Veritas™ Cluster Server Implementation Guide

VMware ESX

5.0

11472287

symantec.

Veritas Cluster Server Implementation Guide

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Third-party legal notices

All third-party copyrights associated with this product are listed in the Third Party Copyrights document, which is included on the product disc.

Technical support

For technical assistance, visit:
http://www.symantec.com/enterprise/support/assistance_care.jsp.

Select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Chapter 9 Configuring virtual machines for high availability

Chapter 10 Configuring virtual machines for disaster recovery

Section III Configuring applications in virtual machines

Chapter 11 Deploying VCS components on virtual machines running Linux

Chapter 12 Deploying VCS components on virtual machines running Windows

Appendix A Advanced topics

Index

Section I

Installing VCS for VMware ESX

This section contains the following chapters:

Chapter 1

Introducing VCS for VMware ESX

This chapter contains the following topics:

Features

The following features appear in this release of VCS.

- High availability
  VCS provides high availability for virtual machines, the applications that run in the virtual machines, and the ESX Server.
- Disaster recovery
  Use VCS to prepare your environments for disaster—and have confidence that your clusters can survive a disaster. Requires a supported VCS agent for replication.
- Fire drill
  Preparing for disaster starts with running fire drills. Run the fire drill to see how well your clusters can survive a disaster. Requires a supported VCS agent for replication.
- Support for VMotion and Distributed Resource Scheduler (DRS)
  In the event that VMotion or DRS needs to move a virtual machine, VCS correctly interprets this and does not register that as a failure.
- Centralized management
  To centrally manage your clusters, use the Veritas Cluster Management Console.
  See the *Veritas Cluster Server User's Guide*.
- The Veritas Virtualization Manager
  Use the Veritas Virtualization Manager for quick deployment and conversion of virtual machines to high availability and for disaster recovery.
- Notification
  VCS can notify you of events. You have access to SMTP email notification and SNMP trap notification.
- Last-known good copy
  After testing application configuration and data integrity, you can take a snap shot of the "last known good copy" of the operating system for safe-keeping. Requires a supported VCS agent for replication.
- Virtual machine storage management
  Enables you to easily grow your application data mounts.

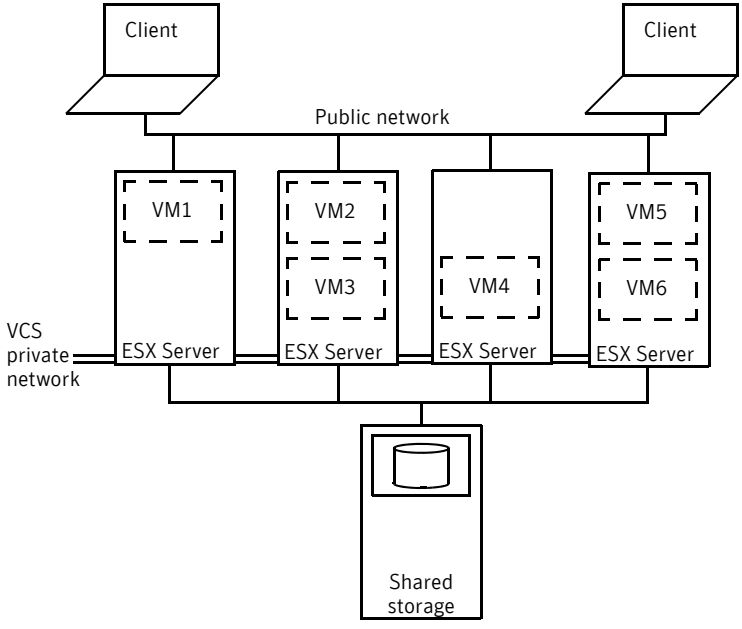
About VCS

Veritas Cluster Server (VCS) can monitor sites, clusters, systems, virtual machines, and applications. When you group two or more ESX Server systems together with VCS, they form a cluster. Each ESX Server that runs VCS becomes a node in a cluster. VCS enables you to manage groups of applications. These groups of applications are called service groups. A VCS cluster can use shared storage devices. In the event of hardware or software failure, VCS fails over the service group, either wholly or partially depending on your configuration, to another node in the same cluster, or even to a remote node in a different cluster.

VCS for VMware ESX runs the majority of the VCS components (the engine, agents, GAB, and LLT) at the ESX console operating system, and not in the individual virtual guest operating systems.

Figure 1-1 illustrates a typical four-node VCS cluster configuration connected to shared storage. Client workstations receive service over the public network from applications running on VCS nodes. VCS monitors the nodes, virtual machines, and applications on the nodes. VCS nodes in the cluster communicate over a private network.

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



Multiple nodes

VCS runs on each node in the cluster. The private network enables the nodes to share identical state information about all resources and to recognize: active nodes, nodes that are joining or leaving the cluster, and failed nodes. The private network requires two communication channels for heartbeats.

Virtual machines and applications

You can make the virtual machines and applications that run inside the virtual machines highly available. When the virtual machine or application faults, VCS can take corrective actions. In some cases, you might want it to restart the virtual machine. In other situations, you might want it to fail over to a different node entirely.

Detailed and basic monitoring

For certain applications, VCS supports detailed application monitoring and the ability to detect a graceful shut down. If confronted with the failure of an application, VCS moves the virtual machine that runs the application onto another node. If confronted with a user intentionally moving the virtual machine, VCS takes no action.

In general, basic monitoring checks for running application processes. Detailed monitoring, however, performs application-specific tasks to check the application's health.

The Veritas Virtual Machine Toolkit

The Veritas Virtual Machine Toolkit is a package of tools that reside in the virtual machine and that provide configuration resources and wizards. You can make this toolkit available through the Veritas Virtualization Manager.

Shared storage

A VCS hardware configuration usually consists of multiple nodes that are connected to shared storage through I/O channels. Shared storage provides multiple access paths to the same data, and enables VCS to restart virtual machines on alternate nodes when a node fails.

LLT and GAB

VCS uses two components, LLT and GAB, to share data over private networks among nodes.

- LLT (Low Latency Transport) provides fast, kernel-to-kernel communications, and monitors network connections. The system administrator configures LLT by creating the configuration files:
  - /etc/llthosts, which lists all the nodes in the cluster
  - /etc/lltab, which 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 required to maintain a synchronized state among the nodes. It monitors disk communications such as the VCS heartbeat utility. The system administrator configures the GAB driver by creating a configuration file (/etc/gabtab).

Network channels for heartbeats

For the VCS private network, heartbeats travel over two network channels. These network channels are also used for transmitting information.

Each cluster configuration requires at least two network channels between the systems. The requirement for two channels is to protect your cluster against network partitions. For more information about network partitions:

- See the *Veritas Cluster Server User's Guide*.
- "Setting up the private network" on page 35

Service groups

Service groups are a basic building block of resources for VCS. A service group is how you structure dependencies among resources. For example, your virtual machine must have storage to work. The virtual machine has a dependency on its storage.

When you use the Veritas Virtualization Manager to configure virtual machines, it also creates service groups. The service group that it creates is for the virtual machine, its network, and storage.

For applications, like Oracle or SQL, the service group becomes slightly more complicated. These applications require the addition of the GuestOSApp resource. Finally, if you want disaster recovery, the service group requires the VMIP and DNS resources. For more information on service groups:

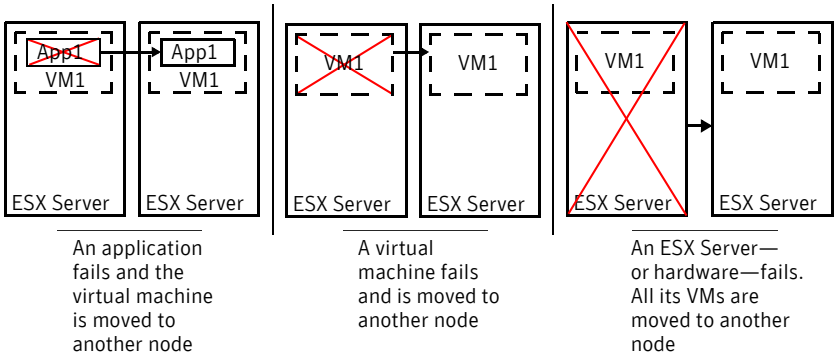
See the *Veritas Cluster Server User's Guide*.

About high availability using VCS for VMware ESX

In the event that a node, virtual machine, or application in a virtual machine fails, VCS can automatically move the virtual machine to another node.

VCS monitors applications within virtual machines. For all applications inside of virtual machines, configure them to start automatically when the virtual machine starts. When you want to stop the application, you stop it as you normally would stop the application.

Figure 1-2 A failed node, virtual machine, or application moved to a working system



About disaster recovery using VCS for VMware ESX

In the event of a disaster, you can use VCS software to ensure that your data remains online and that your customers remain happy. Disaster recovery protects your servers from unwanted downtime in the event of a disaster to a cluster. VCS can migrate your applications to a safe, predetermined location, and with a minimum of downtime, to keep your services running.

You need to test your systems to see if they can survive a disaster. Veritas provides for this testing with fire drills. These fire drills give your nodes a full test of their functionality during an emergency.

When you prepare for disaster, you should have a last known good copy of your host and its transactions available. With the last known good copy, even if a disaster strikes within a disaster (a corrupted boot image), you can recover with the last stable copy of the virtual machine.

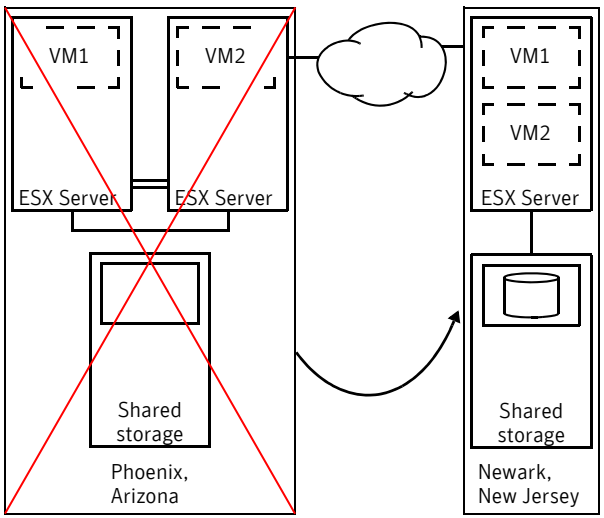
Replicated storage

VCS supports several replication technologies, and uses them for disaster recovery. VCS agents manage the replication status between primary and secondary sites. Contact your Symantec sales representative for a list of replication technologies supported with this release of VCS.

Global clusters

You can create clusters that operate in two geographically diverse locations. In the event that one cluster fails completely, the entire cluster fails over to the back-up location. As its virtual machines come back online, clients re-direct to the new site. Applications restart in the virtual machines.

Figure 1-3 A two-node cluster with one globally clustered node



Global clustering requires a separate license. For more information:

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

Installation road map

The following road map illustrates a VCS for VMware ESX installation.

Figure 1-4 Suggested installation flow

The following table describes where to look for the pertinent road map information.

Table 1-1 Installation road map

Road map entry	Document or chapter
Install the ESX Servers, the VirtualCenter Server, and the VMware license server.	See the appropriate VMware documentation.
Install VCS on the ESX Servers. Optionally install the global clustering option and disaster recovery agents.	■ See "Requirements" on page 25. ■ See "Planning to install VCS on an ESX Server" on page 31. ■ See "Installing and configuring VCS on ESX Servers" on page 43. ■ See "Verifying VCS on ESX Servers" on page 77.
Install the Veritas Virtual Manager on a standalone system.	See "Installing the Veritas Virtualization Manager (VVM)" on page 121.
Run the Veritas Virtual Manager to configure virtual machines.	■ See "Configuring virtual machines for high availability" on page 127. ■ See "Configuring virtual machines for disaster recovery" on page 133.
Install the guest application in the virtual machine.	See the application's documentation.
Install and configure the Virtual Machine Toolkit in the virtual machine.	■ See "Deploying VCS components on virtual machines running Linux" on page 155. ■ See "Deploying VCS components on virtual machines running Windows" on page 183.
Configure your applications.	■ See "Deploying VCS components on virtual machines running Linux" on page 155. ■ See "Deploying VCS components on virtual machines running Windows" on page 183.
Manage VCS components.	See the *Veritas Cluster Server User's Guide*.

Chapter 2

Requirements

This chapter contains the following topics:

Hardware requirements

Make sure that your hardware meets the following requirements.

Table 2-1 Hardware requirements for a cluster

Item	Description
VCS systems	From one to eight ESX Servers that run the supported ESX Server operating system version. See "Required servers" on page 27.
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 applications that migrate between systems in the cluster.
Disk space	See Table 2-2, "Disk space requirements and totals."
Network Interface Cards	In addition to the built-in public Network Interface Card (NIC), VCS requires at least one more NIC per system. Symantec recommends two additional NICs.
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 system requires at least 256 megabytes in addition to other system and application requirements.

Required disk space

Confirm that your system has enough free disk space to install VCS. The following table shows the approximate disk space usage by directory for the Veritas Cluster Server RPMs.

Table 2-2 Disk space requirements and totals

Package	/	/opt	/usr	/var	Totals
Required	336 MB	324 MB	7 MB	4 MB	671 MB
Optional	40 MB	41 MB	1 MB	1 MB	83 MB
Required and optional total	376 MB	365 MB	7 MB	2 MB	750 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.

Required servers

These servers are required to run VCS for VMware ESX 5.0.

- ESX Server 3.0
- VirtualCenter Server
- VMware License server

Refer to the VMware documentation for more information about these servers.

Required VMware components

- VMware Tools installed in the guest operating system of each virtual machine. VCS requires VMware Tools for application monitoring.
- VMware VirtualCenter Web Service properly configured to enable SSL communication for the Virtual Machine Deployment wizard.
- Set up the VirtualCenter Server up with cluster objects that have a one-to-one mapping between the VCS cluster and the VMWare cluster object.
- Configure the ESX firewall to open all incoming and outgoing ports. Refer to the VMware documentation for more information.

Supported software

VCS supports several replication solutions. Contact your Symantec sales representative for the solutions supported by VCS.

Supported guest operating systems

Table 2-3 lists the architectures and operating systems that VCS for VMware ESX 5.0 supports for guest operating systems.

Table 2-3 Supported operating systems and architectures

Guest operating systems	Kernels	Architectures	File systems/volume managers
Windows 2000	---	32-bit	NTFS/---
†Windows Server 2003	---	32-bit	*NTFS/---
†Red Hat Enterprise Linux 4 (RHEL 4) Update 3	2.6.9-34.EL 2.6.9-34.smp 2.6.9-34.hugemem	x86 (32-bit)	ext2, *ext3, reiserfs/LVM
†SUSE Linux Enterprise Server 9 (SLES 9) with SP3	2.6.5-7.244 2.6.5-7.244-smp 2.6.5-7.244-bigsmp	x86 (32-bit)	ext2, ext3, *reiserfs/LVM

* Supports increasing allocation of storage.

† Supports the mount .iso feature.

Symantec products will 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. Read this TechNote *before* installing any Symantec product: http://support.veritas.com/docs/281993.

Supported guest applications for detailed monitoring

Table 2-4 lists the applications that VCS for VMware ESX 5.0 supports for detailed monitoring.

Table 2-4 Supported operating systems and architectures

Applications	Versions
IIS	5.0 and 6.0
SQL	■ Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (both require SP4), or ■ Microsoft SQL Server 2005, 32-bit (SP1 required)
Apache Web Server	1.3, 2.0, and 2.2
IBM HTTP Server	1.3 and 2.0
Oracle	10g

Chapter 3

Planning to install VCS on an ESX Server

This chapter contains the following topics:

About installing VCS on an ESX Server

Before you perform the VCS installation, read the following Veritas Technical Support TechNote for the latest information on updates, patches, and software issues:

http://entsupport.symantec.com/docs/285191

About optional VCS features

Make sure to install all RPMs when the installation program prompts you to get the optional features. Review the description of each optional feature and decide which features that you want to configure with VCS:

- Veritas Cluster Management Console
- SMTP email notification for VCS events
- SNMP trap notification for VCS events
- Global clusters using VCS

Note: This release does not support configuring clusters in the secure mode. Do not configure the Symantec Product Authentication server while installing or configuring VCS.

Veritas Cluster Management Console

The Veritas Cluster Management Console is a management interface that enables you to monitor and administer clusters from a web console.

You install one instance of the Cluster Management Console outside all of your clusters on a standalone server. With the console, you can input commands to the multi-cluster management engine, the management server.

If a firewall separates the management server and cluster nodes, you need to install a component called the cluster connector on each cluster node. The cluster connector enables communication with clusters through firewalls and provides buffering for cluster data. If the console goes offline and then comes back online, it can retrieve data collected during the offline period from the cluster connector buffer.

For more information:

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

Notifications

VCS for VMware ESX offers two server-side notification services. You can get notification from SMTP email or using SNMP traps.

For more information:

See the *Veritas Cluster Server User's Guide*

SMTP email notification for VCS events

You have the option to configure SMTP email notification of VCS events by the VCS Notifier component. If you choose SMTP notification, have the appropriate information ready.

SNMP trap notification for VCS events

You have the option to configure SNMP trap notification of VCS events by the VCS Notifier component. If you choose SNMP notification, have the appropriate information ready.

Global clusters using VCS

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.

If you choose to configure global clusters, the installer enables you to choose whether or not to use the same NIC, virtual IP address, and netmask as are configured for the ClusterService group, which are the defaults. If you choose not to use the same networking information, you must specify appropriate values for the NIC, virtual IP address, and netmask when you are prompted.

Preparing to install VCS

Make sure that each system where you want to install VCS meets both the hardware and software requirements.

See "Requirements" on page 25.

After planning the VCS features that you want to configure, you must prepare to configure these features.

Performing pre-installation tasks

Table 3-1 lists the tasks you must perform before proceeding to install VCS.

Table 3-1 Pre-installation tasks

Task	Reference
Set the PATH and MANPATH variables.	"Setting the PATH variable" on page 34 "Setting the MANPATH variable" on page 35
Set up the private network.	"Setting up the private network" on page 35
Configuring the private network.	"Selecting virtual interfaces for use by the private network" on page 36
Enable communication between systems.	"Enabling communication between systems" on page 37
Review basic instructions to optimize LLT media speeds.	"Optimizing LLT media speed settings on private NICs" on page 37
Review guidelines to help you set the LLT interconnects.	"Guidelines for setting the media speed of the LLT interconnects" on page 37
Set up `ssh` on cluster systems.	"Setting up ssh on cluster systems" on page 37
Obtain license keys.	"Obtaining VCS license keys" on page 39
Mount the product disc	"Preparing your VCS installation and configuration information" on page 39

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

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
```

Setting up the private network

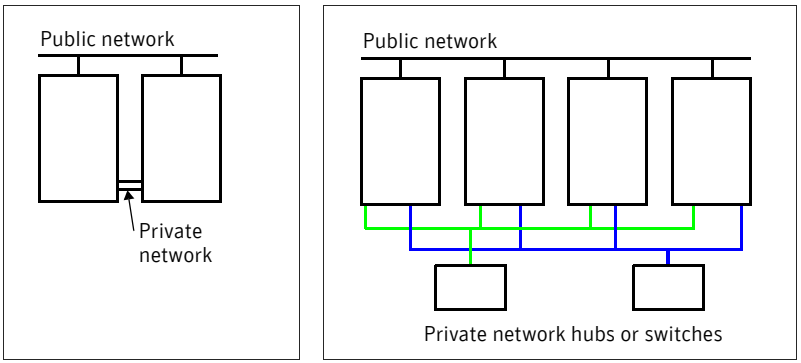
VCS requires you to setup a private network between the systems that form part of a cluster. If you have more than one private network setup for VCS, you can share it with VMotion.

To set up the private network hardware

1. Install the required network interface cards (NICs).
2. Connect the private NICs on each system.
3. Use cross-over Ethernet cables (supported only on two systems), or independent hubs, for each VCS communication network. Ensure that power to the hubs comes from separate sources. On each system, use two independent network cards to provide redundancy.

   During the process of setting up heartbeat connections, note that a chance for data corruption exists if a failure removes all communications between the systems and still leaves the systems running and capable of accessing shared storage.

Figure 3-1 Private network setups: two-node and four-node clusters



4 Test network connections by temporarily assigning network addresses and use `telnet` or `ping` to verify communications.
LLT uses its own protocol, and does not use TCP/IP. Therefore, to ensure the private network connections are used only for LLT communication and not for TCP/IP traffic, unconfigure the temporary addresses after testing.
The installvcs program configures the private network in the cluster during installation.
See "About installing and configuring VCS" on page 44.

Selecting virtual interfaces for use by the private network

VCS uses LLT private links to monitor network communication. LLT requires virtual interfaces that it can use for private links.

During installation you can either specify physical interface or virtual interface information for the private links.

- If you choose to specify physical interface information, the installer creates a virtual interface that is mapped to the physical interface that you chose.
- If you choose to specify an existing virtual interface, verify that it is mapped to the correct physical interface.

On each node, Symantec recommends that you map at least two virtual interfaces to two separate physical interfaces to provide redundancy.

Using network switches

You can use network switches instead of hubs.

Enabling communication between systems

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 permissions for the system where you run installvcs program to issue `ssh` commands as root 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.

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

See "Performing VCS installation in a secure environment" on page 60.

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 switches or hubs used for the interconnects 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

If you have hubs or switches for LLT interconnects, Symantec recommends using the Auto_Negotiation media speed setting on each Ethernet card on each node. If you do not use Auto_Negotiation, you have to set it to the same speed on all nodes for all NICs used by LLT.

If you have hubs or switches for LLT interconnects and you do not use the Auto_Negotiation media speed setting, set the hub or switch port to the same setting as that 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.

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. Verify that `ssh` is configured correctly before starting the installation process.

Configuring ssh

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

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 prompted, 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 beginning with ssh_dss and ending 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 VCS is to be installed.
   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 from which the installation is taking place:
   ```
   # 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 prompted, enter your DSA passphrase.
   You are ready to install VCS on several systems by running the installvcs program on any one of them or 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 will not be prompted for the passphrase. Refer to the Red Hat documentation for more information.
9. To verify that you can connect to the systems on which VCS is to be installed, type:
   ```
   # ssh -x -l root north ls
   # ssh -x -l root south ifconfig
   ```

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

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

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

http://www.veritas.com/buy/vLicense/vLicenseHome.jhtml

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

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

Preparing your VCS installation and configuration information

When you perform the installation, ready the following information.

- To install the VCS RPMs, prepare the system names and license keys.
  - The system names
    The names of the systems where you plan to install VCS.
  - The license keys
    Keys can include: a valid site license, a demo license, a VCS global cluster license key.
    See "Obtaining VCS license keys" on page 39.
- To configure VCS, prepare the cluster's name, the cluster's unique ID, and the names for the private network's NICs.
  - The cluster's name
    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 "_".
    For example: **`vcs_cluster27`**

- The cluster's unique ID number
  A number in the range of 0-65535. Within the site that contains the cluster, each cluster must have a unique ID.
- The private network's device names for the NICs
  The device names of the NICs that the private networks use among systems.
  Do not use the public network's name of the network interface card, which is typically vswif0.
  Example: **`vswif1, vswif2`**

- To add users to VCS, prepare the VCS user's name, password, and privileges.
  - The VCS user's privileges
    Users have three levels of privilege: A=Administrator, O=Operator, or G=Guest.
- For the Cluster Management Console to locally manage this cluster (optional), prepare the names of the public NICs for each node in the cluster, and the virtual IP address of the NIC for the console.
  - The name of the public NIC for each node in the cluster
    The device name for the NIC that provides public network access.
    Example: vswif0
  - A virtual IP address of the NIC for the Cluster Management Console
    This virtual IP address becomes a resource for use by the ClusterService group that includes the Cluster Management Console. The cluster virtual IP address can fail over to another cluster system, making the Web Console highly available.
- For the configuration of the cluster connector for the Cluster Management Console, prepare the management server's network address for the console, the Cluster Management Console's service account password, and the root hash of the management server.
  - The management server network address for Cluster Management Console
    The Cluster Management Console cluster connector requires the management server network address.
    For example: mgmtserver1.symantecexample.com
    See "Veritas Cluster Management Console" on page 32.
  - A Cluster Management Console service account password
    You need to set this account password while you install the management server.

