Veritas™ Cluster Server Implementation Guide

ESX

5.1
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:

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.
## Section I  Installing VCS for VMware ESX

### Chapter 1  Introducing VCS for VMware ESX

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>16</td>
</tr>
<tr>
<td>About VCS</td>
<td>17</td>
</tr>
<tr>
<td>Multiple nodes</td>
<td>18</td>
</tr>
<tr>
<td>Virtual machines and applications</td>
<td>18</td>
</tr>
<tr>
<td>Shared storage</td>
<td>18</td>
</tr>
<tr>
<td>LLT and GAB</td>
<td>19</td>
</tr>
<tr>
<td>Network channels for heartbeats</td>
<td>19</td>
</tr>
<tr>
<td>Service groups</td>
<td>19</td>
</tr>
<tr>
<td>About high availability using VCS for VMware ESX</td>
<td>20</td>
</tr>
<tr>
<td>About disaster recovery using VCS for VMware ESX</td>
<td>20</td>
</tr>
<tr>
<td>Replicated storage</td>
<td>21</td>
</tr>
<tr>
<td>Global clusters</td>
<td>21</td>
</tr>
<tr>
<td>Installation road map</td>
<td>22</td>
</tr>
</tbody>
</table>

### Chapter 2  Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware requirements</td>
<td>26</td>
</tr>
<tr>
<td>Required and recommended servers</td>
<td>27</td>
</tr>
<tr>
<td>Required</td>
<td>27</td>
</tr>
<tr>
<td>Recommended</td>
<td>27</td>
</tr>
<tr>
<td>Required VMware components</td>
<td>28</td>
</tr>
<tr>
<td>Required cluster configuration</td>
<td>28</td>
</tr>
<tr>
<td>Supported software</td>
<td>28</td>
</tr>
<tr>
<td>Replication solutions</td>
<td>28</td>
</tr>
<tr>
<td>Supported guest operating systems</td>
<td>29</td>
</tr>
<tr>
<td>Supported VMware editions and datastores</td>
<td>30</td>
</tr>
<tr>
<td>Supported applications for detailed application monitoring</td>
<td>30</td>
</tr>
<tr>
<td>VMotion and DRS</td>
<td>31</td>
</tr>
<tr>
<td>Bind utilities update</td>
<td>31</td>
</tr>
</tbody>
</table>
# Chapter 3
Planning to install VCS on an ESX Server

About installing VCS on an ESX Server .................................................. 34
About optional VCS features .................................................................. 34
Cluster Management Console ............................................................... 34
Cluster Manager (Java Console) ............................................................. 35
Notifications ....................................................................................... 35
Global clusters using VCS ...................................................................... 35
Performing pre-installation tasks .......................................................... 36
Setting environment variables ............................................................... 37
Setting up the private network ............................................................... 37
Selecting virtual interfaces for use by the private network .................. 38
Enabling communication between systems ........................................ 39
Optimizing LLT media speed settings on private NICs ...................... 39
Setting the media speed of the LLT interconnects .............................. 39
Enabling password free SSH-communication between systems .......... 40
Obtaining VCS license keys ................................................................. 42
Preparing your VCS installation and configuration information .......... 43
Optional VCS RPMs ........................................................................... 46
Service console firewall ports that installevc opens during installation .... 46

# Chapter 4
Installing and configuring VCS on ESX Servers

About installing and configuring VCS ..................................................... 48
Installation quick start ......................................................................... 48
About the VCS installation program .................................................... 48
Optional installevc program actions ..................................................... 49
Interacting with the installevc program .............................................. 49
Installing and configuring VCS 5.1 ....................................................... 50
Installation and configuration task overview ....................................... 50
Checking the systems for installation ................................................... 51
Starting the software installation ......................................................... 52
Specifying systems for installation ..................................................... 52
Licensing VCS .................................................................................... 53
Choosing VCS RPMs .......................................................................... 54
Choosing to install VCS RPMs or to configure VCS .......................... 54
Configuring the cluster ....................................................................... 55
ESX network configuration ................................................................. 56
Adding VCS users ............................................................................... 57
Configuring cluster connector ............................................................ 57
Configuring the Veritas Cluster Management Console ....................... 59
Chapter 6  Adding and removing cluster nodes

About adding and removing nodes .............................................. 100
  Adding nodes ............................................................................ 100
  Removing nodes ......................................................................... 100
Adding a node to a cluster ............................................................... 100
  Setting up the hardware ............................................................... 101
  Preparing for a manual installation .............................................. 102
  Installing VCS RPMs for a manual installation .............................. 102
  Adding a license key ................................................................... 103
  Configuring LLT and GAB ............................................................ 103
  Adding the node to the existing cluster ....................................... 105
  Starting VCS and verifying the cluster .......................................... 105
  Adding the node to the VMware cluster ...................................... 106
Removing a node from a cluster ..................................................... 106
  Verify the status of nodes and service groups .............................. 107
  Deleting the node from the VMware cluster ................................ 107
  Deleting the departing node from VCS configuration .................... 107
  Modifying configuration files on each remaining node ................. 109
  Unloading LLT and GAB and removing VCS on the departing node 110

Chapter 7  Installing VCS on a single node

About installing VCS on a single node ........................................ 114
Creating a single-node cluster using the installvcs program ............ 114
  Preparing for a single node installation ....................................... 114
  Starting the installvcs program for the single node cluster .......... 115
Creating a single-node cluster manually ....................................... 115
  Setting the PATH variable ......................................................... 116
  Installing VCS RPMs for a manual installation ............................. 116
  Adding a license key ................................................................... 117
  Renaming the LLT and GAB startup files ..................................... 117
  Modifying the startup files ......................................................... 118
  Configuring VCS ...................................................................... 118
  Verifying single-node operation .................................................. 119
Adding a node to a single-node cluster ........................................ 120
  Setting up a node to join the single-node cluster .......................... 121
  Installing and configuring Ethernet cards for private network ....... 121
  Configuring the shared storage .................................................... 122
  Bringing up the existing node ..................................................... 122
  Installing the VCS RPMs and license key .................................... 123
  Configuring LLT and GAB ........................................................... 123
  Starting LLT and GAB ................................................................. 125
## Contents

Reconfiguring VCS on the existing node .............................................. 125  
Verifying configuration on both nodes .............................................. 126

Chapter 8 Upgrading to VCS 5.1  
About upgrading to VCS 5.1 .......................................................... 128  
Upgrading VCS on ESX Server nodes .............................................. 128  
Starting the upgrade .................................................................. 129  
Checking upgrade requirements ................................................. 129  
Upgrading VCS 5.0 packages to VCS 5.1 RPMs .............................. 130  
ESX network configuration ......................................................... 132  
Upgrading the Veritas Virtual Machine Tools on virtual machines .......... 133  
Upgrading Linux virtual machines ............................................. 133  
Upgrading Windows virtual machines ......................................... 133  
Completing the VCS upgrade on the ESX Server nodes ..................... 135

Section II Configuring VCS for virtual machines

Chapter 9 Installing the Veritas Virtualization Manager (VVM)  
About Veritas Virtualization Manager (VVM) ................................. 140  
Installing the Veritas Virtualization Manager (VVM) ......................... 141  
Veritas Virtualization Manager hardware requirements .................. 141  
Installing the Veritas Virtualization Manager ................................. 141  
Preparing keystores .................................................................... 142  
Finding the path information on the VirtualCenter Server ................ 143  
Creating the certificate store for the Veritas Virtualization Manager .......................... 144  
Copying the keystore file from the VirtualCenter Server to the Veritas Virtualization Manager ............................................. 145  
Copying the keystore file from the VirtualCenter Server to each of the ESX Server nodes in the VCS cluster ................................. 145  
Removing the Veritas Virtualization Manager (VVM) ...................... 146  
Upgrading the Veritas Virtualization Manager (VVM) ...................... 147

Chapter 10 Configuring virtual machines for high availability  
About configuring virtual machines ............................................. 150  
Configuring virtual machines for high availability using the Veritas Virtualization Manager .............................................. 150  
Prerequisites for configuring virtual machines for high availability ....... 150  
Reviewing the generated service groups ................................... 152  
Accessing the service groups .................................................. 153  
Verifying virtual machine failover ............................................ 153
Chapter 11  Configuring virtual machines for disaster recovery

