method between systems.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{DONOTINSTALL}<br>{RPM} | Instructs the installation to not install the optional RPMs in the list.<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{DONOTREMOVE}<br>{RPM} | Instructs the uninstallation to not remove the optional RPMs in the list.<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{VCS_CLUSTERNAME} | Defines the name of the cluster.<br>List or scalar: scalar<br>Optional or required: required |
| $CPI::CFG{VCS_CLUSTERID} | An integer between 0 and 65535 that uniquely identifies the cluster.<br>List or scalar: scalar<br>Optional or required: required |

**Table A-3** Response file variables *(continued)*

| Variable | Description |
|---|---|
| $CPI::CFG{KEYS}<br>{SYSTEM} | List of keys to be registered on the system.<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{OPT_LOGPATH} | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{CONFIGURE} | Performs the configuration if the RPMs are already installed using the `-installonly` option.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{VCS_LLTLINK#}<br>{SYSTEM} | Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (LLTLINK1 and LLTLINK2). Up to four LLT links can be configured.<br>List or scalar: scalar<br>Optional or required: required |
| $CPI::CFG{VCS_LLTLINKLOWPRI}<br>{SYSTEM} | Defines a low priority heartbeat link. Typically, LLTLINKLOWPRI is used on a public network link to provide an additional layer of communication.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{VCS_SMTPSERVER} | Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for Web notification.<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{VCS_SMTPRECP} | List of full email addresses (example: user@symantecexample.com) of SMTP recipients.<br>List or scalar: list<br>Optional or required: optional |

**Table A-3** Response file variables *(continued)*

| Variable | Description |
|---|---|
| $CPI::CFG{VCS_SMTPRSEV} | 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.<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{VCS_SNMPPORT} | Defines the SNMP trap daemon port (default=162).<br>List or scalar: scalar<br>Optional or required: optional |
| $CPI::CFG{VCS_SNMPCONS} | List of SNMP console system names<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{VCS_SNMPCSEV} | 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.<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{VCS_USERENPW} | List of encoded passwords for users<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{VCS_USERNAME} | List of names of users<br>List or scalar: list<br>Optional or required: optional |
| $CPI::CFG{VCS_USERPRIV} | List of privileges for users<br>List or scalar: list<br>Optional or required: optional |

**Table A-3** Response file variables *(continued)*

| Variable | Description |
|---|---|
| $CPI::CFG{OPT}{UNINSTALL} | List of systems where VCS must be uninstalled.<br>List or scalar: scalar<br>Optional or required: optional |

# Installing VCS with a response file where ssh or rsh are disabled

In secure enterprise environments, ssh or rsh communication is not allowed between systems. In such cases, the installvcs program can install and configure VCS only on systems with which it can communicate—most often the local system only. When installation is complete, VCS creates a response file.

See "Response file variable definitions" on page 166.

The response file that the installvcs program generates contains descriptions and explanations of the variables and their values. You copy this file to the other systems in the cluster, and edit it to reflect the current local system. You can use the installation program with the `-responsefile` option to install and configure VCS identically on each system without being prompted.

**To use installvcs in a secure environment**

1. On one node in the cluster, start VCS installation using the installvcs program.

   See "Starting the software installation" on page 61.

2. Review the output as the installer performs the initial system checks.

   The installer detects the inability to communicate between systems.

3. Press the Enter key to install VCS on one system and create a response file with which you can install on other systems.

   ```
   Would you like to install Cluster Server on systems galaxy only
   and create a responsefile for systems nebula? [y,n,q] (y)
   ```

4. Enter all cluster information. Proceed with the installation and configuration tasks.

   See "Installing and configuring VCS 5.0 RU3" on page 60.

   The installvcs program installs and configures VCS on systems where communication is possible.

5 After the installation is complete, review the installer report.

The installer stores the installvcs-*universaluniqueidentifier* response file in the /opt/VRTS/install/logs/installvcs-*universaluniqueidentifier*/.response directory where *universaluniqueidentifier* is a variable to uniquely identify the file.

6 If you start VCS before VCS is installed and started on all nodes in the cluster, you see the output similar to:

```
VCS:11306:Did not receive cluster membership, manual
intervention may be needed for seeding
```

7 Use a method of your choice (for example, by using NFS, ftp, or a floppy disk). Copy the response file in a directory such as /tmp on the system where you want to install VCS.

8 Edit the response file.

For the variables in the example, change the name of the system to reflect the current local system:

```
.
$CFG{SYSTEMS} = ["east"];
.
.
$CFG{KEYS}{east} = ["XXXX-XXXX-XXXX-XXXX-XXXX-XXX"];
.
```

For demo or site licenses, the license key need not be changed.

9 On the next system, perform the following:

- Mount the product disc.
  See "Mounting the product disc" on page 49.
- Start the software installation using the `installvcs -responsefile` option.

  ```
  # ./installvcs -responsefile /tmp/installvcs-uui.response
  ```

  Where uui is the Universal Unique Identifier that the installer automatically assigned to the response file.
  See "Starting the software installation" on page 61.

10 Repeat step 7 through step 9 until VCS has been installed on all nodes in the cluster.

# Index

## M



## N



## O



## P



## R



## S

## U



## V