- The root hash of the management server
  You can use `vssat showbrokerhash` command and copy the root hash of the management server.

- To configure SMTP email notification (optional), prepare the domain-based address of the SMTP server, the email addresses recipients, and select the event's severity.
  - The domain-based address of the SMTP server
    The SMTP server sends notification emails about the events within the cluster.
    Example: smtp.symantecexample.com
  - The email address of each SMTP recipient to be notified
    Example: john@symantecexample.com
  - 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.
    Example: E

- To configure SNMP trap notification (optional), prepare the SNMP trap daemon's port, the SNMP console's system name, and select the event's severity.
  - The port for the SNMP trap daemon
    The default port 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.
    Example: E

- To configure global clusters (optional), prepare the name of the public NIC, the NIC's virtual IP address, and the netmask for the NIC's virtual IP address.
  - The name of the public NIC
    You can use the same NIC that you configured for the ClusterService group. Otherwise, specify appropriate values for the NIC.
    Example: **`vswif0`**
  - The virtual IP address of the NIC
    You can use the same virtual IP address that you configured for the ClusterService group. Otherwise, specify appropriate values for the virtual IP address.
    Example: **`10.10.12.1`**

- The netmask for the virtual IP address
  You can use the same netmask as configured for the ClusterService group. Otherwise, specify appropriate values for the netmask.
  Example: `255.255.240.0`

Optional VCS RPMs

The optional VCS RPMs include:

- VRTScmccc — Veritas Cluster Management Console Cluster Connector
- VRTScmcs — Veritas Cluster Management Console
- VRTScssim — VCS Simulator
- VRTSvcsdc - VCS documentation
- VRTSvcsmn - Manual pages for VCS commands

Chapter 4

Installing and configuring VCS on ESX Servers

This chapter contains the following topics:

About installing and configuring VCS

You install VCS on ESX Servers. You can install VCS on clusters of up to eight systems. The installvcs program uses `ssh` to install by default. To install VCS, you can use either:

- The Veritas product installer — Use the product installer to install different Symantec products, including VCS.
- The installvcs program — Use the installvcs program to install VCS.

Installation quick start

If you are comfortable loading enterprise-level software, review the following list, gather your information, and start the installation.

If you have not installed VCS before, or you are new to installing enterprise-level software, continue through this chapter.

- Prepare your hardware.
  See "Performing pre-installation tasks" on page 34.
- Prepare the information you need.
  See "Preparing your VCS installation and configuration information" on page 39.
- Start the installation and follow the installer's instructions.
  See "Starting the software installation" on page 48.

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 enables you to install, configure, license, and start VCS on multiple nodes.

You can configure optional VCS components:

- The Web-based Cluster Management Console
- Notification features such as SNMP and SMTP
- The wide area Global Cluster feature

Note: This release does not support configuring clusters in the secure mode. Do not configure the Symantec Product Authentication server while installing or configuring VCS.

Optional installvcs program actions

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

Table 4-1 Optional installvcs program features

Optional action	Reference
Check the systems to verify that they meet the requirements to install VCS.	See "Checking the systems for installation" on page 47.
Install VCS RPMs without configuring VCS.	See "Installing VCS using installonly option" on page 60.
Configure or reconfigure VCS when VCS RPMs are already installed.	See "Configuring VCS using configure option" on page 60.
Perform secure installations using values stored in a configuration file.	See "Performing VCS installation in a secure environment" on page 60.
Perform automated installations using values stored in a configuration file.	See "Performing automated installations" on page 62.

Interacting with the installvcs program

The installer program displays question prompts, such as: **[y, n, q, ?] (y)**. The response in parentheses is the default answer. To accept the default value press the Return key. Enter the **?** character to get help to answer the prompt. Enter **q** to quit the installation.

At other times during the installation, the installer prompts you to type information. The installer program 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.

When the installer prompts you to answer a series of configuration-related 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 re-enter all of the information for the set.

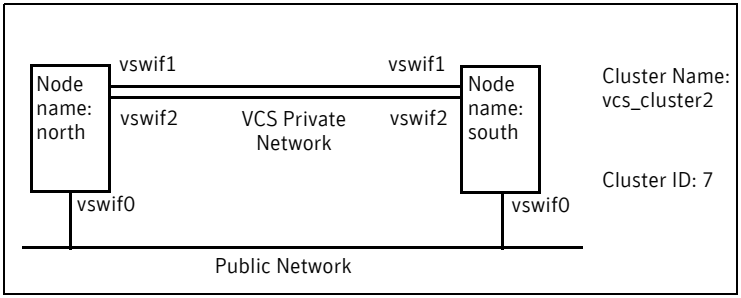
Installing and configuring VCS 5.0

Figure 4-1 illustrates an example VCS installation. The two systems where you install VCS are: north and south. 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.

For the purposes of this example, virtual interface vswif1 is mapped to physical interface vmnic1. Similarly vswif2 is mapped to vmnic2.

See "Selecting virtual interfaces for use by the private network" on page 36.

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



Installation and configuration task overview

Table 4-2 lists the installation and configuration tasks.

Table 4-2 Installation and configuration tasks

Task	Reference
Start the installation process and choose the installation	■ "Checking the systems for installation" on page 47 (optional) ■ "Starting the software installation" on page 48 ■ "Specifying systems for installation" on page 48 ■ "Licensing VCS" on page 49 ■ "Choosing VCS RPMs" on page 50 ■ "Choosing to install VCS RPMs or to configure VCS" on page 50

Table 4-2 Installation and configuration tasks

Task	Reference
Configure the cluster and optional features	■ "Configuring the cluster" on page 51 ■ "Adding VCS users" on page 52 (optional) ■ "Configuring cluster connector" on page 53 (optional) ■ "Configuring SMTP email notification" on page 55 (optional) ■ "Configuring SNMP trap notification" on page 56 (optional) ■ "Configuring global clusters" on page 57 (optional)
Install the RPMs and create configuration files	■ "Installing the VCS RPMs" on page 58 ■ "Creating VCS configuration files" on page 58
Start VCS and its components	■ "Starting VCS" on page 59 ■ "Completing the installation" on page 59
Perform the post-installation tasks	■ "Copying the Implementation Guide to each node" on page 59
Verify the cluster	■ "Verifying the cluster after installation" on page 60

Checking the systems for installation

Before beginning 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 ...
```

To check the systems

1 Navigate to the folder containing the installvcs program.

```
# cd /cdrom/cluster_server
```

2 Start the pre-installation check:

```
# ./installvcs -precheck north south
```

The program proceeds in a non-interactive mode, examining 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 to a log file.

See "About installvcs command options" on page 69.

Starting the software installation

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

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 containing the installvcs program.
   ```
   # cd /cluster_server
   ```
3. Start the installvcs program.
   ```
   # ./installvcs
   ```
   The installer begins with a copyright message and specifies the directory where the logs are created.

Specifying systems for installation

The installer program prompts you for the system names where you want to install VCS. It 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: north south
   ```
   For a single node installation, enter one name for the system.
   See "Starting the installer for the single node cluster" on page 107.

2 Review the output as the installer verifies the systems you specify. The installer program:

- Checks that the local node that runs 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 a previous version of VCS is installed

Licensing VCS

The installer checks whether VCS license keys are currently in place on each system. If the license keys are absent, the installer prompts you for them.

See "Checking licensing information on the system" on page 68.

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 north: [?) XXXX-XXXX-XXXX-XXXX-XXX
XXXX-XXXX-XXXX-XXXX-XXX successfully registered on north
VCS license registered on north
```

3 Enter keys for additional product features.

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

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

Do you want to enter another license key for north? [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 south
VCS license registered on south

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

Choosing VCS RPMs

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 previously installed RPMs.
2. Choose the VCS RPMs.

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

3. View the list of RPMs that the installer installs 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 to 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 cluster" on page 51.
- Install RPMs on the systems and leave the cluster configuration steps for later.

To install VCS RPMs 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 RPMs.
3. Configure the cluster later.
   See "Configuring VCS using configure option" on page 60.

Configuring the cluster

The installer provides you an option to configure VCS and its optional features.

Note: You can use `installvcs -configure` command to configure the cluster later and enter the system names where you want to configure VCS when the installer prompts you.

To configure the cluster

1. Enter **y** or press **Enter** at the prompt to configure VCS.

```
It is optional to configure VCS now. If you choose to configure
VCS later, you can either do so manually or run the
installvcs -configure command.
Are you ready to configure VCS?
[y,n,q] (y) y
```

2. Review the configuration requirements that the installer lists.
3. Enter a unique cluster name and cluster ID.

```
Enter the unique cluster name: [?] vcs_cluster2
Enter the unique Cluster ID number between 0-65535: [b,?] 7
```

4. Review the physical or virtual interfaces that are available on the first system as the installer discovers and reports them.
5. Choose from the virtual or physical interfaces for the private heartbeat links. Note that before you select a virtual interface, make sure that it is mapped to the correct physical interface.

   You must not enter the interface that is used for the public network (typically vswif0.)

```
Enter the NIC for the first private heartbeat NIC on north:
[b,?] vmnic1
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 north:
[b,?] vmnic2
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)
```

6 Choose whether to use the same interface on all nodes.

- If you want to use the same interface for private heartbeat links on all nodes, make sure the same interfaces are available on each system and enter **y**.
- Enter **n** to use interfaces with different device names on some of the nodes.

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

7 Verify and confirm the information that the installer summarizes. For the specified physical interfaces, the installer creates virtual interfaces that are mapped to the physical interfaces.

Adding VCS users

If you have enabled Symantec Product Authentication Service, you do not need to add VCS users now. Proceed to configure the Cluster Management Console cluster connector.

- See "Adding VCS users" on page 52.
- See "Configuring cluster connector" on page 53.

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 cluster connector

If you configured the Cluster Management Console management server to centrally manage this cluster, you can now configure cluster connector. If a firewall exists between the management server and this cluster, then you must configure cluster connector. Make sure you meet the prerequisites to configure cluster connector.

To configure cluster connector

1. Review the information to configure Cluster Management Console.
2. Choose whether to configure cluster connector or not. Do one of the following:
   - To configure cluster connector on the systems, press Enter.

     ```
     Do you want this cluster to be managed by a management
     server? Enter 'y' if you have set up a management server.
     [y,n,q] (y) y
     ```
   - To skip configuring cluster connector and advance to configuring Cluster Management Console for local cluster management, enter **n**.
3. Review the required information to configure cluster connector.
4. Enter the management server network address for the Cluster Management Console.

   ```
   Enter the network address used by the management server [?]
   (north) mgmtserver1.symantecexample.com
   ```
5. Verify and confirm the management server information.
6. Enter the following information that is required to securely communicate with the management server.
   - Password for the service account that is created during the management server installation
   - Hash of the Cluster Management Console management server's root broker
7. Verify and confirm the information.

Configuring the Cluster Management Console

If you want to locally manage this cluster, then you must configure the Cluster Management Console. Note that this cluster can also be a part of the clusters that are centrally managed by the management server.

To configure the Cluster Management Console

1 Choose whether to configure the Cluster Management Console or not. Do one of the following:

- To configure the Cluster Management Console on the systems, press **Enter**.

  ```
  Do you want to configure the Cluster Management Console
  [y,n,q](y)
  ```

- To skip configuring the Cluster Management Console and advance to configuring SMTP, enter **n**.

  See "Configuring SMTP email notification" on page 55.

2 Confirm whether you want to use the discovered public NIC on the first system. Do one of the following:

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

```
Active NIC devices discovered on north: vswif0
Enter the NIC for Cluster Management Console to use on north:
[b,?](vswif0)
```

3 Confirm whether you want to use the same public NIC on all nodes. Do one of the following:

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

```
Is vswif0 to be the public NIC used by all systems [y,n,q,b,?]
(y)
```

4 Enter the virtual IP address for the Cluster Management Console.

```
Enter the Virtual IP address for Cluster Management Console:
[b,?] 10.10.12.1
```

5 Confirm the default netmask or enter another one:

```
Enter the netmask for IP 10.10.12.1: [b,?] (255.255.240.0)
```

6 Verify and confirm the Cluster Management Console information.

```
Cluster Management Console verification:

    NIC: vswif0
    IP: 10.10.12.1
    Netmask: 255.255.240.0

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

Configuring SMTP email notification

You can choose to configure VCS to send event notifications to SMTP e-mail services. You need to provide the SMTP server name and e-mail addresses of people to be notified. Note that it is also possible to configure 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 one of the following:

- To configure SMTP notification, press **Enter**.

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

- To skip configuring SMTP notification and advance to configuring SNMP notification, enter **n**.

  See "Configuring SNMP trap notification" on page 56.

3 Provide information to configure SMTP notification.

- 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 it is also possible to configure 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 one of the following:

- To configure SNMP notification, press **Enter**.

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

- To skip configuring SNMP notification and advance to configuring global clustering option, enter **n**.

  See "Configuring global clusters" on page 57.

3 Provide information to configure SNMP trap notification.

- 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

You can configure global clusters to connect clusters at separate locations and enable wide-area failover and disaster recovery. Note that you must have entered a valid license key for VCS global clusters.

To configure the global cluster option

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

2 Specify whether you want to configure the global cluster option. Do one of the following:

- To configure global cluster option, press **Enter**.

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

- To skip configuring global cluster option and advance to installing VCS RPMs, enter **n**.
  See "Installing the VCS RPMs" on page 58.

3 Provide information to configure the Global Cluster option.
If you configured Cluster Management Console to manage this cluster locally, the installer discovers and displays the virtual IP address and netmask used by the Cluster Management Console. You can use the same virtual IP address and netmask.

Do one of the following:

- If you want to use the default values, press **Enter**.
- If you do not want to use the default value, enter another IP address. The installer prompts you for a NIC and value for the netmask.

```
Enter the Virtual IP address for Global Cluster Option:
[b,?] (10.10.12.1)
```

4 Verify and confirm the configuration of the global cluster.

```
Global Cluster Option configuration verification:

NIC: vswif0
IP: 10.10.12.1
Netmask: 255.255.240.0

Matching Cluster Management Console Virtual IP configuration

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

Installing the 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 58.

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. Review the output as the installer uninstalls any previous versions and installs the VCS 5.0 RPMs.

Creating VCS configuration files

After installing the RPMs, the installer continues to create configuration files and copies them to each system:

```
Creating Cluster Server configuration files ..... Done
Copying configuration files to north..... Done
Copying configuration files to south..... 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 creates security principal or executes the encrypted file to create security principal on each node in the cluster. The installer creates the VxSS service group, creates Authentication

Server credentials on each node in the cluster, and Web credentials for VCS users, and sets up trust with the root broker. Then, the installer proceeds to start VCS in secure mode.

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.

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

Completing the installation

After VCS 5.0 installation completes successfully, the installer creates summary, log, and response files. The files provide useful information that can assist you with the installation and can also assist future installations. Table 4-3 specifies the files created at the end of the installation.

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

Table 4-3 File description

File	Description
summary file	■ Lists RPMs installed on each system. ■ Describes the cluster and its configured resources. ■ Provides information for managing the cluster.
log file	Details the entire installation.
response file	Contains configuration information that can be used to perform secure or unattended installations on other systems. See “Example response file” on page 63.

Copying the Implementation Guide to each node

After you install VCS, Symantec recommends that you copy the PDF version of this guide from the installation disc (cluster_server/docs/vcs_implementation.pdf) to the directory /opt/VRTS/docs on each node to make it available for reference.

Verifying the cluster after installation

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

See "Verifying VCS on ESX Servers" on page 77.

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 entered 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 to 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 cluster" on page 51.

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

Performing VCS installation in a secure environment

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, a "response" file is created.

See "Example response file" on page 63.

Note that a response file generated by the installvcs program contains descriptions and explanations of the variables and their values. By copying this file to the other systems in the cluster and editing 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 48.
2. Review the output as the installer performs the initial system checks.
   The installer detects the inability to communicate between systems.
3. Press Enter 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 north only
   and create a responsefile for systems south? [y,n,q] (y)
   ```
4. Enter all cluster information. Proceed with the installation and configuration tasks.
   See "Installing and configuring VCS 5.0" on page 46.
   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 response file within the file /opt/VRTS/install/logs/installvcs-*universaluniqueidentifier/*installvcs-*universaluniqueidentifier*.response.
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. Using a method of your choice (for example, by using NFS, ftp, or a floppy disk), place a copy of the response file in a directory such as /tmp on the next system to install VCS.
8. On the next system in your cluster, edit the response file.
   For the variables described 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:
   - Mount the product disc.
     See "Preparing your VCS installation and configuration information" on page 39.

- 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 48.

10 Repeat step 7 through step 9 until VCS has been installed on all nodes in the cluster.

Performing automated installations

Using installvcs program with the `-responsefile` option is useful not only for installing and configuring VCS within a secure environment, but 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.

Assuming the systems are set up and meet the requirements for installation, you can perform unattended installation from one of the cluster systems where you have copied the response file.

To perform unattended 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 used in response file

The syntax of Perl statements included in the response file varies, depending on whether "Scalar" or "List" values are required by the variables.

For example,

```
$CFG{Scalar_variable}="value";
```

or, in the case of an integer value:

```
$CFG{Scalar_variable}=123;
```

or, in the case of a list:

```
$CFG(List_variable}=["value", "value", "value"];
```

Example response file

The example response file resembles the file created by installvcs after the example VCS installation. It 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 required for installation.

See Table 4-4, "Response file variables."

```
#
# 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}="758a33dbd6fae751630058ace3dedb54e5
62fe98";
$CPI::CFG{CMC_SERVICE_PASSWORD}="U2FsdGVkX18vE5tn0hTSWwodThACc+
rX";
$CPI::CFG{ENCRYPTED}="U2FsdGVkX1+k2DHKVcnW7b6vrVghdh+zW4G0WFj5I
JA=";
$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}="vswif0";
$CPI::CFG{VCS_CSGVIP}="10.10.12.1";
$CPI::CFG{VCS_LLTLINK1}{east}="vswif1";
$CPI::CFG{VCS_LLTLINK1}{west}="vswif1";
$CPI::CFG{VCS_LLTLINK2}{east}="vswif2";
$CPI::CFG{VCS_LLTLINK2}{west}="vswif2";
$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 4-4 lists the variables used in the response file and their definitions. Note that while some variables are labeled as required and others as optional, some of the optional variables, if used, make it necessary to define other optional variables. For example, all variables related to the cluster service group (CSGNIC, CSGVIP, and CSGNETMASK) must be defined if any are defined. The same is true for the SMTP notification (SMTPSERVER, SMTPRECP, and SMTPRSEV), SNMP trap notification (SNMPPORT, SNMPCONS, and SNMPCSEV), and the Global Cluster Option (CGONIC, GCOVIP, and GCONETMASK).

Table 4-4 Response file variables

Variable	List/ Scalar	Opt'l/ Req'd	Description
$CPI::CFG{OPT}{INSTALL}	Scalar	Req'd	List of systems where VCS must be installed and configured.
$CPI::CFG{OPT}{INSTALLONLY}	Scalar	Opt'l	List of systems where VCS RPMs must be installed. Configuration can be performed at a later time using the `-configure` option.
$CPI::CFG{SYSTEMS}	List	Req'd	List of systems on which the product is to be installed, uninstalled, or configured.
$CPI::CFG{SYSTEMSCFG}	List	Opt'l	List of systems to be recognized in configuration if secure environment prevents all systems from being installed at once.
$CPI::CFG{UPI}	Scalar	Req'd	Defines the product to be installed, uninstalled, or configured.
$CPI::CFG{OPT}{KEYFILE}	Scalar	Opt'l	Defines the location of an ssh keyfile that is used to communicate with all remote systems.
$CPI::CFG{OPT}{LICENSE}	Scalar	Opt'l	Licenses VCS only.

Table 4-4 Response file variables

Variable	List/ Scalar	Opt'l/ Req'd	Description
$CPI::CFG{OPT}{NOLIC}	Scalar	Opt'l	installs the product without any license.
$CPI::CFG{AT_ROOTDOMAIN}	List	Opt'l	Defines the name of the system where the root broker is installed.
$CPI::CFG{OPT}{PKGPATH}	Scalar	Opt'l	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.
$CPI::CFG{OPT}{TMPPATH}	Scalar	Opt'l	Defines the location where a working directory is created to store temporary files and depots needed during the install. The default location is /var/tmp.
$CPI::CFG{OPT}{RSH}	Scalar	Opt'l	Defines that rsh must be used instead of ssh as the communication method between systems.
$CPI::CFG{DONOTINSTALL} {*RPM*}	List	Opt'l	Instructs the installation to not install the optional RPMs designated in the list.
$CPI::CFG{DONOTREMOVE} {*RPM*}	List	Opt'l	Instructs the uninstallation to not remove the optional RPMs designated in the list.
$CPI::CFG{VCS_CLUSTERNAME}	Scalar	Req'd	Defines the name of the cluster.
$CPI::CFG{VCS_CLUSTERID}	Scalar	Req'd	An integer between 0 and 65535 that uniquely identifies the cluster.
$CPI::CFG{KEYS}{*SYSTEM*}	Scalar	Opt'l	List of keys to be registered on the system.

Table 4-4 Response file variables

Variable	List/ Scalar	Opt'l/ Req'd	Description
$CPI::CFG{OPT_LOGPATH}	Scalar	Opt'l	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.
$CPI::CFG{CONFIGURE}	Scalar	Opt'l	Performs configuration if the RPMs are already installed using the `-installonly` option.
$CPI::CFG{VCS_LLTLINK#}{*SYSTEM*}	Scalar	Req'd	Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (LLTLINK1 and LLTLINK2). Up to four LLT links can be configured.
$CPI::CFG{VCS_LLTLINKLOWPRI}{*SYSTEM*}	Scalar	Opt'l	Defines a low priority heartbeat link. Typically, LLTLINKLOWPRI is used on a public network link to provide an additional layer of communication.
$CPI::CFG{VCS_CSGNIC}	Scalar	Opt'l	Defines the NIC for Cluster Management Console to use on a system. 'ALL' can be entered as a system value if the same NIC is used on all systems.
$CPI::CFG{CSGVIP}	Scalar	Opt'l	Defines the virtual IP address to be used by the Cluster Management Console.
$CPI::CFG{VCS_CSGNETMASK}	Scalar	Opt'l	Defines the Netmask of the virtual IP address to be used by the Cluster Management Console.
$CPI::CFG{VCS_SMTPSERVER}	Scalar	Opt'l	Defines the domain-based hostname (example: smtp.symantecexample.com) of the SMTP server to be used for web notification.

Table 4-4 Response file variables

Variable	List/ Scalar	Opt'l/ Req'd	Description
$CPI::CFG{VCS_SMTPRECP}	List	Opt'l	List of full email addresses (example: user@symantecexample.com) of SMTP recipients.
$CPI::CFG{VCS_SMTPRSEV}	List	Opt'l	Defines 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.
$CPI::CFG{VCS_SNMPPORT}	Scalar	Opt'l	Defines the SNMP trap daemon port (default=162).
$CPI::CFG{VCS_SNMPCONS}	List	Opt'l	List of SNMP console system names
$CPI::CFG{VCS_SNMPCSEV}	List	Opt'l	Defines 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.
$CPI::CFG{VCS_GCONIC}{*SYSTEM*}	Scalar	Opt'l	Defines the NIC for the Virtual IP used for the Global Cluster Option. 'ALL' can be entered as a system value if the same NIC is used on all systems.
$CPI::CFG{VCS_GCOVIP}	Scalar	Opt'l	Defines the virtual IP address to be used by the Global Cluster Option.
$CPI::CFG{VCS_GCONETMASK}	Scalar	Opt'l	Defines the Netmask of the virtual IP address to be used by the Global Cluster Option.
$CPI::CFG{VCS_USERENPW}	List	Opt'l	List of encoded passwords for users

Table 4-4 Response file variables

Variable	List/ Scalar	Opt'l/ Req'd	Description
$CPI::CFG{VCS_USERNAME}	List	Opt'l	List of names of users
$CPI::CFG{VCS_USERPRIV}	List	Opt'l	List of privileges for users
$CPI::CFG{OPT}{UNINSTALL}	Scalar	Opt'l	List of systems where VCS must be uninstalled.