About VCS global clusters ................................................................. 156
VCS global clusters: The building blocks ..................................... 157
Prerequisites for global clusters .................................................. 158
Setting up a global cluster manually ............................................ 159
  Configuring the ClusterService group ..................................... 160
  Configuring replication ............................................................. 161
  Configuring the second cluster .................................................. 163
  Linking clusters ..................................................................... 163
  Creating the global service group ............................................. 164
Configuring virtual machines for disaster recovery
  using the Veritas Virtualization Manager .................................. 165
Overview of tasks ...................................................................... 166
Prerequisites for configuring virtual machines for disaster recovery .................................................. 167
Setting up secure DNS update ..................................................... 167
Using Veritas Virtualization Manager to configure virtual machines for disaster recovery .................. 168
Deploying VCS components on the virtual machines in the primary site ........................................... 170
Confirming service group availability ........................................ 170
Reversing the direction of replication ........................................ 170
Using VVM to configure virtual machines for disaster recovery on the secondary site ..................... 170
Deploying VCS components on virtual machines in the secondary site ............................................ 171
Verifying the service group on the secondary site and using the Global Wizard .................................. 171
Post-failover actions .................................................................. 171
Reviewing the generated service groups ................................. 172
Accessing the service groups ..................................................... 173
Verifying virtual machine failover ............................................. 173
Fire drills ................................................................................. 174

Section III  Configuring applications in virtual machines

Chapter 12  Configuring applications and resources in Linux virtual machines

About VCS components for virtual machines
  running Linux ........................................................................ 178
About monitoring levels .......................................................... 179
Supported software .................................................................. 179
Contents

About the VCS agent for Oracle ..................................................179
About the VCS agent for the Apache Web server ..................188
About the VCS agent for SAP NetWeaver ..........................192
About the Application agent ...................................................198
About the Mount agent ..........................................................202

How VCS monitors applications and resources on
virtual machines ...........................................................................206
Installing the applications ........................................................207
Installing the Veritas Virtual Machine Tools .........................207
Mounting, installing, and configuring Veritas Virtual Machine
Tools on the virtual machine ..................................................207
Validating the configuration of Veritas Virtual Machine Tools ....209

Chapter 13 Configuring applications and resources in Windows virtual
machines

About VCS components on virtual machines running Windows ....218
About monitoring levels .............................................................218
Supported software .................................................................219
About the VCS agents for SQL Server ..................................220
About the VCS agent for Internet Information Services (IIS) ..........227
About the VCS agent for Exchange Server 2003 .....................230
About the VCS agent for generic services ..............................234

How VCS monitors applications and resources on
virtual machines ...........................................................................237
Installing the applications ........................................................238
Installing Veritas Virtual Machine Tools ...............................238
Validating the configuration of Veritas Virtual Machine Tools ....241
Configuring application monitoring .........................................241
Prerequisites ..............................................................................242
Configuring the SQL Server agents ....................................242
Configuring the IIS agent .........................................................245
Configuring the Exchange agents .......................................247
Configuring the GenericService agent ...............................249
Verifying the configuration for application monitoring .................. 250
Applying the configuration and creating the corresponding GuestOSApp resource ................................................................. 250
Removing Veritas Virtual Machine Tools from the virtual machine running Windows ......................................................... 251

Section IV  Administering VCS for VMware ESX

Chapter 14  Administration

Administering a VCS cluster .......................................................................................................................... 256
Using VMware features and commands in a VCS environment ................................................................. 256
  Using VMotion in a VCS environment ................................................................................................. 256
  Using DRS in a VCS environment ..................................................................................................... 259
  Using maintenance mode in VCS environment .................................................................................. 260
Increasing allocated storage .................................................................................................................... 261
  Prerequisites .................................................................................................................................. 261
  Increasing storage ............................................................................................................................ 262
Preserving the last-known good copy of your configuration .................................................................. 263
Using raw devices for the virtual machine's boot image ........................................................................ 263
  Setting up shared raw device storage under VCS ........................................................................ 263
  The service group for the shared raw device .................................................................................... 264
Performing maintenance on virtual machines and applications in virtual machines ................................................................. 265
Performing maintenance on a virtual machine ....................................................................................... 265
Performing maintenance on applications inside the virtual machine .................................................. 266
Troubleshooting maintenance .............................................................................................................. 267

Index .......................... 269
Installing VCS for VMware ESX

This section contains the following chapters:

- Chapter 1. “Introducing VCS for VMware ESX” on page 15
- Chapter 2. “Requirements” on page 25
- Chapter 3. “Planning to install VCS on an ESX Server” on page 33
- Chapter 4. “Installing and configuring VCS on ESX Servers” on page 47
- Chapter 5. “Verifying VCS on ESX Servers” on page 83
- Chapter 6. “Adding and removing cluster nodes” on page 99
- Chapter 7. “Installing VCS on a single node” on page 113
- Chapter 8. “Upgrading to VCS 5.1” on page 127
Introducing VCS for VMware ESX

This chapter contains the following topics:

- Features
- About VCS
- About high availability using VCS for VMware ESX
- About disaster recovery using VCS for VMware ESX
- Installation road map
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, storage and networking components of the ESX Server, and the ESX Server itself.

- **Disaster recovery**
  Use VCS to prepare your environments for disaster—and have confidence that your clusters can survive a disaster. Requires a supported replication infrastructure and 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 replication infrastructure and VCS agent for replication.

- **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.

- **Support for VMotion and Distributed Resource Scheduler (DRS)**
  When VMotion or DRS moves a virtual machine, VCS correctly interprets this and does not register the movement as a failure.

- **Management options**
  Manage your clusters and nodes with the Java Console, the Veritas Cluster Management Console, or from the command line.

- **The Veritas Virtualization Manager**
  Use the Veritas Virtualization Manager for quick deployment and configuration 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.

- **Virtual machine storage management**
  Enables you to easily grow your application data mounts. Note that in certain configurations you can use NFS and raw devices for storage.
About VCS

Veritas Cluster Server (VCS) monitors sites, clusters, systems, virtual machines, and applications. You can group up to 16 ESX Server systems together with VCS to 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. Depending on your configuration, when hardware or software fails, VCS moves the service group to another node in the same cluster, or to a remote node in a different cluster.

VCS for VMware ESX runs the majority of the VCS components (the VCS engine, most 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 virtual machines. VCS nodes in the cluster communicate over a private network.

![Figure 1-1 Example of a four-node VCS cluster configuration](image)
**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 takes corrective actions. In some cases, you might want VCS to restart the application. In other situations, you might want VCS to fail over to a different node entirely.

**Detailed and basic monitoring**

For certain applications, VCS supports detailed monitoring and the ability to detect a graceful shut down. If confronted with the failure of an application, VCS attempts to restart the application or move the virtual machine that runs the application onto another node. If confronted with a user intentionally shutting down an application or 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.

An example of this is monitoring an Apache instance in a RHEL guest operating system. With basic monitoring, VCS ensures that a specific httpd process (and pid) is in the process list. Detailed monitoring takes this a step further by attempting to connect to the Apache service and evaluate its response.

**Veritas Virtual Machine Tools**

Veritas Virtual Machine Tools is a package of tools that reside in the virtual machine and that provides configuration resources and wizards. You can make these tools available through the Veritas Virtualization Manager by mounting an ISO file.

**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 very fast, kernel-to-kernel communications, and monitors network connections. During installation and subsequent changes to the cluster configuration, VCS creates or modifies the following text-readable files:
  - /etc/llthosts, which lists all the nodes in the cluster
  - /etc/llttab, 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. VCS creates or modifies the gab configuration file (/etc/gabtab) during cluster creation or modification.

Network channels for heartbeats

For the VCS private network, heartbeats travel over two or more 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 the failure of a single network, and subsequent cluster corruption. For more information about network partitions refer to the following information:

Service groups

A service group is a collection of all of the items (resources) needed to provide a particular service. In the VCS for ESX paradigm, each virtual machine (and the applications it hosts) is considered a service. 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 contains additional resources for these applications. For more information on service groups:
About high availability using VCS for VMware ESX

When an ESX Server node, a virtual machine, or application in a virtual machine fails, VCS moves virtual machines to other nodes.

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

Use VCS to ensure that your applications and data remain online. Disaster recovery protects your servers from unwanted downtime due to a cluster- or site-wide event. 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 infrastructure and configuration to see if it can survive a disaster. VCS for VMware ESX provides for this testing with fire drills. These fire drills give your applications a full test of their functionality during an emergency.

When you prepare for disaster, you should have a last known good copy of your application and guest data 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 monitor, and if needed change, the replication state 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, the network configuration is changed to re-direct clients 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, refer to the Veritas Cluster Server User’s Guide.
Installation road map

Figure 1-4 on page 22 illustrates a VCS for VMware ESX installation.

Figure 1-4  Suggested installation flow

- Install the ESX Servers
- Install the VirtualCenter Server
- Install the VMware license server
- Install the guest operating system and application in the virtual machine
- Install Veritas Virtual Manager on a standalone system
- Run the Veritas Virtual Manager to configure virtual machines
- Install VCS on the ESX Servers—optionally with the global clustering option and disaster recovery agents
- Install VMware tools
- Install and configure Veritas Virtualization Tools on the virtual machines
- Complete the service group configuration
- Manage VCS components
Table 1-1 on page 23 describes where to look for the pertinent road map information.

<table>
<thead>
<tr>
<th>Road map entry</th>
<th>Document or chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the ESX Servers, the VirtualCenter Server, and the VMware license server.</td>
<td>See the appropriate VMware documentation.</td>
</tr>
<tr>
<td>Install the guest application in the virtual machine.</td>
<td>See the application's documentation.</td>
</tr>
</tbody>
</table>
| 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 33.  
■ See “Installing and configuring VCS on ESX Servers” on page 47.  
■ See “Verifying VCS on ESX Servers” on page 83. |
| Install the Veritas Virtual Manager on a standalone system.                    | See “Installing the Veritas Virtualization Manager (VVM)” on page 139.               |
| Run the Veritas Virtual Manager to configure virtual machines.                 | ■ See “Configuring virtual machines for high availability” on page 149.  
■ See “Configuring virtual machines for disaster recovery” on page 155.                                       |
| Install and configure Virtual Machine Tools in the virtual machine.           | ■ See “Configuring applications and resources in Linux virtual machines” on page 177.  
■ See “Configuring applications and resources in Windows virtual machines” on page 217. |
| Configure VCS to monitor your applications.                                   | ■ See “Configuring applications and resources in Linux virtual machines” on page 177.  
■ See “Configuring applications and resources in Windows virtual machines” on page 217. |
| Manage VCS components.                                                        | See the Veritas Cluster Server User's Guide.                                         |
Installation road map
Chapter 2

Requirements

This chapter contains the following topics:

- Hardware requirements
- Required and recommended servers
- Required VMware components
- Required cluster configuration
- Supported software
Hardware requirements

Make sure that your hardware meets the following requirements.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCS systems</td>
<td>From one to sixteen ESX Servers that run the supported ESX Server operating system version. See “Required and recommended servers” on page 27.</td>
</tr>
<tr>
<td>DVD drive</td>
<td>One drive in a system that can communicate to all the nodes in the cluster.</td>
</tr>
<tr>
<td>Disks</td>
<td>Typical VCS configurations require that shared disks support applications that migrate between systems in the cluster.</td>
</tr>
<tr>
<td>Disk space</td>
<td>See Table 2-2, &quot;Disk space requirements and totals.&quot;</td>
</tr>
<tr>
<td>Network Interface Cards</td>
<td>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.</td>
</tr>
<tr>
<td>Fibre Channel or SCSI host bus adapters</td>
<td>Typical VCS configuration requires at least one SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.</td>
</tr>
<tr>
<td>RAM</td>
<td>Each VCS system requires at least 256 megabytes in addition to other system and application requirements.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Package</th>
<th>/</th>
<th>/opt</th>
<th>/usr</th>
<th>/var</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>2 MB</td>
<td>280 MB</td>
<td>9 MB</td>
<td>1 MB</td>
<td>292 MB</td>
</tr>
<tr>
<td>Optional</td>
<td>1 MB</td>
<td>45 MB</td>
<td>0 MB</td>
<td>0 MB</td>
<td>46 MB</td>
</tr>
<tr>
<td>Required and optional total</td>
<td>3 MB</td>
<td>325 MB</td>
<td>9 MB</td>
<td>1 MB</td>
<td>338 MB</td>
</tr>
</tbody>
</table>

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 and recommended servers

For minimal functionality, use the required server. For full functionality, use all the required and recommended servers.

Required

You need ESX Server 3.0 or 3.01 to run VCS for VMware ESX 5.1.

Recommended

For full VCS for VMware ESX 5.1 functionality, use the following servers:

- 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.

Required cluster configuration

The nodes that are defined in the VCS cluster and the nodes that are defined in the VMware cluster must be identical. A one-to-one parity between these cluster objects must exist at all times. This requirement applies to all aspects of using VCS for VMware ESX. It also covers compatibility with VMotion and DRS.

Supported software

Replication solutions

VCS supports several replication solutions. Contact your Symantec sales representative for the solutions supported by VCS.
Supported guest operating systems

Refer to the Veritas Cluster Server Release Notes for the most current information concerning the supported guest operating systems.

Table 2-3 lists the architectures and operating systems that VCS for VMware ESX 5.1 supports for guest operating systems.

* Supports increasing storage allocation.

Table 2-3  Supported operating systems and architectures

<table>
<thead>
<tr>
<th>Guest operating systems</th>
<th>Kernels</th>
<th>Architectures</th>
<th>File systems/ Volume managers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Server or Advanced Server with Service Pack 4</td>
<td>---</td>
<td>x86 (32-bit)</td>
<td>NTFS/*--</td>
</tr>
<tr>
<td>Windows Server 2003: Standard Edition or Enterprise Edition (SP1 required)</td>
<td>---</td>
<td>x86 (32-bit)</td>
<td>NTFS/*--</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4 (RHEL 4) Update 3</td>
<td>2.6.9-34.EL 2.6.9-34.smp 2.6.9-34.hugemem</td>
<td>x86 (32-bit) x86 (64-bit)</td>
<td>ext2, *ext3, reiserfs/LVM</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 9 (SLES 9) with SP3</td>
<td>2.6.5-7.244 2.6.5-7.244-smp 2.6.5-7.244-bigsmp</td>
<td>x86 (32-bit) x86 (64-bit)</td>
<td>ext2, ext3, *reiserfs/LVM</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10 (SLES 10) with SP1</td>
<td>2.6.16-21-0.8 2.6.16-37-0.18-bigsmp</td>
<td>x86 (32-bit) x86 (64-bit)</td>
<td>ext2, ext3, *reiserfs/LVM</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>---</td>
<td>x86</td>
<td>n/a</td>
</tr>
</tbody>
</table>

* 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:

Supported VMware editions and datastores

VCS for VMware ESX supports the following VMware editions:

- VMware Infrastructure Enterprise. This edition is required for full VCS functionality and integration.
- VMware Infrastructure Standard. This edition has certain limitations.
  - Veritas Virtualization Manager (VVM) is not supported.
  - Service group migration via VMotion is not supported.

VCS supports datastores on VMFS 3 (SAN-attached or NFS.) VCS does not support the iSCSI protocol.

Supported applications for detailed application monitoring

Table 2-4 lists the applications that VCS for VMware ESX 5.1 supports for detailed monitoring and the ability to detect the graceful administrative shutdown of an application in a virtual machine.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Applications</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Apache Web server</td>
<td>1.3, 2.0, and 2.2</td>
</tr>
<tr>
<td></td>
<td>IBM HTTP Server</td>
<td>1.3 and 2.0</td>
</tr>
<tr>
<td></td>
<td>Oracle</td>
<td>10g</td>
</tr>
<tr>
<td></td>
<td>SAP NetWeaver</td>
<td>SAP R/3-4.6C with a 4.6D Kernel, 4.6D, 4.7 Enterprise Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP Web AS-6.20, 6.40, 7.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAP NetWeaver-2004, 2004s</td>
</tr>
<tr>
<td>Windows</td>
<td>Exchange</td>
<td>Exchange Server 2003</td>
</tr>
<tr>
<td></td>
<td>GenericService</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>IIS</td>
<td>5.0 and 6.0</td>
</tr>
<tr>
<td></td>
<td>SQL</td>
<td>Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (both require SP4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft SQL Server 2005, 32-bit (SP1 required)</td>
</tr>
</tbody>
</table>
VMotion and DRS

VCS for VMware ESX supports both VMotion and DRS. Both of these VMware features require exact parity among the nodes in the VCS and VMware clusters. Both of these VMware features have VCS equivalents, and certain requirements for their proper use.

See “Using VMware features and commands in a VCS environment” on page 256.