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 output to determine:

- 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.

```
License Key                          = xxx-xxx-xxx-xxx-xxx
   Product Name                        = Veritas Cluster Server
   Serial Number                       = 1249
   License Type                        = PERMANENT
   OEM ID                              = 478

 Features :=
   Platform                            = VMware ESX
   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 are using a demo license, you can replace the demo license.

See "Replacing a VCS demo license with a permanent license" on page 69.

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 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.
5. Start VCS on each node:

```
# hastart
```

About installvcs command options

Table 4-5 lists the `installvcs` 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 4-5 installvcs options

Option and Syntax	Description
`-configure`	Configure VCS after using `-installonly` option to install VCS. See "Configuring VCS using configure option" on page 60.
`-enckeyfile` *`encryption_key_file`*	See the `-responsefile` and the `-encrypt` options.
`-encrypt` *`password`*	Encrypt *password* using the encryption key provided with the `-enckeyfile` option so that the encrypted password can be stored in response files.
`-installonly`	Install product RPMs on systems without configuring VCS. See "Installing VCS using installonly option" on page 60.
`-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. **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.
`-nooptionalpkgs`	Specifies that the optional product RPMs such as man pages and documentation need not be installed.

Table 4-5 installvcs options

Option and Syntax	Description
`-nostart`	Bypass starting VCS after completing installation and configuration.
`-pkgpath` *pkg_path*	Specifies that *pkg_path* contains all RPMs to be installed by installvcs program on all systems; *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. Symantec recommends doing a precheck before installing VCS. See "Checking the systems for installation" on page 47.
`-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 system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. If not specified, the response file is automatically generated as installerer*number*.response where *number* is random. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. The `-enckeyfile` option and *encryption_key_file* name are required with the `-responsefile` option when the response file contains encrypted passwords. See "Performing VCS installation in a secure environment" on page 60. See "Performing automated installations" on page 62.
`-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 pre-configured such that rsh commands between systems execute without prompting for passwords or confirmations. **Note:** Note that rsh is not a part of the VCS for VMware ESX installation.

Table 4-5 installvcs options

Option and Syntax	Description
`-tmppath tmp_path`	Specifies that *tmp_path*, not /var/tmp, is the working directory for installvcs program. This destination is where initial logging is performed and where RPMs are copied on remote systems before installation.

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 RPM 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 removing it.

Prerequisites

- Before removing VCS from any node in the cluster, you must shut down applications such as the Console or any VCS enterprise agents that depend on VCS.
- Before removing VCS from fewer than all nodes in a cluster, make sure that no service groups are running on the nodes from which VCS is uninstalled. You must also reconfigure VCS on the remaining nodes.
  See "Adding and removing cluster nodes" on page 93.

Uninstalling VCS 5.0

The example demonstrates how to uninstall VCS on two nodes: north and south.

Removing VCS 5.0 RPMs

The program stops the VCS processes that are currently running during the uninstallation process.

To uninstall VCS

1. Do one of the following to begin uninstalling:
   - If you can execute commands as superuser on the remote nodes in the cluster using `ssh` without supplying a password, run uninstallvcs program on one node to uninstall VCS on all nodes in the cluster.

- If you cannot execute commands as superuser on remote nodes in the cluster using ssh, you must run uninstallvcs program on each node in the cluster.

2 Start uninstallvcs program.

```
# cd /opt/VRTS/install
# ./uninstallvcs
```

The program specifies the directory where the logs are created and displays a copyright notice followed by 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: north south
    Service Groups: ClusterService groupA groupB
```

3 Answer the prompt to proceed with uninstalling the software.

- To uninstall VCS on all nodes, press **Enter**.
- To uninstall VCS only on specific nodes, enter **n**.
  Note that if you enter **n** or if no VCS configuration files are found on the local node, the uninstallvcs program prompts you to enter a list of nodes from which you want to uninstall VCS.

  ```
  Do you want to uninstall VCS from these systems? [y,n,q] (y)
  ```

4 Review the output as the uninstallvcs program continues to verify communication between systems and check the installations on each system to determine the RPMs to be uninstalled.

5 If RPMs, such as enterprise agents, are found to be dependent on a VCS RPM, the uninstaller prompts you on whether you want them removed. Enter **y** to remove the designated RPMs.

6 Review the uninstaller report after the verification.

7 Press Enter to uninstall the VCS RPMs.

```
Are you sure you want to uninstall VCS rpms? [y,n,q] (y)
```

8 Review the output as the uninstaller stops processes, unloads kernel modules, and removes the RPMs.

9 Note the location of summary and log files that the uninstaller creates after removing all the RPMs.

Running uninstallvcs from the VCS 5.0 disc

If you need to uninstall VCS after an incomplete installation, or if the uninstallvcs program is not available in /opt/VRTS/install, you may need to use the uninstallvcs program on the VCS 5.0 disc.

Uninstalling the Cluster Management Console cluster connector

Perform the following procedure to remove the cluster connector from UNIX or Windows systems.

Uninstalling cluster connector from UNIX systems

Use this procedure to remove the Cluster Management Console cluster connector from each cluster.

On UNIX systems, the default installer option is -ssh. If you are performing a remote uninstallation and ssh is not enabled, run the installer program with the -rsh option. Otherwise, the installer generates an error during the uninstallation.

To uninstall cluster connector from UNIX systems

1. Insert the product disc into the drive on the local system. At the command prompt, type the following command to run the installer program:
   `./installer [-rsh]`
   The installer program presents copyright information followed by a menu titled, “Storage Foundation and High Availability Solutions 5.0”.
2. Enter **u** to specify uninstallation.
   `Enter a Task: [I,C,L,P,U,D,Q,?]` **`u`**
   The installer program displays another menu that lists products that are available for uninstallation.
3. Enter the menu number that corresponds to Veritas Cluster Management Console.
   `Select a product to uninstall:`***`nn`***
   The installer program presents a description of the product.
4. Enter **2** if you are prompted to select a product component. Otherwise, proceed to step 6.
   `Enter '1' to install the Management Server, '2' to install the Cluster Connector: [1-2,q] (1)` **`2`**
   The installer program presents a message stating that it will uninstall cluster connector.
5. The uninstall program prompts you for the name of at least one node in the cluster.
   `Enter one system name from each cluster separated by spaces from which to uninstall CMC:` ***`sysA`***
   Based on this, it determines the nodes from which to uninstall and perform the necessary checks.

Note: If you get an error message similar to this:

```
Checking ssh communication with sysA Enter passphrase for key
'/.ssh/id_dsa'
```

You must return and set up ssh.

6 Enter **y** to verify that the information up to this point is correct.

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

The installer program performs an initial system check of the cluster nodes and checks for installed packages on the cluster nodes. If these checks are satisfactory, the installer program lists the packages to be uninstalled.

7 Enter **y** to verify that you want to uninstall cluster connector.

```
Are you sure you want to uninstall CMC? [y,n,q] (y)
```

The installer program lists package dependencies and uninstallation progress percentages. If the uninstallation is successful, the installer program displays this message followed by the location of the uninstallation logs:

```
Uninstall completed successfully
```

Chapter 5

Verifying VCS on ESX Servers

This chapter contains the following topics:

About verifying the VCS installation

After successful installation, you can inspect the contents of the key configuration files that you have installed and modified during the process. These files reflect the configuration based on the information you supplied.

Verifying 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.

/etc/llthosts

The file `llthosts(4)` is a database, containing one entry per system, that 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 entries that resemble:

```
0   north
1   south
```

/etc/llttab

The file `lltab(1M)` contains 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 entries that resemble:

```
set-node north
set-cluster 2
link link1 vswif1 vswif1 - ether - -
link link2 vswif2 vswif2 - ether - -
```

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

```
set-node north
set-cluster 2
link vswif1 eth-00:04:23:AC:12:C4 - ether - -
link vswif2 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, beginning with the `link` command, identify the two network cards used by the LLT protocol.

Refer to the `lltab(4)` manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the `lltab` file.

/etc/gabtab

After you install VCS, the file /etc/gabtab contains a `gabconfig(1)` command that configures the GAB driver for use.

The file /etc/gabtab contains a line that resembles:

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

where the `-c` option configures the driver for use and `-nN` specifies that the cluster is not formed until at least *N* nodes are ready to form the cluster. By default, *N* is the number of nodes in the cluster.

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

Verifying the main.cf file

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

- See "Example main.cf, for clusters without the GCO option" on page 80.
- See "Example main.cf, for clusters with the GCO option" on page 87.

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 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 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 and includes the following:

- The ClusterService service group includes the IP, NIC, and VRTSWebApp resources.
- If you configured Cluster Management Console to manage this cluster locally, the main.cf includes the VRTSWebApp resource that includes AppName = cmc attribute.
- If you configured Cluster Connector so that Cluster Management Console can centrally manage this cluster, the main.cf includes the CMC service group.

The CMC service group includes the ClusterConnectorConfig and Process resources.

- The service group also includes the notifier resource configuration, which is based on your input to installvcs program prompts about notification.
- The installvcs program also creates a resource dependency tree.
- If you installed VCS with the Global Cluster Option, the ClusterService service group contains an Application resource, wac (wide-area connector), whose attributes contain definitions for controlling the cluster in a Global Cluster environment.

  For for information about managing VCS global clusters:

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

Refer to the *Veritas Cluster Server User's Guide* and review the chapter on configuration concepts for descriptions and examples of main.cf and types.cf files for ESX systems.

Example main.cf, for clusters without the GCO option

The following sample main.cf is for a cluster. This example is a stub for nine virtual machine service groups, all that is needed is to add applications.

```
Main.cf:

include "types.cf"

cluster vcs (
        UserNames = { admin = IpqIpkPmqLqqOyqKpn }
        Administrators = { admin }
        )

system sysA (
        )

system sysB (
        )
```

```
group vm2 (
        SystemList = { sysA = 0, sysB = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm2_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm2/vm2.v
mx"
                VCserver = "648G771.example.com"
                username = v023968
                password = 123123123
                sslcert = "/etc/my.keystore"
                esxhostdomain = "veritas.com"
                )

        VMFSVolume vm2_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm2_switch (
                VirtualSwitch = vSwitch0
                )

        vm2_ESX requires vm2_vmfs
        vm2_vmfs requires vm2_switch


        // resource dependency tree
        //
        //      group vm2
        //      {
        //      ESXVirtualMachine vm2_ESX
        //          {
        //          VMFSVolume vm2_vmfs
        //              {
        //              VSwitch vm2_switch
        //              }
        //          }
        //      }group vm3 (
        SystemList = { sysA = 0, sysB = 1 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm3_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm3/vm3.v
mx"
                VCserver = "648G771.example.com"
                username = v023968
```

```
                password = 123123123
                sslcert = "/etc/my.keystore"
                esxhostdomain = "veritas.com"
                )

        VMFSVolume vm3_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm3_switch (
                VirtualSwitch = vSwitch0
                )

        vm3_ESX requires vm3_vmfs
        vm3_vmfs requires vm3_switch


        // resource dependency tree
        //
        //      group vm3
        //      {
        //      ESXVirtualMachine vm3_ESX
        //          {
        //          VMFSVolume vm3_vmfs
        //              {
        //              VSwitch vm3_switch
        //              }
        //          }
        //      }

group vm4 (
        SystemList = { sysA = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm4_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm4/vm4.v
mx"
                )

        VMFSVolume vm4_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm4_switch (
                VirtualSwitch = vSwitch0
                )
```

```
        vm4_ESX requires vm4_vmfs
        vm4_vmfs requires vm4_switch


        // resource dependency tree
        //
        //      group vm4
        //      {
        //      ESXVirtualMachine vm4_ESX
        //          {
        //          VMFSVolume vm4_vmfs
        //              {
        //              VSwitch vm4_switch
        //              }
        //          }
        //      }


group vm5 (
        SystemList = { sysA = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm5_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm5/vm5.v
mx"
                )

        VMFSVolume vm5_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm5_switch (
                VirtualSwitch = vSwitch0
                )

        vm5_ESX requires vm5_vmfs
        vm5_vmfs requires vm5_switch


        // resource dependency tree
        //
        //      group vm5
        //      {
        //      ESXVirtualMachine vm5_ESX
        //          {
        //          VMFSVolume vm5_vmfs
        //              {
```

```
        //              VSwitch vm5_switch
        //              }
        //          }
        //      }


group vm6 (
        SystemList = { sysA = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm6_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm6/vm6.v
mx"
                )

        VMFSVolume vm6_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm6_switch (
                VirtualSwitch = vSwitch0
                )

        vm6_ESX requires vm6_vmfs
        vm6_vmfs requires vm6_switch


        // resource dependency tree
        //
        //      group vm6
        //      {
        //      ESXVirtualMachine vm6_ESX
        //          {
        //          VMFSVolume vm6_vmfs
        //              {
        //              VSwitch vm6_switch
        //              }
        //          }
        //      }

group vm7 (
        SystemList = { sysA = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm7_ESX (
```

```
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm7/vm7.v
mx"
                )

        VMFSVolume vm7_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm7_switch (
                VirtualSwitch = vSwitch0
                )

        vm7_ESX requires vm7_vmfs
        vm7_vmfs requires vm7_switch


        // resource dependency tree
        //
        //      group vm7
        //      {
        //      ESXVirtualMachine vm7_ESX
        //          {
        //          VMFSVolume vm7_vmfs
        //              {
        //              VSwitch vm7_switch
        //              }
        //          }
        //      }


group vm8 (
        SystemList = { sysA = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm8_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm8/vm8.v
mx"
                )

        VMFSVolume vm8_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm8_switch (
                VirtualSwitch = vSwitch0
```

```
                )

        vm8_ESX requires vm8_vmfs
        vm8_vmfs requires vm8_switch


        // resource dependency tree

        //
        //      group vm8
        //      {
        //      ESXVirtualMachine vm8_ESX
        //          {
        //          VMFSVolume vm8_vmfs
        //              {
        //              VSwitch vm8_switch
        //              }
        //          }
        //      }


group vm9 (
        SystemList = { sysA = 0 }
        AutoStartList = { sysA }
        )

        ESXVirtualMachine vm9_ESX (
                CfgFile =
"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm9/vm9.v
mx"
                )

        VMFSVolume vm9_vmfs (
                Volume = {

"/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b" }
                )

        VSwitch vm9_switch (
                VirtualSwitch = vSwitch0
                )

        vm9_ESX requires vm9_vmfs
        vm9_vmfs requires vm9_switch


        // resource dependency tree
        //
        //      group vm9
        //      {
        //      ESXVirtualMachine vm9_ESX
        //          {
```

```
//           VMFSVolume vm9_vmfs
//               {
//               VSwitch vm9_switch
//               }
//           }
//       }
```

Example main.cf, for clusters with the GCO option

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

```
.
.
group ClusterService (
    SystemList = { north = 0, south = 1 }
    UserStrGlobal = "LocalCluster@https://10.182.2.78:8443;"
    AutoStartList = { north, south }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

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

Verifying LLT, GAB, and cluster operation

Before attempting to verify the operation of LLT, GAB, or the cluster, you must:

- Log in to any node in the cluster as superuser.
- Place the VCS command directory in your `PATH` variable:

  `# export PATH=$PATH:/sbin:/usr/sbin:/opt/VRTS/bin`

Verifying LLT

Use the `lltstat` command to verify that links are active for LLT. This command 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.

Using lltstat -n

In the following example, `lltstat -n` is typed on each node in the cluster:

Node 1

```
# lltstat -n
```

Output resembles:

```
LLT node information:
    Node           State      Links
    *0 north       OPEN       2
     1 south       OPEN       2
```

Node 2

```
# lltstat -n
```

Output resembles:

```
LLT node information:
    Node           State      Links
     0 north       OPEN       2
    *1 south       OPEN       2
```

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

Using lltstat -nvv

With LLT configured correctly, the output of `lltstat -n` shows all the nodes in the cluster and two links for each node. If the output shows otherwise, you can use the verbose option of `lltstat`.

For example, type `lltstat -nvv | more` on a node to view additional information about LLT. In the following example, `lltstat -nvv | more` is typed on node north in a two-node cluster:

```
# lltstat -nvv | more
```

Output resembles:

```
Node        State       Link    Status     Address
*0 north    OPEN
                        link1 UP       08:00:20:93:0E:34
                        link2 UP       08:00:20:93:0E:34
1 south     OPEN
                        link1 UP       08:00:20:8F:D1:F2
                        link2 DOWN
2           CONNWAIT
                        link1   DOWN
                        link2   DOWN
3           CONNWAIT
                        link1   DOWN
                        link2   DOWN
.
.
```

```
.

31          CONNWAIT
                        link1    DOWN
                        link2    DOWN
```

Note that the output lists 32 nodes. It reports on the two nodes in the cluster, north and south, plus non-existent nodes. For each correctly configured node, the information should show a state of OPEN, a status for each link of UP, and an address for each link. However, the output in the example shows that for the node south the private network connection is possibly broken or the information in the /etc/llttab file may be incorrect.

To obtain information about the ports open for LLT, type `lltstat -p` on any node. In the following example, `lltstat -p` is typed on one node in a two-node cluster:

Node 1

```
# lltstat -p
```

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

To verify that GAB is operating, type the following command on each node:

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

If GAB is operating, the following GAB port membership information is returned:

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

Port a indicates that GAB is communicating, gen a36e0003 is a randomly generated number, and membership 01 indicates that nodes 0 and 1 are connected.

Port h indicates that VCS is started, gen fd570002 is a randomly generated number, and membership 01 indicates that nodes 0 and 1 are both running VCS.

If GAB is not operating, 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
```

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

Verifying the cluster

To verify that the cluster is operating, type the following command:

```
# hastatus -summary
```

The output resembles:

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

A  north                RUNNING            0
A  south                RUNNING            0

-- GROUP STATE
-- Group           System     Probed  AutoDisabled   State

B  ClusterService  north      Y       N              ONLINE
B  ClusterService  south      Y       N              OFFLINE
```

Note the system state. If the value is RUNNING, VCS is successfully installed and running. The group state lists the ClusterService group, which is ONLINE on north and OFFLINE on south. Refer to the `hastatus(1M)` manual page. In the *Veritas Cluster Server User's Guide*, look for a description of system states and the transitions between them.

hasys -display

On one of the nodes, use the `hasys(1M)` command:

```
# /opt/VRTSvcs/bin/hasys -display
```

On each node, the output should be similar. For more information on the `hasys -display` command, refer to the `hasys(1M)` manual page. Also refer to the *Veritas Cluster Server User's Guide* for information about administering VCS from the command-line.

The example shows the output when the `hasys -display` command is run on the node north; the list continues with similar information for south (not shown) and any other nodes in the cluster:

```
#System  Attribute          Value

north    AgentsStopped      0

north    AvailableCapacity  100

north    CPUUsage           0

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

north    Capacity           100

north    ConfigBlockCount   142

north    ConfigCheckSum     4085

north    ConfigDiskState    CURRENT

north    ConfigFile         /etc/VRTSvcs/conf/config

north    ConfigInfoCnt      0

north    ConfigModDate      Fri May 26 17:22:48 2006

north    ConnectorState     Down

north    CurrentLimits

north    DiskHbStatus

north    DynamicLoad        0

north    EngineRestarted    0

north    EngineVersion      5.0.00.0

north    Frozen             0

north    GUIIPAddr

north    LLTNodeId          0

north    LicenseType        DEMO

north    Limits

north    LinkHbStatus       vswif1 UP vswif2 UP
```

```
north    LoadTimeCounter    0
north    LoadTimeThreshold  600
north    LoadWarningLevel   80
north    NoAutoDisable      0
north    NodeId             0
north    OnGrpCnt           1
north    ShutdownTimeout    120
north    SourceFile         ./main.cf
north    SysInfo            Linux:north,#1 Fri Apr 22 18:13:58 EDT
                            2005,2.6.9-34-default,i686
north    SysName            north
north    SysState           RUNNING
north    SystemLocation
north    SystemOwner
north    TFrozen            0
north    TRSE               0
north    UpDownState        Up
north    UserInt            0
north    UserStr
north    VCSFeatures        DR
north    VCSMode            VCS
```

Accessing the VCS documentation

If you had chosen to install the optional RPM VRTSvcsdc, then the directory /opt/VRTS/docs contains the documentation for VCS in Portable Document Format (PDF). The directory contains the following documents:

- vcs_users.pdf, *Veritas Cluster Server User's Guide*
- vcs_bundled_agents.pdf, *Veritas Cluster Server Bundled Agents Reference Guide*
- vcs_agent_dev.pdf, *Veritas Cluster Server Agent Developer's Guide*

Chapter 6

Adding and removing cluster nodes

This chapter contains the following topics:

About adding and removing nodes

After installing VCS and creating a cluster, you can add and remove nodes from the cluster. You can create a clusters 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.

See "Planning to install VCS on an ESX Server" on page 31.

Table 6-1 specifies the tasks involved in adding a cluster. The example demonstrates how to add a node east to already existing nodes, north and south.

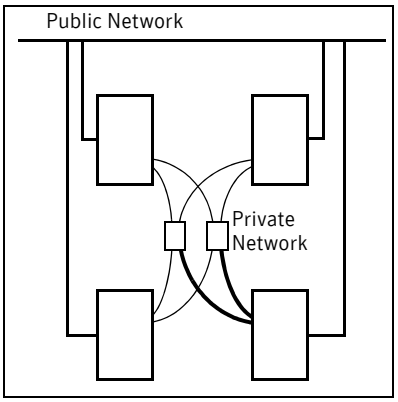
Table 6-1 Tasks involved in adding a node to a cluster

Task	Reference
Set up the hardware.	"Setting up the hardware" on page 94
Install the software manually.	"Installing VCS software manually" on page 119
Add a license key.	"Adding a license key" on page 96
Configure LLT and GAB.	"Configuring LLT and GAB" on page 97
Add the node to the existing cluster.	"Adding the node to the existing cluster" on page 99
Start VCS and verify the cluster.	"Starting VCS and verifying the cluster" on page 99

Setting up the hardware

Before configuring a new system to an existing cluster, you must physically add the system to the cluster.

Figure 6-1 Adding a node to a three-node cluster using two independent hubs



To set up the hardware

1 Connect the VCS private Ethernet controllers.

- If you are expanding from a two-node cluster, you need to use independent hubs for the private network connections, replacing crossover cables if they are used.
- If you already use independent hubs, connect the two Ethernet controllers on the new node to the independent hubs.

Figure 6-1 illustrates a new node being added to an existing three-node cluster using two independent hubs.

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

Preparing for a manual installation

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

To prepare for installation

- Depending on the OS distribution, replace the dist in the command with rhel4 or sles9. Depending on the architecture, replace the arch in the command with i686, i586, or x86_64. Type the command:

  ```
  # 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 selecting the optional RPMs, note:

- Symantec recommends that you install the RPMs for VCS manual pages (VRTSvcsmn) and VCS documentation (VRTSvcsdc). Install the documentation RPM on nodes where you want access to the documentation.
- The VCS configuration wizard (VRTScscw) RPM includes wizards for the installation and configuration of Veritas products that require VCS configuration.

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

To install VCS RPMs on a node

1 Install the required VCS RPMs in the order shown. Do not install any RPMs already installed on the system.