Bind utilities update

The disaster recovery configuration requires the latest bind utilities. The DNS agent requires bind-utils-9.2.4-16.EL4. Symantec recommends installing the latest version of bind utilities before configuring the cluster for disaster recovery.
Supported software
Planning to install VCS on an ESX Server

This chapter contains the following topics:

- About installing VCS on an ESX Server
- About optional VCS features
- Performing pre-installation tasks
- Preparing your VCS installation and configuration information
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/289940

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:

- 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.

Cluster Management Console

The 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 management server. Use the console to give commands to the multi-cluster management engine.

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, refer to the Veritas Cluster Server User’s Guide.
Planning to install VCS on an ESX Server

About optional VCS features

Cluster Manager (Java Console)

The Cluster Manager (Java Console) is a light-weight Java-based interface. You install the Java Console on a Windows client, and you use it to manage your clusters and the service groups that comprise your cluster. The Java Console is automatically installed when you install the Veritas Virtualization Manager.

For more information, refer to the *Veritas Cluster Server User’s Guide.*

See “Installing the Cluster Manager (Java Console)” on page 65.

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 about these notification services, refer to 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 from 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 from 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. 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 installvcs program 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 prompted.
Performing pre-installation tasks

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the PATH and MANPATH variables.</td>
<td>“Setting environment variables” on page 37</td>
</tr>
<tr>
<td>Set up the private network.</td>
<td>“Setting up the private network” on page 37</td>
</tr>
<tr>
<td>Configure the private network.</td>
<td>“Selecting virtual interfaces for use by the private network” on page 38</td>
</tr>
<tr>
<td>Enable communication between systems.</td>
<td>“Enabling communication between systems” on page 39</td>
</tr>
<tr>
<td>Review basic instructions to optimize LLT media speeds.</td>
<td>“Optimizing LLT media speed settings on private NICs” on page 39</td>
</tr>
<tr>
<td>Review guidelines to help you set the LLT interconnects.</td>
<td>“Setting the media speed of the LLT interconnects” on page 39</td>
</tr>
<tr>
<td>Set up SSH on cluster systems.</td>
<td>“Enabling password free SSH-communication between systems” on page 40</td>
</tr>
<tr>
<td>Obtain license keys.</td>
<td>“Obtaining VCS license keys” on page 42</td>
</tr>
<tr>
<td>Mount the product disc</td>
<td></td>
</tr>
</tbody>
</table>
Planning to install VCS on an ESX Server

Performing pre-installation tasks

Setting environment variables

**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. You need to add these directories to your PATH environment variable to access the commands.

To set the PATH variable

* Do one of the following:
  - For the Bourne Shell (sh or ksh), type:
    ```bash
    $ PATH=/usr/sbin:/sbin:/opt/VRTS/bin:/opt/VRTSvcs/bin:$PATH; export PATH
    ```
  - For the C Shell (csh or tcsh), type:
    ```bash
    % setenv PATH /usr/sbin:/sbin:/opt/VRTS/bin:
    /opt/VRTSvcs/bin:$PATH
    ```

**Setting the MANPATH variable**

To set the MANPATH variable

* Do one of the following:
  - For the Bourne Shell (sh or ksh), type:
    ```bash
    $ MANPATH=/usr/share/man:/opt/VRTS/man; export MANPATH
    ```
  - For the C Shell (csh or tcsh), type:
    ```bash
    % 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.

```bash
# export LC_ALL=C
```

**Setting up the private network**

VCS requires you to set up a private network between the systems that form part of a cluster.

**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 switches for each VCS communication network. (Hubs work too.) Ensure that power to the switches comes from separate sources.
4. On each system, use two independent network cards to provide redundancy. When you set up heartbeat connections, if a failure removes all communications between nodes, a chance for shared storage data corruption exists. For this reason, heartbeat network architecture must be as robust as possible, reducing or eliminating potential single points of failure (SPOFs).

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

![Diagram of private network setups]

5. 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. 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 48.

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 or virtual interface information for the private links.

- If you choose to specify physical interface information, the `installvcs` program creates a virtual interface (vswif) 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. Make sure that all the systems in the cluster have virtual interfaces configured.

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

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 installvcs program 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 67.

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.

Setting the media speed of the LLT interconnects

If you have switches or hubs 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 switches or hubs 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.
Enabling password free SSH-communication between systems

VCS requires password free SSH-based communication for installation. The following is an example of how to set up SSH-based password free communication between a source system (north) and a target system (south). In this procedure, you first create a DSA key pair. You then check to see if the .ssh directory is in place on the target system (south). If doesn’t exist, create it and set permission to 700. From the key pair, you append the public key from the source system (north) to the authorized_keys file on the target systems.

Visit the OpenSSH website located at: http://openssh.org to access online manuals and other resources.

To create the DSA key pair

1. On the source system (north), log in as root to generate a DSA key pair. Enter the following command:
   
   ```
   # ssh-keygen -t dsa
   ```
   Output that resembles the following appears:
   
   Generating public/private dsa key pair.
   Enter file in which to save the key (/root/.ssh/id_dsa):
   
   Press the Enter key to accept the default location of /root/.ssh/id_dsa.

2. Press the Enter key to accept the default location of /root/.ssh/id_dsa.

3. When the program asks you to enter the passphrase, press the Enter key twice.
   
   Enter passphrase (empty for no passphrase):
   
   Press the Enter key.
   
   Enter same passphrase again:
   
   Press the Enter key again. Output that resembles the following lines appears:
   
   Your identification has been saved in /root/.ssh/id_dsa.
   Your public key has been saved in /root/.ssh/id_dsa.pub.
   The key fingerprint is:
   
   1f:00:e0:c2:9b:4e:29:b4:0b:6e:08:f8:50:de:48:d2 root@north
To check the .ssh directory on the target system

1. Log in to the target system (south).
2. Change to the /root/.ssh directory.
   
   ```
   # cd /root/.ssh
   ```
3. If the directory doesn’t exist, add it.

To add and set permissions for the .ssh directory on the target system

1. Log in to the target system (south).
2. Change to the root directory.
   
   ```
   # cd /root
   ```
3. Create the .ssh directory.
   
   ```
   # mkdir .ssh
   ```
4. Change the directory’s permission to 700.
   
   ```
   # chmod 700 .ssh
   ```

To append the public key from the source system to the authorized_keys file on the target system

1. On the source system (north), run the secure copy command to move the public key to a temporary file on the target system (south):
   
   ```
   # scp ~/.ssh/id_dsa.pub south:~/.ssh/north_id_dsa.pub
   ```
   
   Where north_id_dsa.pub is the name that you have given the temporary public key file.
2. On north, enter the root password for south:
   
   ```
   # south’s password: foobar
   ```
   
   Output that resembles the following line appears:
   
   ```
   id_dsa.pub 100% 603 0.6KB/s 00:00
   ```
3. On north, run the following command to append north’s public key, which is now a temporary file on south, to south’s authorized keys:
   
   ```
   # ssh -l root south "cat ~/.ssh/north_id_dsa.pub >> ~/.ssh/authorized_keys"
   ```
4. On north, enter the root password for south.
   
   ```
   # south’s password: foobar
5 On south, enter the following command:
   # cat ~/.ssh/authorized_keys
   Output that resembles the following appears:
   ssh-dss
   JJCJB3NzaClkc3MJJaJCWBjLNMm7QQfk9lgxKazYarXpjUNNy85sCa5rfacIVU87i
   laGss6NT6pc7N/NeL1cSckc6U1XDSxIGKXpdPw7omHITJkXKMFJNTz5sY/QrUGz
   .
   oTumbLtjennd4jmM4oEOMOFJ+ST7wZgsVn1seHPd3seXr+bUhKI+3hMqvmZa7N
   +Lp36z/YZcOj= root@north

6 On south, remove the temporary file. Enter the following command:
   # rm ~/.ssh/north_id_dsa.pub

7 Repeat this procedure on each target system where you plan to install VCS.

To verify that you can connect to a target system

◆ On the source system (north), type the following command:
   # ssh -l root south
   uname -a
   Where south is the name of the target system. The command should
   execute from the source system (north) to the target system (south) without
   the system requesting a passphrase or password.

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:
   https://licensing.symantec.com

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
Planning to install VCS on an ESX Server

Preparing your VCS installation and configuration information

Accessing documentation

You can access all the documentation for VCS on the product disc. Insert the product disc into the system’s drive and change directory to the docs directory. Copy the contents of this directory to each system where you need to access the documentation.

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 42.

- 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 Veritas 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 Veritas 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 (optional) for the Veritas Cluster Management Console, prepare the management server’s network address for the console, the 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 “Cluster Management Console” on page 34.
- 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: vswnf0
- 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
  Cluster Management Console Cluster Connector
- VRTScmcs
  Cluster Management Console
- VRTScssim
  VCS Simulator
- VRTSvcsmn
  Manual pages for VCS commands

Service console firewall ports that installvcs opens during installation

Note that during installation, the following service console firewall ports are automatically opened. These ports must remain open during normal VCS operations.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>TCP/FTP</td>
<td>FTP</td>
</tr>
<tr>
<td>22/TCP/SSH</td>
<td></td>
<td>SSH</td>
</tr>
<tr>
<td>80/TCP/HTTP</td>
<td></td>
<td>HTTP</td>
</tr>
<tr>
<td>443/TCP/HTTPS</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>8443/TCP/VRTSweb</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>8181/TCP/GCM Web Server port</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14145/TCP/GCM default port</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14147/TCP/GCM slave port</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14143/TCP/GAB simulator</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14153/TCP/Compute server</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14155/TCP/WAC</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>512/TCP/exec</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>514/TCP/RSH</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>514/UDP/syslogd</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14141/TCP/HAD</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14144/TCP/notifier</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14149/TCP/VCSTD</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14150/TCP/Command server</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>14154/TCP/SimServer</td>
<td></td>
<td>VRTSweb</td>
</tr>
<tr>
<td>513/TCP/remote login</td>
<td></td>
<td>VRTSweb</td>
</tr>
</tbody>
</table>
Installing and configuring VCS on ESX Servers

This chapter contains the following topics:
- About installing and configuring VCS
- Installation quick start
- About the VCS installation program
- Installing and configuring VCS 5.1
- Installing VCS using installonly option
- Configuring VCS using configure option
- Performing VCS installation in a secure environment
- Performing automated installations
- Checking licensing information on the system
- Updating product licenses using vxlicinst
- About installvcs command options
- About the uninstallvcs program
- Uninstalling VCS 5.1
About installing and configuring VCS

You install VCS on ESX Servers. You can install VCS on clusters of up to 16 systems. The installvcs program uses ssh to install by default.

Installation quick start

If you are comfortable loading enterprise-level software and VCS, 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 36.

- Prepare the information you need for your new cluster.
  See “Preparing your VCS installation and configuration information” on page 43.

- Start the installation and follow the installvcs program’s instructions.
  See “Starting the software installation” on page 52.

About the VCS installation program

You can access the installvcs program from the command line or through the installvcs program. The installvcs program is interactive and enables you to install, configure, license, and start VCS and its options on multiple nodes.

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>
<thead>
<tr>
<th>Optional action</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the systems to verify that they meet the requirements to install VCS.</td>
<td>See “Checking the systems for installation” on page 51.</td>
</tr>
<tr>
<td>Install VCS RPMs without configuring VCS.</td>
<td>See “Installing VCS using installonly option” on page 67.</td>
</tr>
<tr>
<td>Configure or reconfigure VCS when VCS RPMs are already installed.</td>
<td>See “Configuring VCS using configure option” on page 67.</td>
</tr>
<tr>
<td>Perform secure installations using values stored in a configuration file.</td>
<td>See “Performing VCS installation in a secure environment” on page 67.</td>
</tr>
<tr>
<td>Perform automated installations using values stored in a configuration file.</td>
<td>See “Performing automated installations” on page 69.</td>
</tr>
</tbody>
</table>

Interacting with the installvcs program

The installvcs 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 installvcs program prompts you to type information. The installvcs program expects your responses to be within a certain range or in a specific format. The installvcs program 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 installvcs program 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 installvcs program 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 5.1

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 38.

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>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Start the installation process and choose the installation. | “Checking the systems for installation” on page 51  
“Starting the software installation” on page 52  
“Specifying systems for installation” on page 52  
“Licensing VCS” on page 53  
“Choosing VCS RPMs” on page 54  
“Choosing to install VCS RPMs or to configure VCS” on page 54 |
Table 4-2  Installation and configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the cluster and optional features.</td>
<td>■ “Configuring the cluster” on page 55</td>
</tr>
<tr>
<td></td>
<td>■ “Adding VCS users” on page 57 (optional)</td>
</tr>
<tr>
<td></td>
<td>■ “Configuring cluster connector” on page 57 (optional)</td>
</tr>
<tr>
<td></td>
<td>■ “Configuring SMTP email notification” on page 60 (optional)</td>
</tr>
<tr>
<td></td>
<td>■ “Configuring SNMP trap notification” on page 60 (optional)</td>
</tr>
<tr>
<td></td>
<td>■ “Configuring global clusters” on page 62 (optional)</td>
</tr>
<tr>
<td>Install the RPMs and create configuration files.</td>
<td>■ “Installing the VCS RPMs” on page 63</td>
</tr>
<tr>
<td></td>
<td>■ “Creating VCS configuration files” on page 64</td>
</tr>
<tr>
<td>Start VCS and its components.</td>
<td>■ “Starting VCS” on page 64</td>
</tr>
<tr>
<td></td>
<td>■ “Completing the installation” on page 64</td>
</tr>
<tr>
<td>Perform the post-installation tasks</td>
<td>■ “Copying the Implementation Guide to each node” on page 65</td>
</tr>
<tr>
<td></td>
<td>■ “Installing the Cluster Manager (Java Console)” on page 65</td>
</tr>
<tr>
<td>Verify the cluster</td>
<td>■ “Verifying the cluster after installation” on page 67</td>
</tr>
</tbody>
</table>

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.
   
   ```bash
   # cd /cdrom/cluster_server
   ```

2. Start the pre-installation check:
   
   ```bash
   # ./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 77.
Starting the software installation

Start the installation.

To install VCS

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

2. Navigate to the folder containing the installvcs program.
   # cd /cluster_server

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

Specifying systems for installation

The installvcs 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. Note that these names are case sensitive.
   
   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 installvcs program for the single node cluster” on page 115.

2. Review the output as the installvcs program verifies the systems, the installvcs program performs the following actions:
   - Checks that the local node that runs the installvcs program can communicate with remote nodes.
     If the installvcs program finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
     See “Enabling password free SSH-communication between systems” on page 40.
   - Makes sure the systems use the proper operating system.
   - Checks whether a previous version of VCS is installed.
Licensing VCS

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

See "Checking licensing information on the system" on page 75.

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 installvcs program 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)

   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 installvcs program registers the license key on the other nodes. Enter keys for additional product features on the other nodes when the installvcs program 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 installvcs program checks for any previously installed RPMs. Based on your choice, it then installs only the required RPMs or all the RPMs.

To install VCS RPMs

1. Review the output as the installvcs program checks previously installed RPMs.
2. Select option 1 or 2 to install either all or required RPMs.
3. View the list of RPMs that the installvcs program installs on each node. If the current version of a RPM is on a system, the installvcs program removes it from the RPM installation list for the system.

Choosing to install VCS RPMs or to configure VCS

You can configure VCS now or come back later.

- Configure VCS now.
  See “Configuring the cluster” on page 55.
- 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 installvcs program uninstalls any previous versions and installs the VCS 5.1 RPMs.
3. Configure the cluster later.
   See “Configuring VCS using configure option” on page 67.
Configuring the cluster

The installvcs program 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 installvcs program 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. The product installation scripts can be found in /opt/VRTS/install directory.
   Are you ready to configure VCS? [y,n,q] (y) y

2. Review the configuration requirements that the installvcs program 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
   Review the interfaces that are available on the first system as the installvcs program discovers and reports them.

4. 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}
5 Choose whether to use the same interface on all nodes.
   Are you using the same NICs for private heartbeat links on all systems? [y,n,q,b,?] (y)
   ■ If you want to use the same interfaces for private heartbeat links on all nodes, make sure the same interfaces are available on each system and enter y.
   ■ If the interfaces are not the same on all nodes, enter n. You must configure interface information for each node.

6 Verify and confirm the information that the installvcs program summarizes.
   For the specified physical interfaces, the installvcs program creates virtual interfaces that are mapped to the physical interfaces.

ESX network configuration

To configure the ESX network configuration
1 Review the output as the installvcs program now creates vswifs and configures the service console firewall.