```
# VRTSatClient-4.3.26.9-9.i386.rpm
# VRTSatServer-4.3.26.9-9.i386.rpm
# VRTSperl-5.0.2.1-linux.i386.rpm
# VRTSspt-5.0.00.2-GA.noarch.rpm
# VRTSvlic-3.02.18.0-0.i686.rpm
# VRTSllt-5.0.10.00-GA_ESX30.i686.rpm
# VRTSgab-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcs-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsmg-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSvcsag-5.0.10.00-GA_ESX30.i686.rpm
# VRTSjre-1.4-GA1.i386.rpm
# VRTSjre15-1.5-GA3.i386.rpm
# VRTSweb-5.0.1-GA4_GENERIC.noarch.rpm
# VRTSvcsmn-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSvcsdc-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTScssim-5.0.10.00-GA_ESX30.i686.rpm
# VRTScmcs-5.0.00.00-GA_ESX.i686.rpm
# VRTScmccc-5.0.00.00-GA_ESX.i686.rpm
# VRTSvcsdns-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsm-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsvmip-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsvisdk-5.0.10.00-GA_ESX30.i686.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.

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 are adding east to a cluster consisting of north and south:

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

     ```
     0 north
     1 south
     ```

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

     ```
     0 north
     1 south
     2 east
     ```

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.

   See "/etc/llttab" on page 186.

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

   ```
   set-node east
   set-cluster 2
   link vswif1 vswif1 - ether - -
   link vswif2 vswif2 - 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
  ```
  then the file on the new node should be the same, although it is recommended to 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
  ```
  then, 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
  ```
  See "/etc/gabtab" on page 186.
  The `-n` flag indicates to VCS the number of nodes required to 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 195.

2 Run the same command on the other nodes (north and south) 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 east
   ```
3. Stop VCS on the new node:
   ```
   # hastop -sys east
   ```
4. Copy the main.cf file from an existing node to your new node:
   ```
   # scp /etc/VRTSvcs/conf/config/main.cf
   east:/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 6-2 specifies the tasks involved in removing a node from a cluster. In the example procedure, the cluster consists of nodes A, B, and C; node C is to leave the cluster.

Table 6-2 Tasks involved in removing a node

Task	Reference
■ Back up the configuration file. ■ Check the status of the nodes and the service groups.	"Verify the status of nodes and service groups" on page 100
■ Switch or remove any VCS service groups on the node departing the cluster. ■ Delete the node from VCS configuration.	"Deleting the departing node from VCS configuration" on page 101
Modify the llthosts and gabtab files to reflect the change.	"Modifying configuration files on each remaining node" on page 103
On the node departing the cluster: ■ Modify startup scripts for LLT, GAB, and VCS to allow reboot of the node without affecting the cluster. ■ Unconfigure and unload the LLT and GAB utilities. ■ Remove the VCS RPMs.	"Unloading LLT and GAB and removing VCS on the departing node" on page 103

Verify the status of nodes and service groups

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

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  A           RUNNING        0
A  B           RUNNING        0
A  C           RUNNING        0
```

```
-- GROUP STATE
-- Group    System      Probed   AutoDisabled   State
B  grp1     A           Y        N              ONLINE
B  grp1     B           Y        N              OFFLINE
B  grp2     A           Y        N              ONLINE
B  grp3     B           Y        N              OFFLINE
B  grp3     C           Y        N              ONLINE
B  grp4     C           Y        N              ONLINE
```

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

Deleting the departing node from VCS configuration

Before removing a node from the cluster, you must remove or switch from the departing node the service groups on which other service groups depend.

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 C to node B.

   ```
   # hagrp -switch grp3 -to B
   ```

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, that is, if it is a parent to service groups on other nodes, then 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 C
   ```

5. Check the status again. The state of the departing node should be EXITED. Also, any service groups set up for failover should be online on other nodes:

   ```
   # hastatus -summary
   ```

   ```
   -- SYSTEM STATE
   -- System      State          Frozen
   A  A           RUNNING        0
   A  B           RUNNING        0
   A  C           EXITED         0
   ```

```
-- GROUP STATE
-- Group    System      Probed   AutoDisabled   State
B  grp1     A           Y        N              ONLINE
B  grp1     B           Y        N              OFFLINE
B  grp2     A           Y        N              ONLINE
B  grp3     B           Y        N              ONLINE
B  grp3     C           Y        Y              OFFLINE
B  grp4     C           Y        N              OFFLINE
```

6 Delete the departing node from the SystemList of service groups grp3 and grp4.

```
# hagrp -modify grp3 SystemList -delete C
# hagrp -modify grp4 SystemList -delete C
```

7 For service groups that run only on the departing node, delete the resources from the group before deleting the group.

```
# hagrp -resources grp4
   processx_grp4
   processy_grp4
# hares -delete processx_grp4
# hares -delete processy_grp4
```

8 Delete the service group configured to run on the departing node.

```
# hagrp -delete grp4
```

9 Check the status.

```
# hastatus -summary
   -- SYSTEM STATE
   -- System      State          Frozen
   A  A           RUNNING        0
   A  B           RUNNING        0
   A  C           EXITED         0

   -- GROUP STATE
   -- Group    System      Probed   AutoDisabled   State
   B  grp1     A           Y        N              ONLINE
   B  grp1     B           Y        N              OFFLINE
   B  grp2     A           Y        N              ONLINE
   B  grp3     B           Y        N              ONLINE
```

10 Delete the node from the cluster.

```
# hasys -delete C
```

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`, although 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, then make sure that *N* is not greater than the actual number of nodes in the cluster, or GAB does not automatically seed.

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

2. Modify /etc/llthosts file on each remaining nodes to remove the entry of the departing node.
   For example, change:

   ```
   0 A
   1 B
   2 C
   ```

   to:

   ```
   0 A
   1 B
   ```

Unloading LLT and GAB and removing VCS on the departing node

Perform the tasks on the node departing the cluster.

To stop LLT and GAB and remove VCS

1. Stop GAB and LLT:

   ```
   # /etc/init.d/gab stop
   # /etc/init.d/llt stop
   ```

2. To determine the RPMs to remove, enter:

   ```
   # rpm -qa | grep VRTS
   ```

3. To permanently remove the VCS RPMs from the system, use the `rpm -e` command. Pay special attention to operating system distribution and architecture. Remove the following RPMs in the order shown:

   ```
   # VRTSvcsvisdk-5.0.10.00-GA_ESX30.i686.rpm
   # VRTSvcsvmip-5.0.10.00-GA_ESX30.i686.rpm
   ```

```
# VRTSvcsm-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsdns-5.0.10.00-GA_ESX30.i686.rpm
# VRTScmccc-5.0.00.00-GA_ESX.i686.rpm
# VRTScmcs-5.0.00.00-GA_ESX.i686.rpm
# VRTScssim-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsdc-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSvcsmn-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSweb-5.0.1-GA4_GENERIC.noarch.rpm
# VRTSjre15-1.5-GA3.i386.rpm
# VRTSjre-1.4-GA1.i386.rpm
# VRTSvcsag-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsmg-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSvcs-5.0.10.00-GA_ESX30.i686.rpm
# VRTSgab-5.0.10.00-GA_ESX30.i686.rpm
# VRTSllt-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvlic-3.02.18.0-0.i686.rpm
# VRTSspt-5.0.00.2-GA.noarch.rpm
# VRTSperl-5.0.2.1-linux.i386.rpm
# VRTSatServer-4.3.26.9-9.i386.rpm
# VRTSatClient-4.3.26.9-9.i386.rpm
```

4 Remove the LLT and GAB configuration files.

```
# rm /etc/lltab
# rm /etc/gabtab
# rm /etc/llthosts
```

Chapter 7

Installing VCS on a single node

This chapter contains the following topics:

About installing VCS on a single node

You can install VCS 5.0 on a single node. You can subsequently add another node to the single-node cluster to form a multiple-node 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 106.

See "Creating a single-node cluster manually" on page 107.

Creating a single-node cluster using the installer program

Table 7-1 specifies the tasks involved in installing VCS on a single node using the installer program.

Table 7-1 Tasks to create a single-node cluster using the installer

Task	Reference
Prepare for installation.	"Preparing for a single node installation" on page 106
Install the VCS software on the system using the installer.	"Starting the installer for the single node cluster" on page 107

Preparing for a single node installation

You can use the installer program to install a cluster on a single system for two purposes:

- To prepare the single node cluster to join a larger cluster
- To prepare the single node cluster to be a standalone single node cluster

When you prepare it to join a larger cluster, install it with LLT and GAB. For a standalone cluster, you do not need to enable LLT and GAB.

For more information about LLT and GAB:

See "LLT and GAB" on page 17.

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 See "Starting the software installation" on page 48.

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,?] (n)
```

Answer **n** if you want to use the single node cluster as a standalone 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 49.

Creating a single-node cluster manually

Table 7-2 specifies the tasks involved in installing VCS on a single node.

Table 7-2 Tasks to create a single-node cluster manually

Task	Reference
Set the PATH variable	"Setting the PATH variable" on page 108
Install the VCS software manually and add a license key	"Installing VCS RPMs for a manual installation" on page 108 "Adding a license key" on page 109
Remove any LLT or GAB configuration files and rename LLT and GAB startup files. A single-node cluster does not require the node-to-node communication service, LLT, or the membership communication service, GAB.	"Renaming the LLT and GAB startup files" on page 109

Table 7-2 Tasks to create a single-node cluster manually

Task	Reference
Modify the VCS startup file for single-node operation.	"Modifying the startup files" on page 110
Create and modify the VCS configuration files.	"Configuring VCS" on page 110
Start VCS and verify single-node operation.	"Verifying single-node operation" on page 111

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
    ```

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 selecting the optional RPMs, note:

- Symantec recommends that you install the RPMs for VCS manual pages (VRTSvcsmn) and VCS documentation (VRTSvcsdc). Install the documentation RPM on nodes where you want access to the documentation.
- The VCS configuration wizard (VRTScscw) RPM includes wizards for the installation and configuration of Veritas products that require VCS configuration.

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

To install VCS RPMs on a node

1 Install the required VCS RPMs in the order shown. Do not install any RPMs already installed on the system.

```
# VRTSatClient-4.3.26.9-9.i386.rpm
# VRTSatServer-4.3.26.9-9.i386.rpm
# VRTSperl-5.0.2.1-linux.i386.rpm
# VRTSspt-5.0.00.2-GA.noarch.rpm
# VRTSvlic-3.02.18.0-0.i686.rpm
# VRTSllt-5.0.10.00-GA_ESX30.i686.rpm
# VRTSgab-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcs-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsmg-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSvcsag-5.0.10.00-GA_ESX30.i686.rpm
# VRTSjre-1.4-GA1.i386.rpm
# VRTSjre15-1.5-GA3.i386.rpm
# VRTSweb-5.0.1-GA4_GENERIC.noarch.rpm
# VRTSvcsmn-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTSvcsdc-5.0.10.00-GA_GENERIC.noarch.rpm
# VRTScssim-5.0.10.00-GA_ESX30.i686.rpm
# VRTScmcs-5.0.00.00-GA_ESX.i686.rpm
# VRTScmccc-5.0.00.00-GA_ESX.i686.rpm
# VRTSvcsdns-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsm-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsvmip-5.0.10.00-GA_ESX30.i686.rpm
# VRTSvcsvisdk-5.0.10.00-GA_ESX30.i686.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.

Renaming the LLT and GAB startup files

You may need the LLT and GAB startup files if you need 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
```

Configuring VCS

VCS configuration requires the types.cf and main.cf files on each system in the cluster. Both of the files are in the /etc/VRTSvcs/conf/config directory.

main.cf file

The main.cf configuration file requires the following minimum essential elements:

- An “include” statement that specifies the file, types.cf, which defines the VCS bundled agent resources.
- The name of the cluster.
- The name of the systems that make up the cluster.

Editing the main.cf file

When you manually install VCS, the file /etc/VRTSvcs/conf/config/main.cf contains only the line:

```
include "types.cf"
```

To edit the main.cf file

1. Log in as superuser, and move to the directory containing the configuration file:

   ```
   # cd /etc/VRTSvcs/conf/config
   ```

2. Using vi, or another text editor, edit the main.cf file, defining your cluster name and system names. Refer to the following example.

3. Save and close the file.

Refer to the *Veritas Cluster Server User's Guide* for a full description of the main.cf file, how to edit it and verify it.

Example, main.cf

An example main.cf for a two-node cluster:

```
include "types.cf"
cluster VCSCluster2 ( )
system north
system south
```

An example main.cf for a single-node cluster:

```
include "types.cf"
cluster VCSCluster1 ( )
system sn1
```

types.cf file

Note that the "include" statement in main.cf refers to a file named types.cf. This text file describes the VCS bundled agent resources. During new installations, the types.cf file is automatically copied in to the /etc/VRTSvcs/conf/config directory.

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`(1M) 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

Table 7-3 specifies the activities involved in adding nodes 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 and the node that is to join Node A to form a multiple-node cluster as Node B.

Table 7-3 Tasks to add a node to a single-node cluster

Task	Reference
Set up Node B to be compatible with Node A	"Setting up a node to join the single-node cluster" on page 112
■ Add Ethernet cards for private heartbeat network for Node B ■ If necessary, add Ethernet cards for private heartbeat network for Node A ■ Make the Ethernet cable connections between the two nodes	"Installing and configuring Ethernet cards for private network" on page 113
Connect both nodes to shared storage	"Configuring the shared storage" on page 114
■ Bring up VCS on Node A ■ Edit the configuration file ■ Edit the startup scripts	"Bringing up the existing node" on page 114
If necessary, install VCS on Node B and add a license key. Make sure Node B is running the same version of VCS as the version on Node A.	"Installing VCS RPMs for a manual installation" on page 108 "Adding a license key" on page 109
Edit the configuration files on Node B	"Configuring LLT and GAB" on page 115
Start LLT and GAB on Node B	"Starting LLT and GAB" on page 117
■ Start LLT and GAB on Node A ■ Restart VCS on Node A ■ Modify service groups for two nodes	"Reconfiguring VCS on the existing node" on page 117
■ Start VCS on Node B ■ Verify the two-node cluster	"Verifying configuration on both nodes" on page 118

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:

- 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 removing the node from the cluster, remove the VCS RPMs and configuration files.
  See "Removing a node from a cluster" on page 100.
- If the node you plan to add as Node B is also currently a single VCS node, uninstall VCS.
  See "Uninstalling VCS 5.0" on page 72.
- If you renamed the LLT and GAB startup files, remove them.
  See "Renaming the LLT and GAB startup files" on page 109.

2 If necessary, install VxVM and VxFS.
See "Installing VxVM, VxFS if necessary" on page 113.

Installing VxVM, VxFS if necessary

If VxVM with the cluster option or VxFS with the cluster option is installed on the existing node in the cluster, then the same versions must also be installed on the new node.

Refer to the appropriate documentation for VxVM and VxFS to verify the versions of the installed products and make sure the same version is running on all nodes that are to use any 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, two separate NICs on each node should be used, such that the failure of one NIC does not restrict heartbeating between the nodes.

See "Setting up the private network" on page 35.

To install and configure ethernet cards for private network

1 Shut down VCS on Node A.

```
# hastop -local
```

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

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

3 Install the ethernet card on Node A.

4 Install the ethernet card on Node B.

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 "Enabling communication between systems" on page 37.

Bringing up the existing 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 listed 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 RPMs and license key

Install the VCS 5.0 RPMs manually and install the license key.

See "Installing VCS RPMs for a manual installation" on page 108.

See "Adding a license key" on page 109.

Configuring LLT and GAB

VCS uses LLT and GAB to replace the functions of TCP/IP for VCS private network communications. LLT and GAB provide the performance and reliability required by VCS for these and other functions.

LLT and GAB must be configured as described in the following sections.

Configuring low latency transport (LLT)

To configure LLT, set up two files: /etc/llthosts and /etc/lltab on each node in the cluster.

Setting up /etc/llthosts

The file llthosts(4) is a database, containing 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 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 116.

Using vi or another editor, create the file /etc/lltab that contains entries that resemble:

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

The first line must identify the system on which the file exists. In the example above, the value for `set-node` could be north, 0, or the file name /etc/nodename, provided the file contains the name of the system (north in this example). 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/llttab.

LLT directives

For more information about LLT directives, refer to the `lltab`(4) manual page.

Table 7-4 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 listed in /etc/llthosts file. Note that LLT fails to operate if any systems share the same ID.
`link`	Attaches LLT to a network interface. At least one link is required, and up to eight are supported. The first argument to link is a user-defined tag shown in the `lltstat(1M)` output to identify the link. It may also be used in `lltab` to set optional static MAC addresses. The second argument to link is the device name of the network interface. Its format is *device_name*:*device_instance_number*. The remaining four arguments to link are defaults; these arguments should be modified only in advanced configurations. There should be one link directive for each network interface. LLT uses an unregistered Ethernet SAP of 0xCAFE. If the SAP is unacceptable, refer to the `lltab(4)` manual page for information on how to customize SAP. Note that IP addresses do not need to be assigned to the network device; LLT does not use IP addresses.
`set-cluster`	Assigns a unique cluster number. Use this directive when more than one cluster is configured on the same physical network connection. LLT uses a default cluster number of zero.
`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 and, in addition to enabling VCS communication, broadcasts heartbeats to monitor each network connection.

For more information about LLT directives, refer to the `lltab`(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 group membership and atomic broadcast (GAB)

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 a simple /etc/gabtab file:

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

Where the `-c` option configures the driver for use and `-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

1. On Node A, create the files /etc/llttab, /etc/llthosts, and /etc/gabtab. Use the files 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 listed, add the node.

```
# hagrp -modify group SystemList -add sysB 1
```

Verifying configuration on both nodes

1 On Node B, check the cluster membership.

```
# gabconfig -a
```

2 Start the VCS on Node B.

```
# hastart
```

3 Verify that VCS is up on both nodes.

```
# hastatus
```

4 List the service groups.

```
# hagrp -list
```

5 Unfreeze the service groups.