2 The installvcs program asks if want to keep the default SSL certificate that is used to generate the keystore. Answer y to accept the default.
   Do you want to use default ssl cert to generate keystore on north? [y,n,q] (y) y

3 Enter a password for the keystore for the first system.
   Enter keystore password, not less than 6 characters:
   Re-type the password:
   Enter the keystore password again:

4 Enter the password for the root user on the first system:
   Enter the password for user root on host north:
   Re-type the password:
   Enter the password for user root again:

5 If you have the same root password on all the nodes in the cluster, answer y. The installvcs program generates the security credentials across all the systems in the cluster.
   Do you want to use the same root and keystore password on the other hosts? [y,n,q] (y) y
   If you use different root passwords on any of the nodes in the cluster, installvcs prompts you for those.
   Installvcs now generates the security credentials for VCS agents.
   Generating security credentials for VCS agents .......... Done
Adding VCS users

On systems operating under an English locale, now add VCS users.

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] (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 to proceed.

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 Veritas 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 the Enter key to accept y (yes) as your default answer.
     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)
   - To skip configuring cluster connector and advance to configuring Cluster Management Console for local cluster management, enter n.

3. If you choose to configure the cluster connector, 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
     "Preparing your VCS installation and configuration information" on page 43

7. Verify and confirm the information.
Configuring the Veritas Cluster Management Console

Configure Cluster Management Console to use it.

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 60.

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 61.
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,?] smith@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,?] jones@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 62.

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,?] west
   - 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.
   See “Preparing your VCS installation and configuration information” on page 43.

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 63.
3  Provide information to configure the Global Cluster option.

If you configured the Veritas Cluster Management Console to manage this cluster locally, the installvcs program 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 installvcs program 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 installvcs program gathers all the configuration information, the program installs the RPMs on the cluster systems. If you already installed the RPMs and chose to configure or reconfigure the cluster, the installvcs program proceeds to create the configuration files.

See "Creating VCS configuration files" on page 64.

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 installvcs program uninstalls any previous versions and installs the VCS 5.1 RPMs.
Creating VCS configuration files

After installing the RPMs, the installvcs program 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.

Starting VCS

Start VCS and its components on each system.

To start VCS

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

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

Completing the installation

After VCS 5.1 installation completes successfully, the installvcs program 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 installvcs program displays.

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary file</td>
<td>- Lists RPMs installed on each system.</td>
</tr>
<tr>
<td></td>
<td>- Describes the cluster and its configured resources.</td>
</tr>
<tr>
<td></td>
<td>- Provides information for managing the cluster.</td>
</tr>
<tr>
<td>log file</td>
<td>Details the entire installation.</td>
</tr>
<tr>
<td>response file</td>
<td>Contains configuration information that can be used to perform secure or unattended installations on other systems.</td>
</tr>
<tr>
<td></td>
<td>See “Example response file” on page 70.</td>
</tr>
</tbody>
</table>
Enforcing compatibility between VCS and VMware features (DRS and ESX Server maintenance mode)

During VCS installation, the VCS installation program deploys the ESXHost agent on each node in the cluster. The program also creates a service group called the ESXHostServiceGroup. This is an internal use only service group. The ESXHost agent enforces a two-way compatibility between VCS and VMware's DRS and maintenance mode functions. If you bring a ESX Server into VMware maintenance mode to perform system maintenance tasks, the ESXHost agent evacuates all VCS service groups on that ESX Server to other ESX Server nodes in the VCS cluster. VCS then performs a system freeze for the cluster. The agent also provides reverse compatibility—if it detects that a VCS cluster is frozen, and no active virtual machines are on the host, it puts the ESX Server node into VMware maintenance mode.

For the ESXHost agent to work properly, ensure that there is an exact node list in the definitions between the VCS and VMware clusters. Make sure that one cluster does not have more nodes or fewer nodes than the other cluster. See “Required cluster configuration” on page 28.

Copying the Implementation Guide to each node

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

Installing the Cluster Manager (Java Console)

You can administer VCS using the Cluster Manager (Java Console), which is a Java-based graphical user interface. After VCS has been installed, install the Java Console on a Windows NT or Windows 2000 Professional system. The system from which you run the Java Console can be a system in the cluster or a remote workstation; the latter enables each system in the cluster to be administered remotely.

When installing the Java Console, make sure a printer is configured to that system. On a system without a configured printer, printing from the online JavaHelp could cause the Java Console to hang.

For information about using the Cluster Manager and the Configuration Editor components of the Java Console, see the applicable chapter in the Veritas Cluster Server User's Guide.
Hardware requirements for the Cluster Manager (Java Console)

Symantec recommends a Pentium III at 400 MHz, with 256 MB RAM. Minimum hardware requirements follow:

- Pentium II 300 megahertz CPU
- 256 megabytes RAM
- A display capable of at least 800 x 600 resolution
- 8-bit color display depth
- Graphics card capable of 2D images
- Approximately 40 MB of free hard drive space

The version of the Java™ 2 Runtime Environment (JRE) requires 32 megabytes of RAM and is supported on Intel Pentium platforms running the Linux kernel v 2.2.12 and glibc v2.1.2-11 (or later). Symantec recommends using 48 megabytes of RAM, 16-bit color mode, and KDE and KWM window managers used in conjunction with displays set to local hosts.

Installing the Java Console on a Windows workstation

You can install the Cluster Manager (Java Console) on a Windows NT workstation or a Windows 2000 Professional Workstation to administer the cluster.

To install the Java Console on a Windows system

1. Insert the software disc with the VCS software into a drive on your Windows system.
2. Using Windows Explorer, select the disc drive.
3. Go to \windows\ClusterManager.
4. Open the language folder of your choice, for example EN.
5. Double-click setup.exe.
6. The Veritas Cluster Manager Install Wizard guides you through the installation process.
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 83.

Installing VCS using installonly option

In certain situations, you may choose to install the VCS RPMs on a system before it is ready for cluster configuration. During such situations, use the installvcs -installonly option. 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 55.

The -configure option can be used to reconfigure a VCS cluster. VCS must not be running on systems when you reconfigure it.

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 70.

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.
Performing VCS installation in a secure environment

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 52.

2. Review the output as the installvcs program performs the initial system checks.
   The installvcs program detects the inability to communicate between systems.

3. Press the Enter key to install VCS on one system and create a response file with which you can install on other systems.
   Would you like to install Cluster Server on systems north only and create a response file for systems south? [y,n,q] (y)

4. Enter all cluster information. Proceed with the installation and configuration tasks.
   See “Installing and configuring VCS 5.1” on page 50.
   The installvcs program installs and configures VCS on systems where communication is possible.

5. After the installation is complete, review the installvcs program report.
   The installvcs program stores the response file within the file

6. If you start VCS before VCS is installed and started on all nodes in the cluster, you see the output similar to:
   VCS:11306:Did not receive cluster membership, manual intervention may be needed for seeding

7. 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-XXXX'];
   ...
   
   For demo or site licenses, the license key need not be changed.
On the next system:
- Mount the product disc.
- Start the software installation using the `installvcs -responsefile` option.

```bash
# ./installvcs -responsefile /tmp/installvcs-uui.response
```
Where uui is the Universal Unique Identifier that the installvcs program automatically assigned to the response file.

See “Starting the software installation” on page 52.

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.
   ```bash
   # cd /mnt/cdrom/cluster_server
   ```
2. Start the installation from one of the cluster systems where you have copied the response file.
   ```bash
   # ./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,

```perl
$CFG{Scalar_variable}="value";
```
or, in the case of an integer value:

```perl
$CFG{Scalar_variable}=123;
```
or, in the case of a list:

```perl
$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."

```bash
# installvcs configuration values:
#
$CPI::CFG(AT_ROOTDOMAIN)="root\@east.symantecexample.com";
$CPI::CFG(CMC_ROOTCONFIGURED)=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)="758a33db6afe751630058ace3dedb54e562fe98";
$CPI::CFG(CMC_SERVICE_PASSWORD)="U2FsdGVkX18vE5tnKoT5SwodThAcc+rx";
$CPI::CFG(ENCRIPTED)="U2FsdGVkX18vE5tnKoT5SwodThAcc+rx";
$CPI::CFG(OP2)(INSTALL)=1;
$CPI::CFG(OP2)(NOEXTRAPKG)=1;
$CPI::CFG(OP2)(RSN)=1;
$CPI::CFG(SYSTEMS)=[ qw(east west) ];
$CPI::CFG(USER)="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_SMTPRECIP)=[ qw(earnie@symantecexample.com) ];
$CPI::CFG(VCS_SMTPSERVER)=[ qw(SevereError) ];
$CPI::CFG(VCS_SNMPUSER)="smtp.symantecexample.com";
$CPI::CFG(VCS_SNMPCONS)=[ qw(neptune) ];
$CPI::CFG(VCS_SNMPCESEV)=[ 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>
<thead>
<tr>
<th>Variable</th>
<th>List/Scalar</th>
<th>Opt'lrq'd</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CPI::CFG[OPT][INSTALL]</td>
<td>Scalar</td>
<td>Req'd</td>
<td>List of systems where VCS must be installed and configured.</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][INSTALLONLY]</td>
<td>Scalar</td>
<td>Opt'l</td>
<td>List of systems where VCS RPMs must be installed. Configuration can be performed at a later time using the -configure option.</td>
</tr>
<tr>
<td>$CPI::CFG[SYSTEMS]</td>
<td>List</td>
<td>Req'd</td>
<td>List of systems on which the product is to be installed, uninstalled, or configured.</td>
</tr>
<tr>
<td>$CPI::CFG[SYSTEMSCFG]</td>
<td>List</td>
<td>Opt'l</td>
<td>List of systems to be recognized in configuration if secure environment prevents all systems from being installed at once.</td>
</tr>
<tr>
<td>$CPI::CFG[UPI]</td>
<td>Scalar</td>
<td>Req'd</td>
<td>Defines the product to be installed, uninstalled, or configured.</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][KEYFILE]</td>
<td>Scalar</td>
<td>Opt'l</td>
<td>Defines the location of an ssh keyfile that is used to communicate with all remote systems.</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][LICENSE]</td>
<td>Scalar</td>
<td>Opt'l</td>
<td>Licenses VCS only.</td>
</tr>
</tbody>
</table>
## Table 4-4 Response file variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>List/Scalar</th>
<th>Opt’l/Req’d</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CPI::CFG[OPT][NOLIC]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>installs the product without any license.</td>
</tr>
<tr>
<td>$CPI::CFG[AT_ROOTDOMAIN]</td>
<td>List</td>
<td>Opt’l</td>
<td>Defines the name of the system where the root broker is installed.</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][PKGPATH]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>Defines a location, typically an NFS mount, from which all remote systems can install product depots. The location must be accessible from all target systems.</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][TMPPATH]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>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.</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][RSH]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>Defines that rsh must be used instead of ssh as the communication method between systems.</td>
</tr>
<tr>
<td>$CPI::CFG[DONOTINSTALL][RPM]</td>
<td>List</td>
<td>Opt’l</td>
<td>Instructs the installation to not install the optional RPMs designated in the list.</td>
</tr>
<tr>
<td>$CPI::CFG[DONOTREMOVE][RPM]</td>
<td>List</td>
<td>Opt’l</td>
<td>Instructs the uninstallation to not remove the optional RPMs designated in the list.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_CLUSTERNAME]</td>
<td>Scalar</td>
<td>Req’d</td>
<td>Defines the name of the cluster.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_CLUSTERID]</td>
<td>Scalar</td>
<td>Req’d</td>
<td>An integer between 0 and 65535 that uniquely identifies the cluster.</td>
</tr>
<tr>
<td>$CPI::CFG[KEYS][SYSTEM]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>List of keys to be registered on the system.</td>
</tr>
</tbody>
</table>
Table 4-4  
Response file variables

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>List/ Scalar</th>
<th>Opt’l/ Req’d</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CPI::CFG[VCS_SMTPRECP]</td>
<td>List</td>
<td>Opt’l</td>
<td>List of full email addresses (example: <a href="mailto:user@symantecexample.com">user@symantecexample.com</a>) of SMTP recipients.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_SMTPRSEV]</td>
<td>List</td>
<td>Opt’l</td>
<td>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.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_SNMPPORT]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>Defines the SNMP trap daemon port (default=162).</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_SNMPCONS]</td>
<td>List</td>
<td>Opt’l</td>
<td>List of SNMP console system names.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_SN MPCSEV]</td>
<td>List</td>
<td>Opt’l</td>
<td>Defines minimum severity level of messages (Information, Warning, Error, SevereError) that listed SNMP consoles are to receive. Note that the ordering of severity levels must match that of the SNMP console system names.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_GCONIC] [SYSTEM]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>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.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_GCOVIP]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>Defines the virtual IP address to be used by the Global Cluster Option.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_GCONETMASK]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>Defines the Netmask of the virtual IP address to be used by the Global Cluster Option.</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_USERENPW]</td>
<td>List</td>
<td>Opt’l</td>
<td>List of encoded passwords for users.</td>
</tr>
</tbody>
</table>
Table 4-4  Response file variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>List/Scalar</th>
<th>Opt’l/Req’d</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CPI::CFG[VCS_USERNAME]</td>
<td>List</td>
<td>Opt’l</td>
<td>List of names of users</td>
</tr>
<tr>
<td>$CPI::CFG[VCS_USERPRIV]</td>
<td>List</td>
<td>Opt’l</td>
<td>List of privileges for users</td>
</tr>
<tr>
<td>$CPI::CFG[OPT][UNINSTALL]</td>
<td>Scalar</td>
<td>Opt’l</td>
<td>List of systems where VCS must be uninstalled.</td>
</tr>
</tbody>
</table>

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 = 5.1
Tier = 0
Reserved = 0

Mode = VCS
Installing and configuring VCS on ESX Servers

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 76.

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>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-configure</code></td>
<td>Configure VCS after using <code>-installonly</code> option to install VCS. See “Configuring VCS using configure option” on page 67.</td>
</tr>
<tr>
<td><code>-enckeyfile</code> encryption_key_file</td>
<td>Encrypt password using the encryption key provided with the <code>-enckeyfile</code> option so that the encrypted password can be stored in response files.</td>
</tr>
<tr>
<td><code>-encrypt password</code></td>
<td>Encrypt <code>password</code> using the encryption key provided with the <code>-enckeyfile</code> option so that the encrypted password can be stored in response files.</td>
</tr>
<tr>
<td><code>-installonly</code></td>
<td>Install product RPMs on systems without configuring VCS. See “Installing VCS using installonly option” on page 67.</td>
</tr>
<tr>
<td><code>-installpkgs</code></td>
<td>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 <code>requiredpkgs</code> option.</td>
</tr>
<tr>
<td><code>-keyfile</code> ssh_key_file</td>
<td>Specifies a key file for SSH. The option passes <code>-i ssh_key_file</code> with each SSH invocation.</td>
</tr>
<tr>
<td><code>-license</code></td>
<td>Register or update product licenses on the specified systems. Useful for replacing demo license.</td>
</tr>
<tr>
<td><code>-logpath log_path</code></td>
<td>Specifies that <code>log_path</code>, not <code>/opt/VRTS/install/logs</code>, is the location where <code>installvcs</code> log files, summary file, and response file are saved.</td>
</tr>
<tr>
<td><code>-noextrapkgs</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 4-5  installvcs options

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-nolic</td>
<td>Install product RPMs on systems without licensing or configuration. License-based features or variants are not installed when using this option.</td>
</tr>
<tr>
<td>-nooptionalpkgs</td>
<td>Specifies that the optional product RPMs such as man pages and documentation need not be installed.</td>
</tr>
<tr>
<td>-nostart</td>
<td>Bypass starting VCS after completing installation and configuration.</td>
</tr>
<tr>
<td>-pkgpath pkg_path</td>
<td>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.</td>
</tr>
<tr>
<td>-precheck</td>
<td>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 51.</td>
</tr>
<tr>
<td>-requiredpkgs</td>
<td>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.</td>
</tr>
<tr>
<td>-responsefile</td>
<td>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 installerernumber.response where number is random. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. 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 67.</td>
</tr>
<tr>
<td></td>
<td>See “Performing automated installations” on page 69.</td>
</tr>
</tbody>
</table>
Table 4-5  installvcs options

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| -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. |
| -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 high availability agents, but offers uninstallation if proper RPM dependencies on VRTSvcs are found.

If uninstallvcs program does not remove an high availability agent, see the documentation for the specific high availability agent for instructions on removing it.

**Prerequisites**

- Before removing VCS from any node in the cluster, you must shut down applications such as the Java Console or any VCS high availability 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 99.

**Uninstalling VCS 5.1**

The example demonstrates how to uninstall VCS on two nodes: north and south.
Removing VCS 5.1 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 high availability 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 5.1 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 5.1 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 installvcs program option is -ssh. If you are performing a remote uninstallation and ssh is not enabled, run the installvcs program with the -rsh option. Otherwise, the installvcs program 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:

   ./installer [-rsh]

2 Enter u to specify uninstallation.

   Enter a Task: [I,C,L,P,U,D,?] u

   The installvcs program displays another menu that lists products that are available for uninstallation.

3 Enter the menu number that corresponds to Cluster Management Console.

   Select a product to uninstall: nn

   The installvcs 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 installvcs program presents a message stating that it will uninstall cluster connector.
Installing and configuring VCS on ESX Servers

Uninstalling VCS 5.1

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 installvcs 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 installvcs 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 installvcs program lists package dependencies and uninstallation progress percentages. If the uninstallation is successful, the program displays this message followed by the location of the uninstallation logs:
Uninstall completed successfully
Verifying VCS on ESX Servers

This chapter contains the following topics:

- About verifying the VCS installation
- Verifying LLT and GAB configuration files
- Verifying the main.cf file
- Verifying LLT, GAB, and cluster operation
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 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 llttab contains information that is derived during installation and used by the utility lltconfig. 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 (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 llttab(4) manual page for details about how the LLT configuration may be modified. The manual page describes the ordering of the directives in the llttab file.
Verifying VCS on ESX Servers

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 86.
- See “Example main.cf, for clusters with the GCO option” on page 93.

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 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.

- 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 Veritas Cluster Management Console to manage this cluster locally, the main.cf includes the VRTSWebApp resource that includes AppName = cmc attribute.

/etc/gabtab

After you install VCS, the file /etc/gabtab contains a `gabconfig` 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. Gigabit Ethernet controllers do not support the use of `-c -x`. 
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 more 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.