```
# hagrp -unfreeze group -persistent
```

6 Implement the new two-node configuration.

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

Section II

Configuring VCS for virtual machines

This section contains the following chapters:

Chapter 8

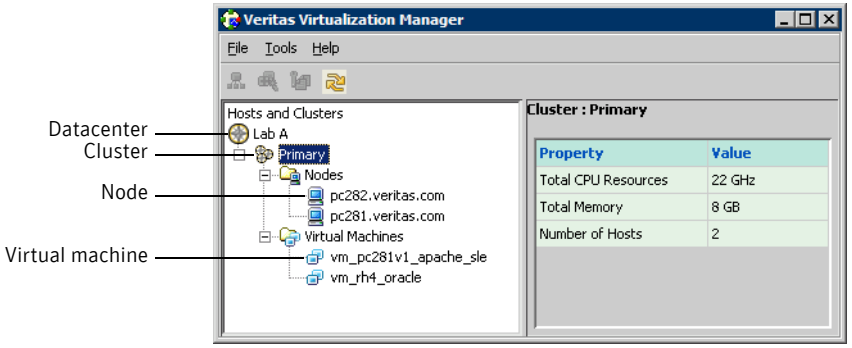
Installing the Veritas Virtualization Manager (VVM)

This chapter contains the following topics:

About Veritas Virtualization Manager

The Veritas Virtualization Manager (VVM) is a user interface that enables you to configure virtual machines for high availability, disaster recovery, or increase allocated storage for a virtual machine. Note that the view that VVM renders is similar to the view from the VMware VI Client—however—VVM displays only nodes and virtual machines that are in VMware clusters.

Figure 8-1 The Veritas Virtualization Manager interface



After you start the application, VVM presents a hierarchy of objects in the left side of the window, and the selected object's properties and values in the right. The hierarchy matches the datacenters, clusters, nodes, and virtual machines that are inside the cluster that you created in VMware. VVM also provides information about the selected object.

You can use VVM for a variety of tasks, with it you can:

- Configure a virtual machine for high availability.
  See "Making virtual machines highly available" on page 128.
- Configure a virtual machine for disaster recovery.
  See "Configuring virtual machines for disaster recovery using the Veritas Virtualization Manager" on page 144.
- Grow storage size for your virtual machines.
  See "Increasing allocated storage" on page 202.
- Add .iso image files to your virtual machines. This gives you easy access to the Veritas Virtual Machine Toolkit.
  - See "Supported software" on page 28.
  - See "Mounting the Veritas Virtual Machine Toolkit ISO file to a virtual machine" on page 172.
  - See "To add the toolkit .iso file" on page 186.

Installing the Veritas Virtualization Manager

Install the Veritas Virtualization Manager on a Windows computer. Install it on a standalone system, which is outside of the cluster.

Veritas Virtualization Manager hardware requirements

Symantec recommends using the Pentium III, 400MHz, 256MB RAM, and 800x600 display resolution as minimum requirements. The following items are the minimum hardware requirements for the Veritas Virtualization Manager:

- Pentium II 300 megahertz
- 256 megabytes of RAM
- 800x600 display resolution
- 8-bit color depth of the monitor
- Graphics card capable of 2D images
- Approximately 40 MB of free hard drive space

Installing the Veritas Virtualization Manager

Before you install the VVM, make sure to check the system requirements.

To install the Veritas Virtualization Manager

1. Insert the product disc into a drive on the client system.
2. Navigate to the cluster_server/vvm directory and open it.
3. Run the vcsvm.msi file.
4. Review the welcome screen and click **Next**.
5. Read the license agreement. If you choose to accept it, click the **I accept the terms in the license agreement** radio button. Click **Next**.
6. Enter your user name, and your organization. Select the radio button that reflects your usage on the client. Click **Next**.
7. Accept the complete setup default and click **Next**.
8. Click the **Install** button to install VVM.
9. Click the **Finish** button.

When the installation program finishes, you need to prepare the SSL certificate for the VirtualCenter Servers that you want to log in to.

Preparing SSL certificates

VMware Web Services require an SSL certificate to operate, and Veritas Virtualization Manager (VVM) uses these Web Services. VVM requires a certificate store for login, which you create by importing a certificate file. For each VirtualCenter Server you have deployed, you must have a certificate store (a keystore file) available for it.

Importing the certificate file on the VirtualCenter Server

You first must import the certificate file to get the certificate store.

To generate the certificate store

1. Open a command prompt on the VirtualCenter Server.
2. Create a temporary directory to hold the keystore file, for example:
   `C:\vmware-certs`
3. Change directory into the directory that you created.
4. Locate and note the directory to a keytool.exe executable. It is commonly in: C:\Program Files\Common Files\VERITAS Shared\VRTSjre\jre1.5\bin.
   Some systems may have this file in a different directory. In this situation, search for the file. If multiple jre directories exist, find the file that is in the version 1.5 directory.
5. From the C:\vmware-certs directory, enter:
   "*pathname*\keytool.exe" -import -file "*pathname*\rui.crt" -alias *server-name* -keystore *vmware.keystore*
   A full command example is:
   ```
   "\Program Files\Java\jre1.5.0_06\bin\keytool.exe" -import -file
   "C:\Documents and Settings\All Users\Application Data\
   VMware\VMware VirtualCenter\SSL\rui.crt" -alias vc-server1
   -keystore vmware.keystore
   ```
   - The pathname and executable for the keytool is the path from root to the keytool.exe file that you found in step 4 (“\Program Files\Java\jre1.5.0_06\bin\keytool.exe” in this example). Note that this path and file name starts and ends with quotes.
   - The pathname and the certificate file leads to the rui.crt certificate file ("C:\Documents and Settings\All Users\ Application Data\ VMware\VMware VirtualCenter\SSL\rui.crt" in this example). Note that this path and file name starts and ends with quotes. If for any reason, the rui.crt file does not exist, refer to VMware SDK documentation for creating it.

- The server-name is the name of the VirtualCenter Server from where you copied the file (vc-server1 in this example).
- The certificate store that you are creating (vmware.keystore in this example).

6 Enter a password for the keystore. Use the same password as the one that you use to log into the VirtualCenter Server. Press the **Enter** key.

7 When asked if you want to trust the certificate, answer **`yes`**.

8 Enter **`yes`** to import the certificate.

Copying the keystore file

You now need to copy the keystore file onto the client where you plan to use VVM.

To copy the file from the VirtualCenter Server to the VVM client

1 On the client where you plan to install VVM, create a new directory to hold the certificate store, for example: vmware-certs.

2 Copy the keystore file that you have created (vmware.keystore in the example) from the VirtualCenter Server to the new directory on your client.

When you log into VVM, it asks for authentication information including the path to the SSL certificate.

To start the Veritas Virtualization Manager

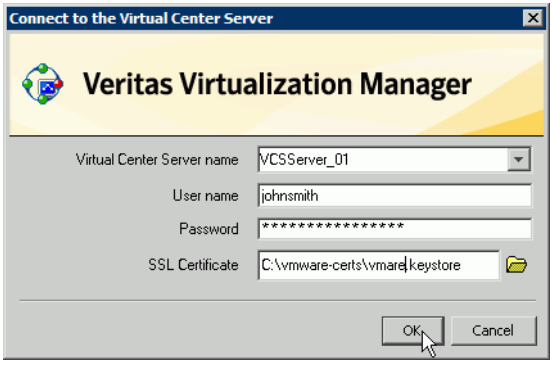
1 From a Windows client, click **Start** > **Programs** > **Veritas** > **Veritas Virtualization Manager**.

2 Enter the name of the VirtualCenter Server, your user name and password, and the full path to the SSL certificate.

To provide the SSL certificate path information for VVM log in

- Enter the path information to the keystore that you created. From the example, enter: C:\vmware-certs\vmware.keystore.

Figure 8-2 Entering the SSL Certificate path information for the keystore



Removing the Veritas Virtualization Manager (VVM)

Use standard Windows Add or Remove functionality to remove the Veritas Virtualization Manager.

To remove the Veritas Virtualization Manager

1. From the Windows client, open the Control Panel.
2. Double-click the **Add or Remove Programs** icon.
3. Scroll down, and click **Veritas Virtualization Manager** to select it.
4. Click the **Remove** button.

Chapter 9

Configuring virtual machines for high availability

This chapter contains the following topics:

About configuring virtual machines

After you install and configure VCS on the ESX Servers, you can configure the virtual machines for high availability. You create the virtual machines using VMware tools and then use the Veritas Virtualization Manager (VVM) to configure them.

A tight link exists between VMware clusters and VCS clusters. You must have an existing VMware cluster before you can use VVM to deploy virtual machines. VVM checks for the existence of the VMware cluster, and uses that foundation to configure highly available virtual machines.

Making virtual machines highly available

You can take existing virtual machines that are part of a VMware cluster, and configure them into virtual machines that run under VCS. When you configure them for VCS, the resources that they use become part of service groups, which you can then manage.

Prerequisites for configuring virtual machines for high availability

Before you start, ensure that:

- The hardware for the cluster is set up and ready to use, which includes shared storage and networks that are visible from all nodes.
- Enough computing power is available for the virtual machines where you plan to add to the nodes.

You need to prepare the VMware configuration, in the following list ensure that:

- The VirtualCenter Server is configured and running.
- You have administrative access to the VirtualCenter Server.
- The nodes are part of a VMware cluster. Also ensure that:
  - Each ESX Server that runs VCS is part of a VMware cluster object in the Virtual Center database.
  - Each ESX server under a particular cluster object maps to a corresponding ESX node in the VCS cluster.
- You have disabled VMware HA on the target clusters.

You must also ensure that:

- VCS for VMware ESX is configured and running on your nodes.
- The SSL certificate for the Veritas Virtualization Manager is available.
  See “Preparing SSL certificates” on page 124.

To start the virtual machine deployment

1. From a Windows client, click **Start** > **Programs** > **Veritas** > **Veritas Virtualization Manager**.
2. Enter the name of the VirtualCenter Server, your user name and password, and the full path to the SSL certificate.
   See "To provide the SSL certificate path information for VVM log in" on page 125.

To configure a virtual machine for high availability

1. Right-click the virtual machine that you want to make highly available. From the pull-down menu, select **Configure HA**.
2. In the next window, enter the user name and password for the VCS cluster. You only need to connect to a cluster once per VVM session.
3. Choose to configure a new administrator. This user administers the service group that VVM creates when you complete this wizard. Note the name and password for future reference.
4. Review the deployment summary.
   - Click on a summary item to edit it. Note that some items cannot be edited.
   - Click the **Back** button to change any values.
   - Click the **Finish** button to finalize the configuration for the virtual machine.

You have now made a virtual machine highly available.

Reviewing the generated service groups

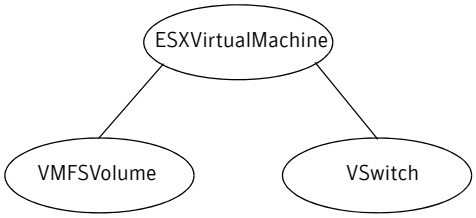
After you have used the Veritas Virtualization Manager to configure a virtual machine for high availability, VVM creates a service group. VVM also creates a service group administrator if you provided the administrator's information while using VVM.

The service group that VVM creates for a highly available virtual machine has an ESXVirtualMachine resource that depends on its storage (VMFSVolume) and network (VSwitch) resources. If any of the resources in this group fails for any reason, VCS moves the ESXVirtualMachine resource to another available node. Note that fail over of the virtual machine does not include applications that you want to monitor within the virtual machines. For application monitoring, see:

- "Deploying VCS components on virtual machines running Windows" on page 183
- "Deploying VCS components on virtual machines running Linux" on page 155

In Figure 9-1, you can see a basic example of a resource dependency graph for a service group.

Figure 9-1 A service group with the ESXVirtualMachine, VSwitch, and VMFSVolume resources



Accessing the service groups

Although the Veritas Virtualization Manager creates a service group for you, use command line tools or the Cluster Management Console to manage resources. Note that you can only manage resources that are outside of virtual machines with these tools.

For information about using service groups, either through a CLI or GUI:

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

Verifying virtual machine failover

Verify the configuration in different situations.

Using a switch command

Switch the virtual machine to another node in the cluster to make sure the service group fails over. If all the resources are properly configured, the service group shuts down on the first node and comes up on the second node.

Other verification scenarios

In all of these verification scenarios, you are stopping or moving a virtual machine, or stopping a resource for that virtual machine. VCS should detect the failure, or the movement, and either fail over the effected virtual machine or take no action. The following list presents some quick testing scenarios:

- From outside of VCS control, stop the virtual machine. VCS should fail the virtual machine over to the other node.
- Boot the virtual machine through VCS by entering a `hagrp -online` command. Move the virtual machine to another node by shutting it down through VCS on the node where the virtual machine is running. Boot the virtual machine outside of VCS control on the other node—the service group comes online on that node.
- Trigger a VMotion for a virtual machine. When you trigger a VMotion for a virtual machine, VCS marks the service group, which contains the virtual machine, as offline on the first node. It then marks the service group as online on the target node.

Chapter 10

Configuring virtual machines for disaster recovery

This chapter contains the following topics:

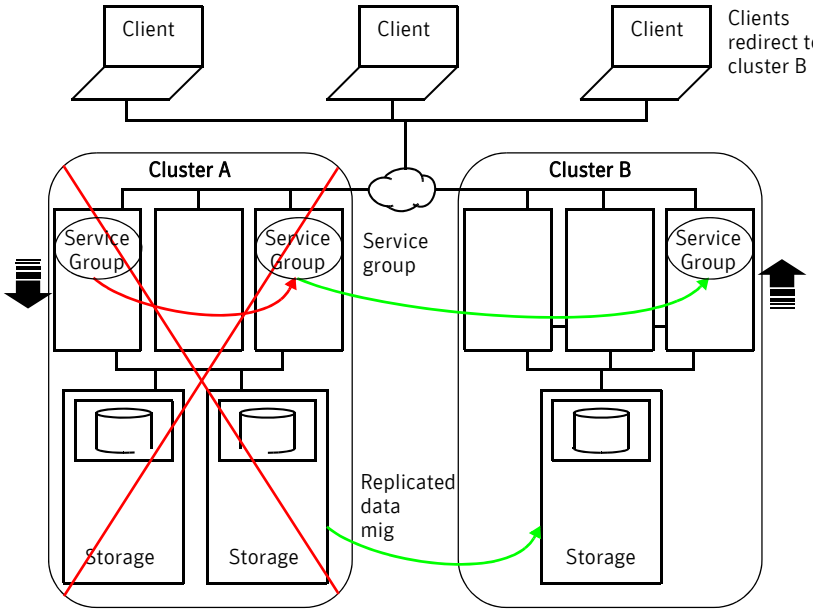
About VCS global clusters

Local clustering provides local failover for each site or building. But, these configurations do not provide protection against large-scale disasters such as major floods, hurricanes, and earthquakes that cause outages for an entire city or region. The entire cluster could be affected by an outage.

In such situations, VCS global clusters ensure application availability by migrating service groups to remote clusters located considerable distances apart.

Let us take the example of an Oracle database configured in a VCS global cluster. Oracle is installed and configured in a virtual machine. The virtual machine is configured in a VCS service group. The service group is online on a system in cluster A and is configured to fail over globally, on clusters A and B.

Figure 10-1 Sample global cluster setup



VCS continuously monitors and communicates events between clusters. Inter-cluster communication ensures that the global cluster is aware of the state of global service group at all times.

In the event of a system or application failure, VCS fails over the virtual machine service group to another system in the same cluster. If the entire cluster fails, VCS fails over the service group to the remote cluster, which is part of the global cluster. VCS also redirects clients once the application is online on the new location.

VCS global clusters: The building blocks

VCS extends clustering concepts to wide-area high availability and disaster recovery with the following building blocks.

Global service groups

A *global* service group is a regular VCS group with additional properties to enable wide-area failover. The global service group attribute ClusterList defines the list of clusters to which the group can fail over. The service group must be configured on all participating clusters and must have the same name on each cluster.

VCS agents manage replication during cross-cluster failover. You must configure a resource of type DNS to perform a canonical name update if cross-cluster failover spans subnets.

Global cluster management

VCS enables you to perform operations (online, offline, switch) on global service groups from any system in any cluster. You must log on with adequate privileges for cluster operations.

You can bring service groups online or switch them to any system in any cluster. If you do not specify a target system, VCS uses the FailOverPolicy to determine the system.

Management of remote cluster objects is aided by inter-cluster communication enabled by the wide-area connector (wac) process.

Resiliency and right-of-way

VCS global clusters maintain resiliency using the wide-area connector process and the ClusterService group. The wide-area connector process runs as long as there is at least one surviving node in a cluster.

The wide-area connector and notifier are components of the ClusterService group.

VCS framework

VCS agents manage external objects that are part of wide-area failover. These objects include replication, DNS updates, and so on. These agents provide a robust framework for specifying attributes and restarts, and can be brought online upon fail over.

Wide-area heartbeats

VCS requires at least one wide-area heartbeat going from each cluster to every other cluster. VCS starts communicating with a cluster only after the heartbeat reports an *alive* state. VCS uses the ICMP ping by default, the infrastructure for which is bundled with the product.

DNS agent

The DNS agent updates the canonical name-mapping in the domain name server after a wide-area failover. For more agent information:

See the *Veritas Cluster Server Bundled Agents Reference Guide*.

VCS agents to manage replication

VCS supports several replication technologies. VCS agents manage the replication status between primary and secondary sites. Contact your Symantec sales representative for a list of replication technologies supported with this release of VCS.

Prerequisites for global clusters

This section describes the prerequisites for configuring global clusters.

Cluster setup

You must have at least two clusters to set up a global cluster. Every cluster must have the required licenses. A cluster can be part of one global cluster. VCS supports a maximum of four clusters participating in a global cluster.

Clusters must be running on the same platform; the operating system versions can be different. Clusters must be using the same VCS version.

Cluster names must be unique within each global cluster; system and resource names need not be unique across clusters. Service group names need not be unique across clusters; however, global service groups must have identical names.

Every cluster must have a valid virtual IP address, which is tied to the cluster. Define this IP address in the cluster's ClusterAddress attribute. This address is normally configured as part of the initial VCS installation. The IP address must have a DNS entry.

For remote cluster operations, you must configure a VCS user with the same name and privileges in each cluster.

ClusterService group

The ClusterService group must be configured with the wac, VSwitch, and IP resources. It is configured automatically when VCS is installed or upgraded, or by the GCO configuration wizard. The service group may contain additional resources for Cluster Management Console and notification, if these components are configured.

If you entered a license that includes VCS global cluster support during the VCS install or upgrade, the ClusterService group, including the wide-area connector process, is automatically configured.

Replication setup

You must set up real-time data replication between clusters. Contact your sales representative for a list of replication technologies supported with this release of VCS.

Setting up a global cluster manually

This section describes the steps for planning, configuring, and testing a global cluster. It describes an example of converting a virtual machine for local high availability in a VCS cluster to a highly available, disaster-protected infrastructure using a second cluster.

- Configuring the ClusterService group
- Configuring replication
- Configuring the second cluster
- Creating the global service group

Note: The procedure assumes your local cluster is set up and that you are replicating data between the local and remote clusters.

Configuring the ClusterService group

Configure the ClusterService group as described in this section.

To configure the ClusterService group

1. Create a service group called ClusterService.
2. Add a resource of type VSwitch to the service group. Name the resource csgnic. Set the value of the Device attribute to the name of the VSwitch. Configure other attributes, if desired.
3. Add a resource of type IP to the service group. Name the resource gcoip. Configure the following attributes for the resource:
   - Address—A virtual IP address assigned to the cluster.
   - Device—The name of the switch on the system. The device is defined as a local attribute for each system in the cluster.
   - NetMask—The subnet to which the virtual IP address belongs.
4. Link the VSwitch and IP resources such that the IP resource depends on the VSwitch resource.
5. Add a resource of type Application to the service group. Name the resource wac. Configure the following attributes for the resource:
   - StartProgram—"/opt/VRTSvcs/bin/wacstart"
   - StopProgram—"/opt/VRTSvcs/bin/wacstop"
   - MonitorProcesses— {"/opt/VRTSvcs/bin/wac" }
   - RestartLimit—3
6. Link the Application and IP resources, making Application the parent resource.
7. Enable both resources.
8. Bring the ClusterService service group online.

Sample configuration

```
group ClusterService (
    SystemList = { thorpc132 = 1, thorpc136 = 2 }
    PrintTree = 0
    AutoStartList = { thorpc132 }
    OnlineRetryLimit = 3
    OnlineRetryInterval = 120
    )

    Application wac (
        StartProgram = "/opt/VRTSvcs/bin/wacstart"
        StopProgram = "/opt/VRTSvcs/bin/wacstop"
```

```
    MonitorProcesses = { "/opt/VRTSvcs/bin/wac" }
    RestartLimit = 3
    )

IP webip (
    Device @thorpc132 = vswif0
    Device @thorpc136 = vswif0
    Address = "10.182.146.154"
    NetMask = "255.255.252.0"
    )

VSwitch csgnic (
    VirtualSwitch @thorpc132 = vSwitch0
    VirtualSwitch @thorpc136 = vSwitch0
    )

wac requires webip
webip requires csgnic
```

Configuring replication

VCS supports several replication solutions for global clustering. Contact your Symantec sales representative for the solutions supported by VCS. This example describes how to set up replication using VCS agent for MirrorView.

Adding the resources for replication

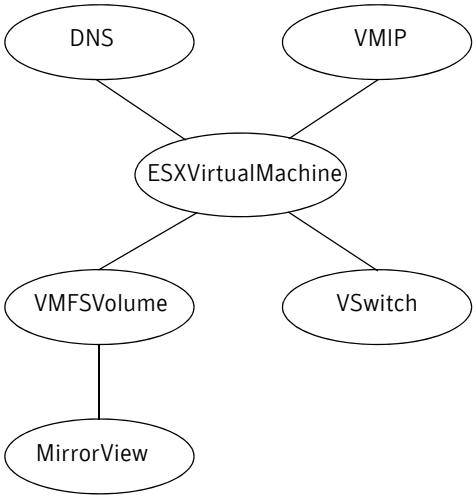
1. Add a resource of type MirrorView to the service group.
2. Configure the attributes of the MirrorView resource.
   - NaviCliHome—NaviCLI installation directory
   - LocalArraySPNames—The list of storage processors within the array to which the local hosts are connected. Can be names or IP addresses.
   - RemoteArraySPNames—The list of storage processors within the array to which the remote hosts are connected. Can be names or IP addresses.
   - Mode—The replication mode, which is either: sync or async.
   - GrpName—The name of the consistency group to which the mirrors belong. This function applies only if the mode is async.
   - MirNames—This function lists individual mirrors that are a part of the replication relationship and managed by VCS. This attribute is ignored if you specify the GrpName attribute.
   - SplitTakeover—This integer indicates whether VCS should forcefully promote a secondary to a primary.
3. Add a resource of type DNS to the service group and configure its attributes:
   - Domain—Domain name. For example, veritas.com.

- Alias—Alias to the canonical name. For example, www.
- Hostname—Canonical name of a system or its IP address. For example, mtv.veritas.com.
- TTL—Time To Live (in seconds) for the DNS entries in the zone being updated. Default value: 86400.
- StealthMasters—List of primary master name servers in the domain. This attribute is optional if the primary master name server is listed in the zone's NS record. If the primary master name server is a stealth server, the attribute must be defined.
  Note that a stealth server is a name server that is authoritative for a zone but is not listed in the zone's NS records.
  Optionally, configure the TSIGKeyFile attribute for secure DNS updates.
  See the *Veritas Cluster Server Bundled Agents Reference Guide*.

4 Add a resource of type VMIP and configure its attributes.
- VMwareResName—The name of the VCS resource that manages the virtual machine.
- IPAddress—The IP address that is assigned to the virtual machine interface.
- MACAddress—The MAC address of the virtual NIC
- NetMask—The subnet mask that is associated with the IP address. You must specify this value in decimal (base 10).
- Gateway—The default gateway for the virtual machine.
- DNS—List of DNS servers in the required search order.

5 Create the following resource dependencies:
- VMFSVol resource depends on the MirrorView resource.
- DNS resource depends on the ESXVirtualMachine resource.
- VMIP resource depends on the ESXVirtualMachine resource.

Figure 10-2 Sample dependency graph



Configuring the second cluster

1. Configure the ClusterService group in the second cluster.
   See "Configuring the ClusterService group" on page 138.
2. Create a configuration that is similar to the one in the first cluster. You can do this by copying the configuration of the service group from the main.cf file in the primary cluster to the secondary cluster.
3. Make appropriate changes to the configuration. For example, you must modify the SystemList attribute to reflect the systems in the secondary cluster. Also, you must modify the VMFSVolume and replication resources to point to the local storage at the remote cluster.
   Make sure that the name of the service group is identical in both clusters.
4. To assign remote administration privileges to users, configure users with the same name and privileges on both clusters.

Linking clusters

Once the VCS and the replication infrastructure has been set up at both sites, you must link the two clusters.

Before linking clusters, verify the virtual IP address for the ClusterAddress attribute for each cluster is set. Use the same IP address as the one assigned to the IP resource in the ClusterService group.

To add a remote cluster to a global environment

1 In the **Cluster:Summary** view, in the **Configuration** task panel, click **Add/Delete Remote Cluster**.

2 In the **Remote Cluster Configuration** wizard, read the introductory information and then click **Next**.

3 In the **Configuration Options** dialog box, click **Add Cluster** and then click **Next**.

4 Do one of the following:

- For nonsecure clusters
  In the **Connection Details** dialog box, specify the following details for the connection to the remote cluster and then click **Next**:
  - A name or address
    Enter the IP address of the cluster, the IP address of a cluster system, or the name of a cluster system.
  - The port
    Verify the port number. The default is 14141.
  - An administrator user name and password.
    Enter an administrator-level user name and password that is valid on the remote cluster.
- For secure clusters
  In the **Connection Details** dialog box, specify the following details for the connection to the remote cluster and then click **Next**:
  - A name or address
    Enter the IP address of the cluster, the IP address of a cluster system, or the name of a cluster system.
  - The port
    Verify the port number. The default is 14141.
  - Authentication credentials
    Choose to connect to the remote cluster with the credentials used for the current cluster connection or enter new credentials. You must specify the user name, password, domain, and domain type. If you have connected to the remote cluster before using this wizard, you can use the credentials from the previous connection.

5 Click **Finish**.
The cluster icon changes to indicate that the cluster is a global cluster.

Creating the global service group

Use Veritas Cluster Management Console to configure the global service group. The Global Group Configuration wizard configures a service group in a local cluster as a global service group.

To convert a service group on a local cluster to a global service group

1. Start Veritas Cluster Management Console and log on to the cluster.
2. In the **Cluster:Summary** view, in the **Groups Listing** table, click the linked name of the service group that you want to convert.
   This service group should already have been commonly configured on at least one local and one remote cluster.
3. In the **Group:Summary** view, in the **Configuration** task panel, click **Configure Global Group**.
4. In the **Global Group Configuration** wizard, read the introductory information and click **Next**.
5. In the **Cluster List Configuration** dialog box, under **Available Clusters**, select the clusters on which the global service group can come online. To select a cluster, click the right-arrow button to move the cluster name under **Selected Clusters**.
6. Select the policy for service group failover and then click **Next**:
   - **Manual** prevents a service group from automatically failing over to another cluster.
   - **Auto** enables a service group to automatically fail over to another cluster if it is unable to fail over within the cluster, or if the entire cluster faults.
   - **Connected** enables a service group to automatically fail over to another cluster if it is unable to fail over within the cluster.
7. In this step, you update the cluster list of remaining instances of the selected global service group. To perform the update, you must first verify or supply the authentication credentials for each remaining global cluster in the list. The Cluster Management Console can then connect to those clusters and update the lists.
   In the **Remote Cluster Configuration** dialog box, verify the required information for the remaining remote clusters and then click **Next**.
   To change authentication information, click a cluster name under E**xisting Clusters** and then enter the authentication information in the fields to the right. The requisite information in this dialog box varies depending upon whether or not the cluster is secure (uses an authentication broker).

8 Click **No** if you want the operation to be completed only if the wizard can connect to all selected clusters.

9 Click **Next**.

10 Click **Finish**.

Configuring virtual machines for disaster recovery using the Veritas Virtualization Manager

You can enable existing virtual machines for disaster recovery using the Veritas Virtualization Manager. Before you start you need to make sure that replication exists between the primary site and the secondary site.

See "Prerequisites for global clusters" on page 136.

Overview of tasks

Table 10-1 Configuration tasks

Task	Reference
Review prerequisites.	See "Prerequisites for configuring virtual machines for disaster recovery" on page 145.
Set up secure DNS update.	See "Setting up secure DNS update" on page 145.
Use VVM to configure virtual machines for disaster recovery.	See "Using Veritas Virtualization Manager to configure virtual machines for disaster recovery" on page 147.
On the primary site, deploy the toolkit and applications.	See "Deploying VCS components on the virtual machines in the primary site" on page 148.
Confirm the availability of the service group.	See "Confirming service group availability" on page 148.
Reverse the direction of replication.	See "Reversing the direction of replication" on page 148.
On the secondary site, use VVM to configure the virtual machines.	See "Using VVM to configure virtual machines for disaster recovery on the secondary site" on page 149.
Deploy VCS components.	See "Deploying VCS components on virtual machines in the secondary site" on page 149.
Verify the service group and use the Global Wizard.	See "Verifying the service group on the secondary site and using the Global Wizard" on page 150.

Table 10-1 Configuration tasks

Task	Reference
Perform post-failover actions.	See "Post-failover actions" on page 150.
Review the service group that VVM creates.	See "Reviewing the generated service groups" on page 150.
Work with the service groups.	See "Accessing the service groups" on page 151.
Verify machine fail over functionality.	See "Verifying virtual machine failover" on page 151.

Prerequisites for configuring virtual machines for disaster recovery

Before you start ensure that:

- The hardware for the cluster is set up and ready to use, which includes shared storage and networks that are visible from all nodes.
- The replication is set up and ready to use. Note that a replication solution is required for disaster recovery. Contact you Symantec representative for a list of supported replication arrays.

You need to prepare the VMware configuration, in the following list ensure that:

- The VirtualCenter Server is configured and running.
- You have administrative access to the VirtualCenter Server.
- The nodes are part of a VMware cluster. Also ensure that:
  - Each ESX Server that runs VCS is part of a VMware cluster object in the VirtualCenter database.
  - Each ESX server under a particular cluster object maps to a corresponding ESX node in the VCS cluster.
- You have disabled VMware HA on the VMware clusters.

You must also ensure that:

- VCS for VMware ESX is configured and running on your nodes.
- The SSL certificate for the Veritas Virtualization Manager is available. See "Preparing SSL certificates" on page 124.

Setting up secure DNS update

VVM requires a secure key to ensure security and thwart spoofing. You need to create a TSIG key (Transaction Signature) as specified in RFC 2845. TSIG is a

shared key message authentication mechanism available in DNS. A TSIG key provides a means to authenticate and verify the validity of DNS data exchanged, using a shared secret key between a resolver and either one or two servers.

Setting up secure updates using TSIG keys

In the following example, the domain is veritas.com.

To use secure updates using TSIG keys

1 Run the `dnssec-keygen` command with the HMAC-MD5 option to generate a pair of files that contain the TSIG key:

```
# dnssec-keygen -a HMAC-MD5 -b 512 -n HOST veritas.com.
    Kveritas.com.+157+00000
```

2 Open the Kveritas.com.+157+00000.key file. After running the `cat` command, the contents of the file resembles:

```
# cat Kveritas.com.+157+00000.key
    veritas.com. IN KEY 512 3 157 +Cdjlkef9ZTSeixERZ433Q==
```

3 Copy the shared secret (the TSIG key), which looks like:

```
+Cdjlkef9ZTSeixERZ433Q==
```

4 Configure the DNS server to only allow TSIG updates using the generated key. Open the named.conf file and add these lines.

```
key veritas.com. {
    algorithm hmac-md5;
    secret "+Cdjlkef9ZTSeixERZ433Q==";
};
```

Where **+Cdjlkef9ZTSeixERZ433Q==** is the key.

5 In the named.conf file, edit the appropriate zone section and add the allow-updates sub-statement to reference the key:

```
allow-update { key veritas.com. ; } ;
```

6 Save and restart the named process.

7 Place the files containing the keys on each of the nodes that is listed in your group's SystemList. The DNS agent uses this key to update the name server. Copy both the private and public key files on to the node. A good location is in the /var/tsig/ directory.

8 Set the TSIGKeyFile attribute for the DNS resource to specify the file containing the private key.

```
DNS www (
Domain = "veritas.com"
Alias = www
Hostname = north
TSIGKeyFile a= "/var/tsig/Kveritas.com.+157+00000.private"
)
```

Using Veritas Virtualization Manager to configure virtual machines for disaster recovery

Use the Veritas Virtualization Manager (VVM) to configure the virtual machines for disaster recovery.

To start the virtual machine deployment

1. From a Windows client, click **Start** > **Programs** > **Veritas** > **Veritas Virtualization Manager**.
2. Enter the name of the VirtualCenter Server, your user name and password, and the full path to the SSL certificate. See "To provide the SSL certificate path information for VVM log in" on page 125.

To configure a virtual machine for disaster recovery

1. Right-click the virtual machine. From the pull-down menu, select **Configure DR**.
2. In the next window, enter the user name and password for the VCS cluster. You only need to connect to a cluster once per VVM session. Click the **OK** button.
3. Choose to configure a new VCS user. This user administers the service group that VVM creates when you complete this wizard. Note the name and password for future reference.
4. Provide the local and remote storage processors' addresses. Click the **Next** button to continue.
5. Enter the requested information for the DNS agent.
   - Domain—The string representing the domain name.
   - Alias—The string representing the alias to the canonical name.
   - Hostname—A string representing canonical name of a system.
   - IPAddress—Specifies the IP address that is assigned to the hostname.
   - TSIGKeyFile—Specifies the absolute path to the file containing the private TSIG (Transaction Signature) key.
6. Enter the required information for VMIP agent.
   - IPAddress—The IP address that is assigned to the virtual machine interface.
   - NetMask—The subnet mask that is associated with the IP address. You must specify this value in decimal (base 10).
   - Gateway—The default gateway for the virtual machine.
   - Primary DNS—The primary DNS for the virtual machine.

- Secondary DNS—The secondary DNS for the virtual machine.
- Tertiary DNS—Other DNS for the virtual machine are optional.

7 Review the deployment summary.

- Click on a summary item to edit it. Note that some items cannot be edited.
- Click the **Back** button to change any previous values.
- Click the **Finish** button to finalize the VCS configuration for the virtual machine.

Repeat this process for each virtual machine that you want in the cluster.

Deploying VCS components on the virtual machines in the primary site

You must install the Veritas Virtual Machine Toolkit and configure the applications on the virtual machine. Perform the procedures in the following chapter depending on operating system:

- Chapter 11, "Deploying VCS components on virtual machines running Linux" on page 155.
- Chapter 12, "Deploying VCS components on virtual machines running Windows" on page 183.

Confirming service group availability

Check to see if the service group, which you have just created with VVM, can come online. Once you have established that it comes online, bring the service group offline.

See "Accessing the service groups" on page 151.

Reversing the direction of replication

You now need to reverse the direction of replication between your primary and secondary arrays. You must reverse replication direction for all the datastores used by the virtual machines that you have configured.

Contact your Symantec sales representative for a list of replication technologies supported with this release of VCS. Consult your replication solution's manual for information on reversing replication direction.

Using VVM to configure virtual machines for disaster recovery on the secondary site

Before you configure the virtual machines on the secondary site, perform the following tasks using the VMware commands:

- Rescan all the storage adapters.
- Verify that all datastores are visible on all nodes on the secondary site.
- Register a virtual machine on a node in the secondary site.

Use VVM to log into the cluster on the secondary site and to configure the virtual machines for disaster recovery.

Refer back to the previous procedure, as follows:

- "Using Veritas Virtualization Manager to configure virtual machines for disaster recovery" on page 147

VVM creates a new service group on the secondary site.

Note: It is very important that you give this new service group the same name that you used for your primary site.

Deploying VCS components on virtual machines in the secondary site

You must now configure the Veritas Virtual Machine Toolkit on the secondary site.

- For Linux:
  - See "Configuring the Veritas Virtual Machine Toolkit" on page 173.
  - See "Validating the configuration of the Veritas Virtual Machine Toolkit" on page 174.
- For Windows:
  - See "Configuring the Veritas Virtual Machine Toolkit" on page 188.
  - See "Validating the configuration of the Veritas Virtual Machine Toolkit" on page 189.

Verifying the service group on the secondary site and using the Global Wizard

Verify that the service group can come online on the secondary site. You are now ready to use the Global Wizard, the wizard configures the service group as a global group.

See "Creating the global service group" on page 143.

Post-failover actions

After a disaster recovery, or after switching the global service group between the clusters, you must reconfigure the Veritas Virtual Machine Toolkit on the site that the cluster has failed over to.

- For Linux:
  - See "Configuring the Veritas Virtual Machine Toolkit" on page 173.
  - See "Validating the configuration of the Veritas Virtual Machine Toolkit" on page 174.
  - Apply the changes to the configuration by running the vcsag_config.pl program with the -apply option, as follows:

    ```
    # /opt/VRTSvcs/bin/vcsag_config.pl -apply
    ```
- For Windows:
  - See "Configuring the Veritas Virtual Machine Toolkit" on page 188.
  - See "Validating the configuration of the Veritas Virtual Machine Toolkit" on page 189.
  - Apply the changes to the configuration by running the vcsag_config.pl program with the -apply option, as follows:

    ```
    C:\> "%VRTS_PERL_BIN%\perl" "%VCS_HOME%\bin\vcsag_config.pl" -apply
    ```

    The default for VRTS_PERL_BIN is C:\Program Files\Veritas\VRTSPerl\bin. The default for the VCS_HOME is C:\Program Files\Veritas\Cluster Server.

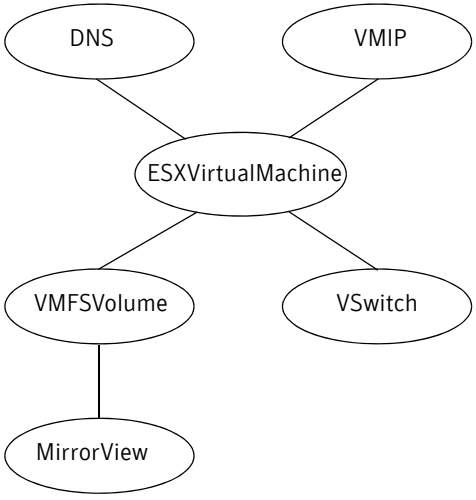
Reviewing the generated service groups

After you have used the Veritas Virtualization Manager to configure a virtual machine for disaster recovery, VVM creates a service group. VVM also creates a service group administrator if you provided the administrator's information while using VVM.

The service group that VVM creates has an ESXVirtualMachine resource that depends on its storage (VMFSVolume) and network (VSwitch) resources. Further, the VMFSVolume resource depends on the replicated array. The VMIP and DNS resources are critical for moving the service group across networks

and subnets. These two resources depend on the ESXVirtualMachine resource itself. If any of the resources in this group fails for any reason, VCS moves the entire service group to another available node. Note that fail over of the virtual machine does not include applications that you want to monitor within the virtual machines. In Figure 10-3, you can see a basic example of a resource dependency graph for a service group.

Figure 10-3 Sample dependency graph



Accessing the service groups

Use the command line tools or the Cluster Management Console to manage resources. Note that you can only manage resources that are outside of virtual machines with these tools.

For information about using service groups, either through a CLI or GUI:

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

Verifying virtual machine failover

Verify the configuration in different situations.

Using a switch command

Switch the virtual machine to another node in the cluster to make sure the service group fails over. If all the resources are properly configured, the service group shuts down on the first node and comes up on the second node.

Other verification scenarios

In all of these verification scenarios, you are stopping or moving a virtual machine, or stopping a resource for that virtual machine. VCS should detect the failure, or the movement, and either fail over the effected virtual machine or take no action. The following list presents some quick testing scenarios:

- From outside of VCS control, stop the virtual machine. VCS should fail the virtual machine over to the other node.
- Boot the virtual machine through VCS by entering a `hagrp -online` command. Move the virtual machine to another node by shutting it down through VCS on the node where the virtual machine is running. Boot the virtual machine outside of VCS control on the other node—the service group comes online on that node.
- Trigger a VMotion for a virtual machine. When you trigger a VMotion for a virtual machine, VCS marks the service group that contains the virtual machine, as offline on the first node. It then marks the service group as online on the target node.

Section II

Configuring applications in virtual machines

This section contains the following chapters:

Chapter 11

Deploying VCS components on virtual machines running Linux

This chapter contains the following topics:

About VCS components for virtual machines running Linux

VCS for VMware ESX provides basic and detailed monitoring for applications that run on the Linux guest operating system in virtual machines. Both kinds of monitoring requires the use of VCS agents. It also requires that you install the Veritas Virtual Machine Toolkit on the virtual machines where you run the applications.

The Oracle and Apache agents support detailed application monitoring and the ability to detect a graceful shut down. If confronted with the failure of either application, VCS moves the virtual machine that runs the application onto another node.

For any other kind of application that you want to monitor in the virtual machine, you use the Application agent. The Application agent provides basic application monitoring. When the application fails, VCS moves the virtual machine that runs the application to another node.

Basic monitoring checks for running application processes. Detailed monitoring performs application-specific tasks to check the application's health. For example, the Oracle agent performs a transaction on the database and checks to see if it succeeds.

Supported software

VCS 5.0 for ESX supports the following software for the detailed monitoring of applications:

Guest operating systems	■ Red Hat Enterprise Linux 4 (Update 3) ■ SUSE Linux Enterprise Server 9 with SP3
Applications	■ Oracle 10g ■ Apache Web server: Apache HTTP server 1.3, 2.0, and 2.2 IBM HTTP Server 1.3 and 2.0

VCS high availability agents monitor specific resources within the application in a clustered environment.

About the VCS agent for Oracle

The VCS agent for Oracle monitors the Oracle processes using the Monitor entry point. The package contains two agents:

- The Oracle agent that monitors the Oracle database processes.
- The Netlsnr agent that monitors the listener process.

The agents include resource type declarations and agent executables, and are represented with the Oracle and Netlsnr resource types, respectively. Both agents work together to make Oracle highly available.

The agent can detect when Oracle is brought down gracefully. When Oracle is brought down gracefully, the agent does not trigger a resource fault even though Oracle is down.

Requirements for detecting an Oracle instance that was brought down intentionally

VCS supports detection of graceful shutdown for Oracle 10g only. You also must set the value of the MonitorOption attribute for the Oracle resource to 1.

Agent functions

The VCS agent for Oracle supports Monitor entry point.

- Oracle agent

  The Monitor entry point verifies the status of the Oracle processes. The Oracle agent provides two levels of monitoring: basic and detail. By default, the agent does a basic monitoring. You must set the DetailMonitor flag to non-zero enables detail monitoring for Oracle.

  The basic monitoring mode has two options: Process check and Health check. Depending on the mode you want to use, you must set the value of the MonitorOption attribute.

Option	Description
0	Process check
(Default)	The agent scans the process table for the ora_dbw, ora_smon, ora_pmon, and ora_lgwr processes to verify that Oracle is running.
1	Health check (supported on Oracle 10*g* and later) The agent uses the Health Check APIs from Oracle to monitor the SGA and retrieve the information about the instance.

  In the detail monitoring mode, the agent performs a transaction on a test table in the database to ensure that Oracle is functioning properly.

- Netlsnr agent

  The Monitor entry point verifies the status of the listener process. The Netlsnr agent provides two levels of monitoring: basic and detail.

- In the basic monitoring mode, the agent scans the process table for the tnslsnr process to verify the listener process is running. (Default)
- In the detail monitoring mode, the agent uses the lsnrctl status $LISTENER command to verify the status of the Listener process.

State definitions

- ONLINE
  Indicates that Oracle is running.
- OFFLINE
  Indicates that Oracle is not running.
- UNKNOWN
  Indicates that a problem exists with the configuration.
- INTENTIONAL OFFLINE
  Indicates that Oracle was stopped by administrative intervention.The Oracle agent detects an intentional offline state only when health check monitoring is enabled, that is, when the MonitorOption attribute is set to 1.

Oracle attribute definitions

Table 11-1 lists the required attributes for Oracle agent.

Table 11-1 Required attributes for Oracle agent

Required attributes	Definition
Sid	The variable $ORACLE_SID that represents the Oracle instance. The Sid is considered case-sensitive by the Oracle agent and by the Oracle database server. Type and dimension: string-scalar
Owner	The Oracle user, as the defined owner of executables and database files in /etc/passwd. Type and dimension: string-scalar
Home	The $ORACLE_HOME path to Oracle binaries and configuration files. For example, you could specify the path as /opt/ora_home. **Note:** Do not append a slash (/) at the end of the path. Type and dimension: string-scalar

Table 11-2 lists the optional attributes for Oracle agent.

Table 11-2 Optional attributes for Oracle agent

Optional Attributes	Definition
StartUpOpt	This attribute is not enabled for this release. Accept the default setting.
ShutDownOpt	This attribute is not enabled for this release. Accept the default setting.
EnvFile	The full path name of the file that is sourced by the entry point scripts. This file contains the environment variables set by the user for the Oracle database server environment such as LD_LIBRARY_PATH, NLS_DATE_FORMAT, and so on. The syntax for the contents of the file depends on the login shell of Owner. File must be readable by Owner. The file must not contain any prompts for user input. Type and dimension: string-scalar
Pfile	The name of the initialization parameter file with the complete path of the startup profile. You can also use the server parameter file. Create a one-line text initialization parameter file that contains only the SPFILE parameter. See the Oracle documentation for more information. Type and dimension: string-scalar
AutoEndBkup	This attribute is not enabled for this release. Accept the default setting.
MonitorOption	Monitor options for the Oracle instance. This attribute can take values 0 or 1. ■ 0 - Process check monitoring (recommended) ■ 1 - Health check monitoring Default: 0 See "Agent functions" on page 157. Type and dimension: integer-scalar

Table 11-2 Optional attributes for Oracle agent

Optional Attributes	Definition
DetailMonitor	Setting this flag to a non-zero enables detail monitoring for Oracle. The value indicates the number of monitor cycles after which the agent will monitor Oracle in detail. For example, the value 5 indicates that the agent will monitor Oracle in detail every five monitor intervals. Default: 0 Type and dimension: integer-scalar
MonScript	Pathname to the script provided for detail monitoring. The default (basic monitoring) is to monitor the database PIDs only. **Note:** Detail monitoring is disabled if the value of the attribute MonScript is invalid or is set to an empty string. The pathname to the supplied detail monitor script is /opt/VRTSagents/ha/bin/Oracle/SqlTest.pl. MonScript also accepts a pathname relative to /opt/VRTSagents/ha. A relative pathname should start with "./", as in the path ./bin/Oracle/SqlTest.pl. Type and dimension: string-scalar
User	Internal database user. Connects to the database for detail monitoring. Type and dimension: string-scalar
Pword	Encrypted password for internal database-user authentication. Encrypt passwords only when entering them using the command-line. Passwords must be encrypted using the VCS Encrypt utility. Type and dimension: string-scalar
Table	Table for update by `User/Pword`. Type and dimension: string-scalar
Encoding	This attribute is not enabled for this release. Accept the default setting.
AgentDebug	Additional debug messages are logged when this flag is set. Default: 0 Type and dimension: boolean-scalar

Table 11-3 lists the internal attribute for Oracle agent. This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table 11-3 Internal attributes for Oracle agent

Optional Attributes	Definition
AgentDirectory	Specifies the location of binaries, scripts, and other files related to the Oracle agent. Default: /opt/VRTSagents/ha/bin/Oracle Type and dimension: static-string

Netlsnr attribute definitions

Table 11-4 lists the required attributes for Netlsnr agent.

Table 11-4 Required attributes for Netlsnr agent

Required attributes	Definition
Owner	Oracle user, as the defined owner of executables and database files in /etc/passwd. Type and dimension: string-scalar
Home	The $ORACLE_HOME path to Oracle binaries and configuration files. For example, you could specify the path as /opt/ora_home. Do not append a slash (/) at the end of the path. Type and dimension: string-scalar

Table 11-5 lists the optional attributes for Netlsnr agent.

Table 11-5 Optional attributes for Netlsnr agent

Optional attributes	Definition
TnsAdmin	The $TNS_ADMIN path to directory in which the Listener configuration file resides (listener.ora). Default: /var/opt/oracle Type and dimension: string-scalar

Table 11-5 Optional attributes for Netlsnr agent

Optional attributes	Definition
Listener	Name of Listener. The name for Listener is considered case-insensitive by the Netlsnr agent and the Oracle database server. Default: LISTENER Type and dimension: string-scalar
LsnrPwd	The VCS encrypted password used to stop and monitor the listener. This password is set in the Listener configuration file. Encrypt passwords only when entering them using the command-line. Passwords must be encrypted using the VCS Encrypt utility. Type and dimension: string-scalar
EnvFile	Specifies the full path name of the file that is sourced by the entry point scripts. This file contains the environment variables set by the user for the Oracle listener environment such as LD_LIBRARY_PATH and so on. The syntax for the contents of the file depends on the login shell of Owner. This file must readable by Owner. The file must not contain any prompts for user input. Type and dimension: string-scalar
MonScript	Pathname to the script provided for detail monitoring. The default (basic monitoring) is to monitor the listener process only. **Note:** Detail monitoring is disabled if the value of the attribute MonScript is invalid or is set to an empty string. The pathname to the supplied detail monitoring script is /opt/VRTSagents/ha/bin/Netlsnr/LsnrTest.pl. MonScript also accepts a pathname relative to /opt/VRTSagents/ha. A relative pathname should start with "./", as in the path ./bin/Netlsnr/LsnrTest.pl. Type and dimension: string-scalar
Encoding	Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default: "" Type and dimension: string-scalar
AgentDebug	Additional debug messages are logged when this flag is set. Default: 0 Type and dimension: boolean

Table 11-6 lists the internal attribute for Netlsnr agent. This attribute is for internal use only. Symantec recommends not to modify the value of this attribute.

Table 11-6 Internal attributes for Netlsnr agent

Optional Attributes	Definition
AgentDirectory	Specifies the location of binaries, scripts, and other files related to the Netlsnr agent. Default: /opt/VRTSagents/ha/bin/Netlsnr Type and dimension: static-string

About the VCS agent for Apache Web server

The Apache Web server agent monitors the Apache server processes. The Apache Web server agent consists of resource type declarations and agent scripts. The Apache agent requires an IP resource for operation.

The agent can detect when Apache is brought down gracefully. When Apache is brought down gracefully, the agent does not trigger a resource fault even though Apache is down.

Agent functions

Monitor

Monitors the state of the Apache server. First it checks for the processes, next it can perform an optional state check.

State definitions

- ONLINE
  Indicates that the Apache server is running.
- OFFLINE
  Indicates that the Apache server is not running.
- UNKNOWN
  Indicates that a problem exists with the configuration.
- INTENTIONAL OFFLINE
  Indicates that the Apache server was stopped by administrative intervention. Note that the PidFile attribute must be set for the agent to detect the INTENTIONAL OFFLINE state.

Apache attribute definitions

Table 11-7 lists the required attributes for the VCS agent for Apache.

Table 11-7 Required attributes

Required attribute	Description

ConfigFile	Full path and file name of the main configuration file for the Apache server.
	Type and dimension: string-scalar
	Example: "/apache/server1/conf/httpd.conf"
	Make sure httpd process is started with the -f <http.conf> option. If the httpd process is not started with the specified option, modify the OPTIONS attribute in Apache startup file to specify full the path to the configuration file.
	For example, on RedHat Linux, with the default httpd installation, you can edit the /file etc/sysconfig/httpd.
	# httpd binary at startup, set OPTIONS here.
	OPTIONS="-f /etc/httpd/conf/httpd.conf"
	Set the ConfigFile attribute of the Apache agent to this configuration file.

httpdDir	Full path of the directory to the httpd binary file Type and dimension: string-scalar Example: "/apache/server1/bin"
HostName	Virtual host name that is assigned to the Apache server instance. The host name is used in second-level monitoring to establish a socket connection with the Apache HTTP server. Specify this attribute only if the SecondLevelMonitor is set to 1 (true). Type and dimension: string-scalar Example: "web1.veritas.com"

Table 11-7 Required attributes

Required attribute	Description
PidFile	The PidFile attribute sets the file to which the server records the process id of the daemon. The value of PidFile attribute must be the absolute path where the Apache instance records the pid. **Note:** You must specify the PidFile attribute to make use of the Intentional Offline feature.If you do not specify the value, the agent will not detect the INTENTIONAL OFFLINE state of the Apache instance. Instead, the agent would cause the resource to fault and invoke the clean entry point. Type and dimension: string-scalar Example: /var/run/httpd.pid
Port	Port number where the Apache HTTP server instance listens. The port number is used in second-level monitoring to establish a socket connection with the server. Specify this attribute only if SecondLevelMonitor is set to 1 (true). Type and dimension: integer-scalar Default: 80 Example: "80"
ResLogLevel	Controls the agent's logging detail for a specific instance of a resource. Values are: ■ ERROR: Logs error messages. ■ WARN: Logs error and warning messages. ■ INFO: Logs error, warning, and informational messages. ■ TRACE: Logs error, warning, informational, and trace messages. Trace logging is verbose. Use for initial configuration or troubleshooting. Type and dimension: string-scalar Default: INFO Example: "TRACE"
User	Account name the agent uses to execute the httpd program. If you do not specify this value, the agent executes httpd as the root user. Type and dimension: string-scalar Example: "apache1"

Table 11-8 lists the optional attributes for the VCS agent for Apache.

Table 11-8 Optional attributes

Optional attribute	Description
DirectiveAfter	A list of directives that httpd processes after reading the configuration file. Type and dimension: string-association Example: DirectiveAfter{} = { KeepAlive=On }
DirectiveBefore	A list of directives that httpd processes before it reads the configuration file. Type and dimension: string-association Example: DirectiveBefore{} = { User=nobody, Group=nobody }
EnableSSL	Set to 1 (true) to have the online agent function add support for SSL by including the option `-DSSL` in the start command. For example: `/usr/sbin/httpd -k start -DSSL` Set to 0 (false) it excludes the `-DSSL` option from the command. Type and dimension: boolean-scalar Default: 0 Example: "1"
EnvFile	Full path and file name of the file that is sourced prior to executing httpdDir/httpd. With Apache 2.0, the file *ServerRoot*/bin/envvars, which is supplied in most Apache 2.0 distributions, is commonly used to set the environment prior to executing httpd. Specifying this attribute is optional. If EnvFile is specified, the login shell for user root must be Bourne, Korn, or C shell. Type and dimension: string-scalar Example: "/apache/server1/bin/envvars"
SecondLevelMonitor	Enables second-level monitoring for the resource. Second-level monitoring is a deeper, more thorough state check of the Apache HTTP server performed by issuing an HTTP GET request on the web server's root directory. Valid attribute values are **1** (true) and **0** (false). Specifying this attribute is required. Type and dimension: boolean-scalar Default: 0 Example: "1"

Table 11-8 Optional attributes

Optional attribute	Description
SharedObjDir	Full path of the directory in which the Apache HTTP shared object files are located. Specifying this attribute is optional. It is used when the HTTP Server is compiled using the SHARED_CORE rule. If specified, the directory is passed to the -R option when executing the httpd program. Refer to the httpd man pages for more information about the -R option. Type and dimension: boolean-scalar Example: "/apache/server1/libexec"
SecondLevelTimeout	Number of seconds monitor entry point will wait on the execution of second-level monitor. If the second-level monitor program does not return to the calling monitor entry point before the SecondLevelTimeout window expires, the monitor entry point will no longer block on the program sub-process but will report that the resource is offline. The value should be sufficiently high to allow second level monitor enough time to complete, but the value should also be less than the value specified by the agent's MonitorTimeout. Type and dimension: integer-scalar Default: 30

About the Application agent

The Application agent brings applications online, takes them offline, and monitors their status. It enables you to specify different executables for the online, offline, and monitor routines, because most applications have executables to start and stop the application. The executables must exist locally on each node.

An application runs in the default context of root. Specify the user name to run an application in a user context.

The agent starts and stops the application with user-specified programs.

You can monitor the application in the following ways:

- Use the monitor program
- Specify a list of processes
- Specify a list of process ID files
- Any combination of the above

Dependencies

Depending on how you plan to use it, this type of resource can depend on IP, IPMultiNIC, and Mount resources.

Agent functions

- Online
  Runs the StartProgram with the specified parameters in the context of the specified user.
- Offline
  Runs the StopProgram with the specified parameters in the context of the specified user.
- Monitor
  If you specify the MonitorProgram, the agent executes the user-defined MonitorProgram in the user-specified context. If you specify PidFiles, the routine verifies that the process ID found in each listed file is running. If you specify MonitorProcesses, the routine verifies that each listed process is running in the context you specify.
  Use any one, two, or three of these attributes to monitor the application.
  If any one process specified in either PidFiles or MonitorProcesses is determined not to be running, the monitor returns OFFLINE. If the process terminates ungracefully, the monitor returns OFFLINE and failover occurs.
- Clean
  Terminates processes specified in PidFiles or MonitorProcesses. Ensures that only those processes (specified in MonitorProcesses) running with the user ID specified in the User attribute are killed. If the CleanProgram is defined, the agent executes the CleanProgram.

State definitions

- ONLINE
  Indicates that all processes specified in PidFiles and MonitorProcesses are running and that the MonitorProgram returns ONLINE.
- OFFLINE
  Indicates that at least one process specified in PidFiles or MonitorProcesses is not running, or that the MonitorProgram returns OFFLINE.
- UNKNOWN
  Indicates an indeterminable application state or invalid configuration.

Application attribute definitions

Table 11-9 lists the required attributes for the VCS agent for the Application agent.

Table 11-9 Required attributes

Required attribute	Description
StartProgram	The executable, created locally on each node, which starts the application. Specify the complete path of the executable. Applicable command line arguments follow the name of the executable and are separated by spaces. Type and dimension: string-scalar Example: "/usr/sbin/samba start"
StopProgram	The executable, created locally on each node, that stops the application. Specify the complete path of the executable. Applicable command line arguments follow the name of the executable and are separated by spaces. Type and dimension: string-scalar Example: "/usr/sbin/sample_app stop"
At least one of the following attributes: ■ MonitorProcesses ■ MonitorProgram ■ PidFiles	See "Optional attributes" on page 170.

Table 11-9 lists the optional attributes for the VCS agent for the Application agent.

Table 11-10 Optional attributes

Optional attribute	Description
CleanProgram	The executable, created locally on each node, which forcibly stops the application. Specify the complete path of the executable. Applicable command line arguments follow the name of the executable and are separated by spaces. Type and dimension: string-scalar
MonitorProcesses	A list of processes that you want monitored and cleaned. Each process name is the name of an executable. Qualify the executable name with its complete path if the path starts the executable. The process name must be the name displayed by the `ps -ef` command for the process. Type and dimension: string-vector Example: "nmbd"
MonitorProgram	The executable, created locally on each node, which monitors the application. Specify the complete path of the executable. Applicable command line arguments follow the name of the executable and are separated by spaces. MonitorProgram can return the following VCSAgResState values: OFFLINE value is 100; ONLINE values range from 101 to 110 (depending on the confidence level); 110 equals confidence level of 100%. Any other value = UNKNOWN. Type and dimension: string-scalar

Table 11-10 Optional attributes

Optional attribute	Description
PidFiles	A list of PID files that contain the process ID (PID) of the processes that you want monitored and cleaned. These are application generated files. Each PID file contains one monitored PID. Specify the complete path of each PID file in the list. The process ID can change when the process restarts. If the application takes time to update the PID file, the agent's monitor script may return an incorrect result. If this occurs, increase the ToleranceLimit in the resource definition. Type and dimension: string-vector
User	The user ID for running StartProgram, StopProgram, MonitorProgram, and CleanProgram. The processes specified in the MonitorProcesses list must run in the context of the specified user. Monitor checks the processes to make sure they run in this context. Type and dimension: string-scalar Default: root

Installing the applications

Install the application on the virtual machine. This is the application that you want VCS to monitor in the virtual machine. See the documentation for the application for instructions.

It is very important to set up the applications to automatically start when the virtual machine starts. You do this as VCS only monitors the applications. It does not start or stop the applications. In case of fail over, VCS moves the entire virtual machine. When the virtual machine starts on the other node, the application must start when the virtual machine boots.

Installing the Veritas Virtual Machine Toolkit

Install the Veritas Virtual Machine Toolkit on a Linux virtual machine where you want to monitor an application for high availability. The toolkit contains different programs that enable high availability and monitoring tools. To access the toolkit installer, you can either use VVM or request the ESX administrator for the installer specifying your Linux operating system. You can use VVM to mount the .iso.

See "Using Veritas Virtualization Manager to configure virtual machines for disaster recovery" on page 147.

Mounting the Veritas Virtual Machine Toolkit ISO file to a virtual machine

VVM can make the Veritas Virtual Machine Toolkit available to you for easy access.

To add the toolkit .iso file

1. From a Windows client, click **Start** > **Programs** > **Veritas** > **Veritas Virtualization Manager**.
2. Right-click the virtual machine where you want to add the .iso file. Select **Add ISO Image**. VVM automatically selects the proper .iso file to match the operating system in the virtual machine.
3. The Add CD-ROM ISO window displays:
   - The name of the virtual machine
   - The guest operating system's IP address
   - The type of guest operating system
   - The file's location and name
4. Click the **OK** button to add the .iso file.

The .iso file is now available for your use.

Installing and configuring the Veritas Virtual Machine Toolkit on the virtual machine

Before you install the Veritas Virtual Machine Toolkit, prepare the following information:

- The virtual IP address for the cluster.
- The username and password required to administer the service group.
- The cluster's service group name.
- The location of the pagefile.

You must also make sure that you have mounted the .iso file for the virtual machine.

Installing the Veritas Virtual Machine Toolkit

You must install the toolkit.

To install the Veritas Virtual Machine Toolkit

1. Navigate to the installer location.
   ```
   cd /media/cdrom/installvcsvm-tools
   ```
2. On the virtual machine, enter the `installvcsvm-tools` command.
   ```
   ./installvcsvm-tools
   ```
3. Answer `y` when you are asked if you want to install the toolkit.
4. When you are asked to configure the application:
   - Answer **`y`** if you are ready to proceed with configuration.
   - Answer **`n`** if you want to return to configure the toolkit installer at a later time.

Configuring the Veritas Virtual Machine Toolkit

You must now configure the Veritas Virtual Machine Toolkit.

To configure the Veritas Virtual Machine Toolkit

1. On the virtual machine, enter the `vcsvm-tools -c` command.
   ```
   ./vcsvm-tools -c
   ```
   On a virtual machine that already has the toolkit mounted, use the full path for the command. At the prompt, enter:
   ```
   /opt/VRTSvcs/bin/vcsvm-tools -c
   ```
2. When asked if you are ready to configure the toolkit, answer **`y`**.
3. Enter the virtual IP address of the VCS cluster that the virtual machine belongs to.

4 Enter the username and password for the cluster that the virtual machine belongs to. This is the same administrator that you created when you configured the virtual machine for high availability or disaster recovery.
   - See "To configure a virtual machine for high availability" on page 129.
   - See "To configure a virtual machine for disaster recovery" on page 147.

5 Enter the service group name that the virtual machine belongs to.

6 Enter the device path for location of the pagefile datastore on the secondary storage device.

The Veritas Virtual Machine Toolkit installation program is now complete. You must now perform post-installation tasks and configure the your highly available resources.

Validating the configuration of the Veritas Virtual Machine Toolkit

You can verify that the toolkit is properly configured.

To validate the toolkit's configuration

1 Get the virtual machine resource's name, which is in the file /etc/VRTSvcs/.vcsvmresname. To get the name, type:

```
# cat /etc/VRTSvcs/.vcsvmresname
```

Warning: Ensure that the .vcsvmresname file does not get deleted. This file is critical to convey application faults to the ESX layer.

2 Use the virtual machine resource's name to run the following command and make sure that the command completes. At the prompt, type:

```
# /opt/VRTSvcs/bin/hares -value vmres_name Type
```

Where vmres_name is the virtual machine resource's name.

3 Again use the virtual machine resource's name and run the following command:

```
# /opt/VRTSvcs/bin/hares -state vmres_name
```

Where vmres_name is the virtual machine resource's name.

Configuring application monitoring

After you have installed the Veritas Virtual Machine Toolkit, you can configure resources within a virtual machine. You use the resource configuration (vcsag_config.pl) program to configuring the resources inside virtual machines.

Before you run the resource configuration program, make sure you review the attributes for the agent that you want to configure. The following list has links to those sections:

- See "Oracle attribute definitions" on page 158.
- See "Netlsnr attribute definitions" on page 161.
- See "Apache attribute definitions" on page 164.
- See "Application attribute definitions" on page 169.

Prerequisites

These prerequisites are to make sure the high availability setup in the virtual machine is correct. Before you start ensure that:

- Before you configure your applications on the virtual machine, ensure that they are running.
- Each virtual machine has VMware Tools installed on it.
- The guestinfo interfaces of the VMware Virtual Machine tools are enabled.
- The virtual machine or application administrator has VCS privileges to configure and fine-tune the application resources.
- The ESX Server administrator has provided the username and password credentials for the service group to the virtual machine or application administrator.
- It is very important to set up the applications to automatically start when the virtual machine starts. You do this as VCS only monitors the applications. It does not start or stop the applications. In case of fail over, VCS moves the entire virtual machine.

Configuring resources inside virtual machines

You need to configure the resources for the applications that you want to monitor inside the virtual machine.

To configure the resources that agents monitor inside of virtual machines

1. In the virtual machine, change directory to /opt/VRTSvcs/bin.
2. To start the configuration program, enter the command:
   `./vcsag_config.pl`
3. Enter the name of the application that you want to monitor. Your choices are:
   - **`Oracle`**
   - **`Netlsnr`**
   - **`Apache`**
   - **`Application`**

   The program lists the resources that are configured for that application. If you have no configured resources, it displays a message.
4. To reconfigure or delete an existing resource, enter the name of the resource from the list.
5. Enter a new name to configure a new resource for that application type.
6. When prompted, enter a value for each attribute. You need to enter these values in the formats requested. The following list defines these formats.

string	String values can include any character. If you use a space character in the string, you must enclose the string within double-quotes. You can use two double-quotes to represent an empty string.
integer	Integer values include the numbers 0 through 9.
boolean	Boolean values include 0 and 1. Zero is false, or off. One is true, or on.

association — Association values are pairs of keys and their values. The keys are always strings, while the data types of the values are provided by the association's data type. All key value pairs are separated by spaces.

Two kinds of association data types exist, they are as follows:

- Integer association—in this kind of association, values must be integers.
- String association—in this kind of association, values are strings.

Examples:

- keyA 1 keyB 3 0 2
  In this integer association, keyA, keyB, and 0 are the keys.
- keyA valA keyB valB keyC valC
  In this string association, keyA, keyB, and keyC are the keys.

vector — A vector is an ordered list of values. Each value is indexed using a positive integer beginning with zero.

7 Enter information for each attribute.

- See "Oracle attribute definitions" on page 158.
- See "Netlsnr attribute definitions" on page 161.
- See "Apache attribute definitions" on page 164.
- See "Application attribute definitions" on page 169.

8 When you are done, enter **done** to end the configuration for that resource type.

9 You can now choose to configure more types, or end the configuration tasks. Enter **done**, which:

- Saves the final configuration.
- Sets up the corresponding configuration on the ESX Server node.
- Restarts the VCS agent management daemon (vcsagmd), which applies the configuration on the virtual machine. The daemon starts the agents on the virtual machine for the resource types that you have configured. It also starts the GrowFS and VMIP agent processes for the virtual machine, which are used for internal purposes.

10 If for any reason step 9 does not complete, you can apply the changes to the configuration by running the vcsag_config.pl program with the -apply option, as follows:

```
# /opt/VRTSvcs/bin/vcsag_config.pl -apply
```

Verifying that the applications are running

You can verify if the application is now running. A simple test is to check for the process.

```
# ps -ef| grep agentname
```

Grep for the agent names oracle or netlsnr.

Applying the configuration and creating the corresponding GuestOSApp resource

After have have configured an application in the virtual machine, the resource configuration program (vcsag_config.pl) or the wizard adds the corresponding resources of type GuestOSApp to the configuration on the node. The resource configuration program or the wizard also restarts the VCS Agent Management Deaemon (vcsagmd) on the virtual machine. This restart applies the newly created configuration inside the virtual machine. The GuestOSApp agent on the node then listens for updates on the corresponding application resources that are configured inside the virtual machine.

Deploying custom agents on virtual machines running Linux

This section describes how to deploy custom agents in a virtual machine running Linux.

VCS does not support detecting an intentional offline for applications monitored by custom agents.

To deploy a custom agent in a virtual machine running Linux

1. Build the custom agent. See the *Veritas Cluster Server Agent Developer's Guide* for detailed information on agent development.
   - Symantec recommends the following naming convention for the agent binary:
     `resource_type`*`Agent`*
   - Place the agent in the following directory:
     `/opt/VRTSvcs/bin/`*`resource_type`*`.`

   For example, the agent binary for the CustomApp agent would be:
   `/opt/VRTSvcs/bin/CustomApp/CustomAppAgent`

2 Implement the Monitor and Clean entry points for the agent. Agents running in a virtual machine do not use the Online and Offline entry points.

- If you implement the entry points using scripts, name the scripts `online` and `clean`.
- Build the Clean script such that it returns 0.

```
#!/bin/sh
exit 0;
```

- Place the script files in the following directory:

`/opt/VRTSvcs/bin/`*`resource_type/`*

For example:

```
/opt/VRTSvcs/bin/CustomApp/online
/opt/VRTSvcs/bin/CustomApp/clean
```

3 The agent requires a resource type definition file. Name the resource type definition file using following the convention

`resource_type``Types.cf`.

For example:

`CustomAppTypes.cf`

4 Populate the types file with the following information:

- The name of the agent
- The attributes associated with the resource type, their names, types, and dimensions
- The ArgList attribute, its data type, dimension, and its values. The ArgList value lists the other attributes of the resource.

  For example:

```
// Define the resource type called FileOnOff (in
FileOnOffTypes.cf).
type FileOnOff (
str PathName;
static str ArgList[] = { PathName };
)
```

5 Create an XML file for the agent. Name the file *resource_type*.XML. For more information, see the *Veritas Cluster Server Agent Developer's Guide*.

6 Copy the existing types. cf file (/opt/VRTSvcs/conf/config/types.cf) to a different location on the virtual machine.

7 Edit the copied file to add the types information about the custom agent. Copy the contents of the file CustomAppTypes.cf to the types.cf file.

8 Verify the syntax of the updated file.

- Copy the updated types.cf file to a directory (*config_directory*) on an ESX Server that is part of the VCS cluster.

- Create a main.cf file in the same directory. In the main.cf file, add the following line:
  ```
  include "types.cf"
  ```
- Run the following command:
  ```
  hacf -verify config_directory
  ```
  The variable *config_directory* refers the directory containing the types.cf file and the main.cf file.
  No error message and a return value of zero indicates that the syntax is valid.

9 If the syntax is valid, replace the current types.cf on the virtual machine with the updated file.

10 Before configuring the agent to start monitoring the application:
- Make sure the application is running.
- Make sure the application is configured to automatically start when the virtual machine starts.

11 In the virtual machine, navigate to /opt/VRTSvcs/bin.

12 Start the configuration utility:
```
./vcsag_config.pl
```

13 Follow the prompts to complete the agent configuration.
The utility restarts the VCS agent management daemon to start monitoring the application.
The utility also configures a resource of type GuestOSApp on the ESX Server. The resource listens for updates on the state of application running inside the virtual machine.

How VCS monitors the application on the virtual machine running Linux

The VCS agent management daemon manages the agents that monitor the applications that are inside of the virtual machine. The daemon notifies VCS on the ESX layer if the application faults. VCS on the ESX layer takes decisions on failover depending on your resource configuration.

Removing the Veritas Virtual Machine Toolkit

To remove the Veritas Virtual Machine Toolkit

1. On the virtual machine where you want to remove the toolkit, enter the command `vcsvm-tools -u`.

   ```
   vcsvm-tools -u
   ```

2. When asked if you are ready to uninstall the toolkit, answer **y**.

The uninstallation program displays the location of the log files after the uninstallation is complete.

Chapter 12

Deploying VCS components on virtual machines running Windows

This chapter contains the following topics:

About VCS components on virtual machines running Windows

Using VMware with its ESX Server, you can cluster virtual machines using a Windows guest operating system as a vehicle for applications and high availability software, such as Microsoft SQL Server and Microsoft Internet Information Services (IIS).

Using components of Veritas Cluster Server (VCS), called the Veritas Virtual Machine Toolkit, you can create a cluster that spans physical servers, where a node in a virtual machine on a single ESX Server can fail over to another physical ESX server.

Prerequisites

- Each guest operating system must have VMware Tools installed on it.
- The guestinfo interfaces of the VMware Virtual Machine tools must be enabled.
- The Veritas Virtual Machine Toolkit must be installed on a virtual machine running Windows.
- The virtual machine or application administrator needs VCS privileges to configure and fine-tune the application resources.
- The ESX Server administrator needs to provide the username and password credentials for the service group to the virtual machine or application administrator.

Software requirements

To successfully cluster Windows nodes, the systems must meet minimum requirements of each to run these clusters.

Note: The GrowFS function is not supported on Windows.

Guest systems

- Windows 2000 Server or Advanced Server with Service Pack 4
  or
  Windows Server 2003: Standard Edition or Enterprise Edition (SP1 required)
- Microsoft .NET Framework version 1.1 with SP1 or higher

- Veritas Virtual Machine Toolkit
- VMware Tools

SQL Server

- Microsoft SQL servers and their operating systems. Note that all systems must be running the same operating system:
  - Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (both require SP4)
    with
    Windows Server 2003: Standard Edition or Enterprise Edition (SP1 required)
    or
    Windows 2000 Server or Windows 2000 Advanced Server (both require SP4)

  or

  - Microsoft SQL Server 2005, 32-bit (SP1 required)
    with
    Windows Server 2003: Enterprise Edition (SP1 required)

Note: Microsoft SQL Server 2000 and Microsoft SQL Server 2005 can exist in the same cluster but cannot operate on or fail over to the same system. If you use both applications in a cluster, select a distinct set of systems for the SystemList attribute of each application's service group.

Installing components

When installing each component, install in the following order:

- Windows guest operating system
  If you plan to monitor IIS, once you have installed Windows, enable IIS as follows:
  - In Control panel, select **Administrative Tools > Services > IIS Admin Services**.
  - Right-click **IIS Admin Services** and click **Start**.
  - IIS is now enabled.

- Microsoft .NET Framework version 1.1 with SP1 or higher (required by both the SQL Server Configuration Wizard and IIS wizard)
  The .NET Framework is installed as part of Windows Server 2003, but not for Windows Server 2000. If the .NET Framework is not installed, download it from the Microsoft Web site.
- SQL Server
  During SQL Server installation, point the database files to an extra volume that you have created in shared storage.

Refer to the Microsoft documentation for complete instructions on installing Windows and SQL Server.

Installing the Veritas Virtual Machine Toolkit

Install the Veritas Virtual Machine Toolkit on a Windows virtual machine where you want to monitor an application for high availability. The utility is on the disc inside the vcsvm_tools directory. It is in the ISO format as win-x86-vcsvm-tools.iso.

To add the toolkit .iso file

1. From a Windows client, click **Start** > **Programs** > **Veritas** > **Veritas Virtualization Manager**.
2. Right-click the virtual machine where you want to add the .iso file. Select **Add ISO Image**. VVM automatically selects the proper .iso file to match the operating system.
3. The Add CD-ROM ISO window displays:
   - The name of the virtual machine
   - The guest operating system's IP address
   - The type of guest operating system
   - The file's location and name
4. Click the **OK** button to add the .iso file.

The ISO file is now available for your use.

To install the Virtual Machine Toolkit

1. Once you have mounted the appropriate ISO file to your virtual machine, run the vcsvm-tools.exe file to install the toolkit.
2. Review the Welcome screen and click **Next**.
3. Review the License Agreement, choose to accept, and then click **Next**.

4 In the Destination Folder screen, either accept the default location or click **Browse** to choose another location. Click **Next** when done.

5 In the Halogin Configuration screen, enter the cluster login credentials. You must configure halogin before running the SQL and IIS agent wizards; otherwise, the wizards won't be able to complete the configuration.

- IP address or DNS name of your VCS ESX cluster
- User name and password for your VCS ESX cluster
- VCS virtual machine resource associated with this system

6 Click **Next**.

7 In the Convert Basic Disks to Dynamic screen, only check the box if you have basic disks that you need to convert to dynamic disks. Make sure that if you have any volumes mounted on a basic disk, unmount the volumes before converting the disks to dynamic.
Note that this applies for Windows 2003 users only, as Windows 2000 users won't see this screen.
Click **Next** when done.

8 In the PageFile Drive Selection screen, you are presented with a list of available drives, the size and type of the pagefile if present, and the available space on the drive.
Select a drive and

- delete the pagefile, if it exists on a replicated volume. Click **Delete Pagefile**.
- create a pagefile. You can choose to either create a Custom pagefile or a System-managed pagefile.
  For a custom pagefile, you must enter the initial size (in MB) and the maximum size (in MB), and then click **Create**. Note that the maximum size is constrained by the Windows maximum size limit of 4096 MB.
  or
  Check the System Managed check box and click **Create**.

Click **Next** when done.

9 In the Ready to Install screen, click **Install**.

10 Click **Finish** to close the installer.

11 Verify the installation. Check to see if the VCSAgMD service is present in the Services panel. (Start > Programs > Administrative Tools > Services)

Configuring the Veritas Virtual Machine Toolkit

If you skipped the configuration of the toolkit, you can return to configure it.

To configure the Veritas Virtual Machine Toolkit

1. On the virtual machine, open the **Control Panel** and go to **Add or Remove Programs**.
2. Select the **Veritas Virtual Machine Toolkit** and click the **Change** button.
3. Click the **Next** button.
4. Select the **Modify** radio button and click the **Next** button.
5. In the Halogin Configuration screen, enter the cluster login credentials. You must configure halogin before running the SQL and IIS agent wizards; otherwise, the wizards won't be able to complete the configuration.
   - IP address or DNS name of your VCS ESX cluster
   - User name and password for your VCS ESX cluster
   - VCS virtual machine resource associated with this system
6. Click **Next**.
7. In the Convert Basic Disks to Dynamic screen, only check the box if you have basic disks that you need to convert to dynamic disks. Make sure that if you have any volumes mounted on a basic disk, unmount the volumes before converting the disks to dynamic.
   Note that this applies for Windows 2003 users only, as Windows 2000 users won't see this screen.
   Click **Next** when done.
8. In the PageFile Drive Selection screen, you are presented with a list of available drives, the size and type of the pagefile if present, and the available space on the drive.
   Select a drive and
   - delete the pagefile, if it exists on a replicated volume. Click **Delete Pagefile**.
   - create a pagefile. You can choose to either create a Custom pagefile or a System-managed pagefile.
     For a custom pagefile, you must enter the initial size (in MB) and the maximum size (in MB), and then click **Create**. Note that the maximum size is constrained by the Windows maximum size limit of 4096 MB.
     or
     Check the System Managed check box and click **Create**.

   Click **Next** when done.

9 In the Ready to Install screen, click **Install**.

10 Click **Finish** to close the installer.

11 Verify the configuration. Check to see if the VCSAgMD service is present in the Services panel. (Start > Programs > Administrative Tools > Services)

Validating the configuration of the Veritas Virtual Machine Toolkit

Use the following procedure to verify that the toolkit is properly configured.

To validate the Virtual Machine Toolkit configuration

1 Get the virtual machine resource name, which is in the file $VCS_HOME\.vcsvmresname. Typically, you can find the .vcsvmresname file in the C:\Program Files\Veritas\cluster server\. To get the name, type the following:

```
C:\Program Files\Veritas\cluster server\.vcsvmresname
```

Warning: Ensure that the .vcsvmresname file does not get deleted. This file is critical to convey application faults to the ESX layer.

2 Use the virtual machine resource name to run the following command and make sure that the command completes. At the prompt, type:

```
C:\Program Files\Veritas\cluster server\hares -value
vmres_name Type
```

Where vmres_name is the virtual machine resource name.

3 Again, use the virtual machine resource name and run the following command:

```
C:\Program Files\Veritas\cluster server\hares -state
vmres_name
```

Where vmres_name is the virtual machine resource name.

About the SQL Server agents

Microsoft SQL Server is a relational database management system (RDBMS) used for building, managing, and deploying business applications. The SQL Server infrastructure provides services such as jobs, notification, and in-built replication.

The SQL Server agents monitor Microsoft SQL Server and its services on a VCS cluster to ensure high availability. VCS provides separate agents for SQL Server 2000 and SQL Server 2005.

The agents can detect when the SQL Server is brought down gracefully. When the SQL Server is brought down gracefully, the agents do not trigger a resource fault even though the SQL Server is down.

Agents for SQL Server 2000 and SQL Server 2005

The SQL agents are as follows:

- **Agent for SQL Server 2000 service**. The agent monitors SQL Server 2000 service.
- **Agent for SQL Server 2005 service**. The agent monitors SQL Server 2005 service.
- **Agent for SQL Server 2005 Agent service**. The agent monitors SQL Server 2005 agent service.
- **Agent for SQL Server 2005 Analysis service**. The agent monitors SQL Server 2005 Analysis service.
- **Agent for SQL Server 2005 Search service**. The agent provides high availability for full-text search indices with a clustered SQL instance.

SQL Server agent functions (entry points)

- Monitor-Verifies the configured SQL Server instance is running.

SQL Server state definitions

- ONLINE-Indicates the configured SQL Server instance is available.
- OFFLINE-Indicates the configured SQL Server instance is not available.
- UNKNOWN-Indicates the agent could not determine the status of SQL Server.
- INTENTIONAL OFFLINE-Indicates the SQL Server instance was stopped by administrative intervention.

Prerequisites

Make sure the following prerequisites have been met before running the wizard.

- Local administrator privileges are assigned to the user running the wizard.
- SQL Server 2000 or SQL Server 2005 are installed on the computer to be monitored.
- SQL Server and SQL Server Browser services for each instance must be online.

Configuring the SQL Server agents

The SQL Server agent can be configured using the SQL Server Configuration wizard.

Configuring the SQL Server Agent

1. Navigate to the configuration wizard by clicking **Start > Programs > Symantec > Veritas Cluster Server > Configuration Wizards > SQL Server Configuration Wizard**.
2. Review the Welcome screen and click **Next**.
3. In the Instance Selection screen, select the SQL Server instance or instances that you want to monitor. By default, once you have selected a SQL Server 2005 instance, the boxes under the Search, SQLAgent, and Analysis fields are selected. You can deselect any of these fields if you do not want that agent monitoring the corresponding SQL Server service. If you select a SQL Server 2000 instance, no fields are displayed.
   The Instance Selection screen in the SQL Server Agent Configuration Wizard corresponds to the Microsoft SQL Server services as follows.

   Table 12-1 List of SQL Server services and agents in Instance Selection screen

Microsoft SQL Server Services	SQL Server Agents
SQL Server [instance name] Is either SQL Server 2000 or 2005	SQL Server (2000 or 2005) instance selected for monitoring
SQL Server (2005) Full-Text Search Creates full-text indexes on content and properties of structured and semi-structured data	Search Monitors the SQL Server Full-Text Search function
SQL Server (2005) Agent Executes jobs, monitors SQL Server, fires alerts, and allows some automation of administrative functions	SQLAgent Monitors the SQL Server Agent
SQL Server (2005) Analysis Services Provides online analytical processing (OLAP) and data mining functionality	Analysis Monitors the Server Analysis Services

4. Select **Configure detailed monitoring for selected instances** to enable detailed monitoring of the selected agents.

5 When you have selected all of the SQL Server instances that you wish to monitor, click **Next**.
If you have selected detailed monitoring for the SQL Server instance, the Detailed Monitoring screen appears.

6 From the SQL Instance List, select an instance and specify the path name, if different from the default path name given.

7 Specify whether you want to logon as the local system account (default) or as a domain account. If you choose to logon as a domain account, you need to enter your username, password, and domain information. Click **Apply**.

8 If you have more than one instance in the list, repeat this step for each instance, and click **Apply** after each selection.
Note that if you do not apply a path name to an instance, you get an error message that reminds you to specify the path name for that instance.

9 When you have finished, click **Next**. The Failure Actions screen appears.
The Failure Action screen lists the Microsoft SQL Server Services that you have chosen to monitor (in step 3).

Table 12-2 List of chosen SQL Server services

Service Name	Description
SQL Server [instance name]	Provides storage, processing and controlled access of data...
SQL Server Full Text Search	Quickly creates full-text indexes on content...
SQL Server Analysis Services	Supplies online analytical processing (OLAP)...
SQL Server Agent	Executes jobs, monitors SQL Server, and fires alerts

10 Double-click one of the Services to open the Recovery Action dialog box. Specify the action to take after the first failure, the second failure, and subsequent failures. The options are:

- Take no action (default for all three)
- Restart the Service
- Run a Script

11 Specify when to reset the fail count (after 1 day is the default value).

12 Specify the script path name. You can accept the default value, or click **Browse** to select a different path name.

13 Enter any command line parameters in the text box (optional) and click **OK**. You are returned to the Failure Actions screen.

14 Repeat step 10 through step 13 for each of the Services listed. Click **Next** when you are done.

15 The Resource Summary page lists the agents, or resources, you have selected: [Instance name]_SQLServer, [Instance name]_SearchService, [Instance name]_SQLAgService, and [Instance name]_SQLAnalysisService.
Select a resource and click it to view its attributes.
In this window, you can rename the resources that you have created. Make sure that these resource names match the GuestOSApp resources that will be monitored at the ESX cluster level.

16 When you are done reviewing the resources, click **Next**.

17 Click **Finish** to close the configuration wizard.

About the Internet Information Services agent

The Internet Information Services (IIS) agent monitors the status of sites configured using IIS 5.0 and 6.0.

The agent provides two ways of monitoring application pools associated with IIS Web sites:

- One IIS resource configures a Web site and sets monitoring options for application pools associated with the site
- One IIS resource configures a Web site; other resources configure individual application pools.

The agent can detect when IIS is brought down gracefully. When the IIS is brought down gracefully, the agent does not trigger a resource fault even though IIS is down.

IIS agent functions (entry points)

- Monitor-Verifies the configured sites or application pools are running.

IIS agent state definitions

- ONLINE-Indicates the configured site or application pool is available.
- OFFLINE-Indicates the configured site or application pool is not available.
- UNKNOWN-Indicates the agent could not determine the status of the resource.
- INTENTIONAL OFFLINE-Indicates the application was stopped by administrative intervention.

Resource type definition

```
type IIS (
    static i18nstr ArgList[] = {SiteType, SiteName,
    "IPResName:Address", PortNumber, AppPoolMon, DetailMonitor,
    DetailMonitorInterval }
    str SiteType
    i18nstr SiteName
    int PortNumber = 80
    str AppPoolMon = NONE
    boolean DetailMonitor = 0
    int DetailMonitorInterval = 5
    str IPResName
)
```

Attribute definitions

To configure the agent to monitor an application pool, configure the SiteType and SiteName attributes only. The agent ignores other attributes when it is configured to monitor an application pool.

Table 12-3 Required attributes

Required Attributes	Description
SiteType	Defines whether the resource is configured to monitor an IIS site or an application pool. If the resource is configured to monitor an application pool, set the attribute to APPPOOL. If the resource is configured to monitor an IIS site, set this attribute to the name of the IIS service associated with the site. The attribute can take any of the following values: ■ W3SVC ■ MSFTPSVC ■ SMTPSVC ■ NNTPSVC Type and dimension: string-scalar

Table 12-3 Required attributes

Required Attributes	Description
SiteName	The name of the IIS site, the virtual server, or the application pool to be monitored by the agent. The value of this attribute depends on that of the SiteType attribute. The SiteName attribute can take the following values: ■ The name of a site, if SiteType is W3SVC or MSFTPSVC ■ The name of a virtual server, if SiteType is SMTPSVC or NNTPSVC ■ The name of an application pool, if SiteType is APPPOOL **Note:** This attribute can take localized values. Type and dimension: string-scalar
IPResName	The name of the IP resource configured for the IP to which the site is bound. Type and dimension: string-scalar
PortNumber	The port to which the site is bound. Type and dimension: string-scalar

Table 12-4 Optional attributes

Optional Attributes	Description
AppPoolMon	Defines the monitoring modes for the application pool associated with the Web site being monitored. Configure this attribute only if SiteType is W3SVC and IIS is configured to run in the Worker Process Isolation mode. The attribute can take one of the following values: ■ **NONE**: Indicates that the agent will not monitor the application pool associated with the Web site. ■ **DEFAULT**: Indicates that the agent will monitor the *root* application pool associated with the Web site. If this attribute is set, the agent starts, stops, and monitors the root application pool associated with the Web site. If the root application pool is stopped externally, the agent fails over the service group. ■ **ALL**: Indicates the agent will start all application pools associated with the Web site, but will monitor and stop the *root* application pool only. Type and dimension: integer-scalar

Table 12-4 Optional attributes

Optional Attributes	Description
DetailMonitor	A flag that defines whether the agent monitors the site in detail. The value 1 indicates the agent will monitor each site in detail by attempting an actual socket connection to the port. Type and dimension: boolean-scalar
DetailMonitorInterval	The number of monitor cycles after which the agent attempts detail monitoring. For example, the value 5 indicates that the agent will monitor the resource in detail after every 5 monitor cycles. Type and dimension: integer-scalar

Prerequisites

Make sure the following prerequisites have been met before running the wizard.

- IP address must have a forward and reverse entry in the DNS.
- The Site Name for the site to be monitored must be unique.

Configuring the IIS agent

Use the following procedure to configure the IIS agent.

To configure the IIS agent

The IIS agent can be configured using the IIS Configuration wizard.

1 Navigate to the configuration wizard by clicking **Start > Programs > Symantec > Veritas Cluster Server > Configuration Wizards > IIS Configuration Wizard**.

1 Review the Welcome screen and click **Next**.

2 In the Configure IIS Sites screen, select the sites that you want to monitor. By default, all listed sites are selected. Note that when you deselect a site, the corresponding check box for detailed monitoring is also deselected.
The Site Name entries correspond to the resources listed under the IIS Manager in Windows Administrative Tools (Control Panel > Administrative Tools > IIS Manager). There are four services associated with the IIS Manager:
   - FTP sites
   - Web Sites

- Default SMTP Virtual Server
- Default NNTP Virtual Server

Each of the four services has resources, or sites, associated with it. For example, under Web Sites you could have Default Web Site, Administration, and Microsoft SharePoint.

3 For each selected site, type the IP address for that site. If you do not enter an IP address, an error message appears that prompts you to enter an IP address.

When you are done, click **Next**.

4 In the Application Pool Configuration screen, select the application pools that you want to monitor, if any. Using the drop-down list, select one of the following options and click **Next** when done:

- DEFAULT to monitor the root application pool.
- NONE for no application pool monitoring.
- ALL to monitor all application pools associated with the site.

5 The Failure Action screen lists the IIS services that you have chosen to monitor.

6 Double-click one of the sites to open the Recovery Action dialog box. Specify the action to take after the first failure, the second failure, and subsequent failures. The options are:

- Take no action (default for all three)
- Restart the Service
- Run a Script

7 Specify when to reset the fail count (after 1 day is the default value).

8 Specify the script path name. You can accept the default value, or click **Browse** to select a different path name.

9 Enter any command line parameters in the text box (optional) and click **OK**. You are returned to the Failure Actions screen.

10 Repeat step 6 through step 9 for each of the Sites listed. Click **Next** when you are done.

11 The Resource Summary page lists the sites, or resources, you have selected. Select a resource and click it to view its attributes.

In this window, you can rename the resources that you have created. Make sure that these resource names match the GuestOSApp resources that will be monitored at the ESX cluster level.

12 When you are done reviewing the resources, click **Next**.

13 Click **Finish** to close the configuration wizard.

Configuring a generic service

If you are using Windows services or applications other than SQL Server or IIS, you need to configure the Service Control Manager (SCM) settings for these generic services. The SCM notifies the ESX cluster if a Windows service stops.

Note: You must have already configured halogin during the toolkit installation before performing this task!

To configure SCM settings for a generic service

1. Click **Start** and select **Programs > Administrative Tools > Services**.
2. Select the service that you want to configure and right-click that service.
3. In the drop-down menu, click **Properties**. The Properties dialog box opens.
4. In the Properties dialog, click the **Recovery** tab.
5. Specify the action to take after the first failure, the second failure, and subsequent failures. The options are:
   - Take no action (default for all three)
   - Restart the Service
   - Run a Program
6. If you want to failover after the third failure, then choose **Run a Program** for subsequent failures.
7. Copy or type the following into your Program text box.
   `C:\program files\veritas\vrtsperl\bin\perl`

   If the Virtual Machine Toolkit is not installed in the default directory, note that you need to substitute `C:\program files\veritas\vrtsperl\bin\` with the value of the VRTS_PERL_BIN environment variable.
8. Enter the following command line parameters in the text box:
   `C:\program files\veritas\cluster server\bin\appstatechange.pl` *`[Windows service name]`* `ONLINE OFFLINE`

   For the *`<Windows service name>`* value, you can use any name that describes the application.
   If the virtual machine toolkit is not installed in the default directory, note that you need to substitute `C:\program files\veritas\cluster server` with the value of the VCS_HOME environment variable.

9 You can specify when to reset the fail count (0 days is the default value) and when to restart the service (1 minute is the default value).

10 Click **OK** to close the Properties dialog box.

11 Repeat these steps if you have more than one service that needs to be configured.

12 For each service configured, create a corresponding GuestOSApp resource on the ESX cluster.

- Name the resource using the following convention:
  [Windows service name]_Virtual machine resource name
  The virtual machine resource name is the one you entered in the Halogin Configuration screen.
- Give this GuestOSApp resource name to the ESX administrator, who will create this resource on the ESX server, and then online the resource.

Applying the configuration and creating the corresponding GuestOSApp resource

After configuring the application in the virtual machine, you must update the VCS configuration on the ESX server. For each application configured as a VCS resource in the virtual machine, you must add a resource of type GuestOSApp to the configuration on the ESX server. The GuestOSApp agent then listens for updates on the corresponding application resource configured inside the virtual machine. The agent enables virtual machine failover when an application in the virtual machine faults.

If you use the wizard to configure a resource, VCS adds the corresponding resources of type GuestOSApp to the configuration on the ESX Server. VCS also restarts the VCS Agent Management Daemon (vcsagmd) on the virtual machine. This restart applies the newly created configuration.

If you configure a generic service using the Windows Service Control Manager, an ESX administrator must add a resource of type GuestOSApp to the configuration on the ESX server.

To manually configure the GuestOSApp resource on the ESX server

1 On the ESX Server, edit the service group that contains the virtual machine configuration.

2 For each service configured using Service Control Manager in the virtual machine, add a resource of type GuestOSApp to the service group.

3 Make sure that the name of the GuestOSApp resource uses the following naming convention:

ServiceName_ESXVirtualMachineResourceName

4 If you want the virtual machine to fail over when the application faults, set the Critical attribute of the GuestOSApp resource to 1.

Verifying the configuration for application monitoring

You can verify your VCS configuration for application monitoring by opening the log file and checking the state of the resource (such as SQL Server or IIS) being logged. The states are:

- ONLINE-Indicates the configured site or application pool is available.
- OFFLINE-Indicates the configured site or application pool is not available.
- UNKNOWN-Indicates the agent could not determine the status of the resource.
- INTENTIONAL OFFLINE-Indicates the application was stopped by administrative intervention.

Example
```
2006/09/27 16:01:15 VCS INFO V-16-2-50017
Resource(VMIP) is in UNKNOWN state
```

Example
```
2006/09/27 16:01:18 VCS INFO V-16-2-13352
Resource(PRSPOOL) is ONLINE
```

Removing the Veritas Virtual Machine Toolkit from the virtual machine running Windows

This section describes steps for uninstalling the Veritas Virtual Machine Toolkit.

1 Open the Windows Control Panel and click **Add or Remove Programs**.

2 Select Veritas Virtual Machine Toolkit and click **Remove**.

3 When asked if you are sure you want to remove the program, click **Yes**.

4 The installer displays the status of uninstallation. When the removal of the Veritas Virtual Machine Toolkit is complete, you can close the Add or Remove Programs screen.

Appendix A

Advanced topics

This chapter contains the following topics:

Increasing allocated storage

You can increase the amount of application datastore storage that you have allocated for use with a virtual machine.

Different operating systems can grow storage on different files systems, for more information on supported file systems:

See "Supported guest operating systems" on page 28.

Prerequisites

- The virtual machine must be configured for VCS.
- The VMware Tools must be installed in the virtual machine.
- The Veritas Virtual Machine Toolkit must be installed on the virtual machine.
- Existing disk space or file system space must be available to increase the storage, with:
  - Non-replicated disk space for virtual machines with high availability
  - Replicated disk space for virtual machines with disaster recovery
- For Linux file systems:
  - The storage must reside on an LVM logical volume
  - The tools to grow file systems (ext2online or resize_reiserfs) must be installed in the virtual machine
- For Windows systems, the disks you want to grow must be:
  - Dynamic disks
  - On the NTFS file system

Increasing storage

From a Windows client, start the Veritas Virtualization Manager.

To increase allocated storage

1. From a Windows client, click **Start** > **Programs** > **Veritas** > **Veritas Virtualization Manager**.
2. Enter the name of the VirtualCenter Server, your user name and password, and the full path to the SSL certificate. See "To provide the SSL certificate path information for VVM log in" on page 125.
3. Right-click the virtual machine where you want to increase storage. Select **Grow FS**.

4 Enter your password and username for the cluster.

5 Select the amount of storage that you want to add.

6 Enter the mount point for the storage. Click the **Next** button.

7 Select the datastore for the application. If the current LUN does not have space for a new datastore, select an available LUN for a new datastore.

8 Review the summary. Click the **Back** button to return and change settings.

9 Click the **Finish** button to increase the allocated storage.

Migrating service groups

VMotion is a VMware feature, with it you can move a running virtual machine from one ESX Server system to another without service interruption. VCS uses the VMware VMotion APIs to trigger a stateful migration of a service group that has virtual machines configured on it. In other words, a service group can migrate from one node to another node and continue to run.

Stateful migration is convenient when you want to move a service group to a different node. For example, if you want to load balance, or when you want to perform maintenance on the node with the service group, you can use service group migration.

The Migratable attribute is a type-level static attribute. The ESXVirtualMachine type has a default value for its Migratable attribute, which means the ESXVirtualMachine resource is a migratable resource. You can migrate the service group that contains this ESXVirtualMachine resource.

For more information on static attributes:

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

Warning: The ability of VMotion to migrate virtual machines (either using the hagrp -migrate interface or through the Virtual Center) is not supported when you have multiple virtual machines configured in a single service group. VMotion is not supported if you have tiered applications configured in a single VCS service group. Tiered applications configured in different service groups are acceptable.

Verifying if a service group can be migrated

Use the testVCConnect action function of the ESXVirtualMachine agent to verify that the ESXVirtualMachine resource's attributes are correctly configured for VMotion. This action function can also verify that the connection to your VirtualCenter Server exists (and indirectly verifies that the SSL certificate is set up too.)

Run the test VCConnect script on each node of the cluster, if you plan to use hagrp -migrate functionality. You can find the script in the actions directory /opt/VRTSvcs/bin/ESXVirtualMachine/actions/

Run the testVCConnect:

```
# hares -action res token -sys system
```

The following line is an example:

```
# hares -action evm testVCConnect -sys esxNode1
```

Where evm is the name of the ESXVirtualMachine resource, testVCConnect is the name of the token, and esxNode1 is the name of the node where you want to test the connection from.

Service group migration restrictions

You can only migrate a service group if it is fully or partially online. The `-migrate` option is not supported for migrating parallel service groups, for migrating hybrid service groups across system zones, nor across clusters. When the migration completes, the service group is offline on the source node and online on the target node. The `-migrate` option is also not supported if the service group contains more than one resources that can be migrated.

Migrating service group

Perform the following procedure to migrate a service group. Note that the service group must have a resource with the Migratable attribute set.

To migrate a service group

- Enter the following command on any VCS node:

  ```
  # hagrp -migrate service_group -to system
  ```

Preserving the last-known good copy of your configuration

VCS replication agents provide the option of running a fire drill to test whether your applications can fail over to a remote site in case of a disaster. When running VCS for VMware, you can run a fire drill in the local cluster to take a snapshot of your application data. See the documentation for the replication agent used in your configuration.

After you run a fire drill, you can keep the final snapshot that passed your basic testing as the last-known good copy of your application as a backup. This copy is preserved until you perform a manual resynchronization on the array, or until you perform another fire drill.

Index

D

E

F

G

H

I

L

S

T

U

V

W