```bash
Main.cf:

include "types.cf"

cluster vcs {
  UserNames = { admin = IpqIpqPmqLqqOyqKpn }  
  Administrators = { admin }  
}

system sysA ()

system sysB ()

group vm2 {
  SystemList = { sysA = 0, sysB = 0 }  
  AutoStartList = { sysA }  
}

  ESXVirtualMachine vm2_ESX {
```
Verifying VCS on ESX Servers

Verifying the main.cf file

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

VMFSVolume vm2_vmfs {
  Volume = {
    
  }
}

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.vmx"
  VCserver = "648G771.example.com"
  username = v023968
  password = 123123123
  sslcert = "/etc/my.keystore"
  esxhostdomain = "veritas.com"
}

VMFSVolume vm3_vmfs {
```
Verifying VCS on ESX Servers

Verifying the main.cf file

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

// resource dependency tree
//
// group vm4
//
// SystemList = { sysA = 0 }
// AutoStartList = { sysA }

ESXVirtualMachine vm4_ESX {
  CfgFile = "*/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm4/vm4.vmx"
}

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
```
Verifying VCS on ESX Servers

Verifying the main.cf file

```c
//
//  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.vmx"
}

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
//  }
//  }
```
Verifying VCS on ESX Servers

Verifying the main.cf file

```plaintext
group vm6 {
    SystemList = { sysA = 0 }
    AutoStartList = { sysA }
}

ESXVirtualMachine vm6_ESX {
    CfgFile = 
    "/vmfs/volumes/44bcfdac-f2362ab4-a390-00093d12792b/vm6/vm6.vmx"
}

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.vmx"
}

VMFSVolume vm7_vmfs {
    Volume = {
```
Verifying VCS on ESX Servers

Verifying the main.cf file

// 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.vmx"
}

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
Verifying VCS on ESX Servers

Verifying the main.cf file

```c
//
//  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.vmx"
}

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
```
Verifying VCS on ESX Servers

Verifying LLT, GAB, and cluster operation

```
*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:
```
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>Link</th>
<th>Status</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OPEN</td>
<td>link1</td>
<td>UP</td>
<td>08:00:20:93:0E:34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>link2</td>
<td>UP</td>
<td>08:00:20:93:0E:34</td>
</tr>
<tr>
<td>1</td>
<td>OPEN</td>
<td>link1</td>
<td>UP</td>
<td>08:00:20:8F:D1:F2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>link2</td>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CONNWAIT</td>
<td>link1</td>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>link2</td>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CONNWAIT</td>
<td>link1</td>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>link2</td>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>CONNWAIT</td>
<td>link1</td>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>link2</td>
<td>DOWN</td>
<td></td>
</tr>
</tbody>
</table>
```

Note that the output lists 16 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
    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` 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 `natsys -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:

<table>
<thead>
<tr>
<th>System</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>north</td>
<td>AgentsStopped</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>AvailableCapacity</td>
<td>100</td>
</tr>
<tr>
<td>north</td>
<td>CPUUsage</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>CPUUsageMonitoring</td>
<td>Enabled 0 ActionThreshold 0</td>
</tr>
<tr>
<td>north</td>
<td></td>
<td>ActionTimeLimit 0 Action NONE</td>
</tr>
<tr>
<td>north</td>
<td></td>
<td>NotifyThreshold 0 NotifyTimeLimit 0</td>
</tr>
<tr>
<td>north</td>
<td>Capacity</td>
<td>100</td>
</tr>
<tr>
<td>north</td>
<td>ConfigBlockCount</td>
<td>142</td>
</tr>
<tr>
<td>north</td>
<td>ConfigCheckSum</td>
<td>4085</td>
</tr>
<tr>
<td>north</td>
<td>ConfigDiskState</td>
<td>CURRENT</td>
</tr>
<tr>
<td>north</td>
<td>ConfigFile</td>
<td>/etcVRTSvcs/conf/config</td>
</tr>
<tr>
<td>north</td>
<td>ConfigInfoCnt</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>ConfigModDate</td>
<td>Fri May 26 17:22:48 2006</td>
</tr>
<tr>
<td>north</td>
<td>ConnectorState</td>
<td>Down</td>
</tr>
<tr>
<td>north</td>
<td>CurrentLimits</td>
<td></td>
</tr>
<tr>
<td>north</td>
<td>DiskHbStatus</td>
<td></td>
</tr>
<tr>
<td>north</td>
<td>DynamicLoad</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>EngineRestarted</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>EngineVersion</td>
<td>5.0.20.0</td>
</tr>
<tr>
<td>north</td>
<td>Frozen</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>GUIIPAddr</td>
<td></td>
</tr>
<tr>
<td>north</td>
<td>LLTNodeId</td>
<td>0</td>
</tr>
<tr>
<td>north</td>
<td>LicenseType</td>
<td>DEMO</td>
</tr>
<tr>
<td>north</td>
<td>Limits</td>
<td></td>
</tr>
<tr>
<td>north</td>
<td>LinkHbStatus</td>
<td>vswif1 UP vswif2 UP</td>
</tr>
</tbody>
</table>
Verifying VCS on ESX Servers

Verifying LLT, GAB, and cluster operation

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoadTimeCounter</td>
<td>0</td>
</tr>
<tr>
<td>LoadTimeThreshold</td>
<td>600</td>
</tr>
<tr>
<td>LoadWarningLevel</td>
<td>80</td>
</tr>
<tr>
<td>NoAutoDisable</td>
<td>0</td>
</tr>
<tr>
<td>NodeId</td>
<td>0</td>
</tr>
<tr>
<td>OnGrpCnt</td>
<td>1</td>
</tr>
<tr>
<td>ShutdownTimeout</td>
<td>120</td>
</tr>
<tr>
<td>SourceFile</td>
<td>./main.cf</td>
</tr>
<tr>
<td>SysInfo</td>
<td>Linux:north,#1 Fri Apr 22 18:13:58 EDT 2005,2.6.9-34-default,i686</td>
</tr>
<tr>
<td>SysName</td>
<td>north</td>
</tr>
<tr>
<td>SysState</td>
<td>RUNNING</td>
</tr>
<tr>
<td>SystemLocation</td>
<td>north</td>
</tr>
<tr>
<td>SystemOwner</td>
<td></td>
</tr>
<tr>
<td>TFrozen</td>
<td>0</td>
</tr>
<tr>
<td>TRSE</td>
<td>0</td>
</tr>
<tr>
<td>UpDownState</td>
<td>Up</td>
</tr>
<tr>
<td>UserInt</td>
<td>0</td>
</tr>
<tr>
<td>UserStr</td>
<td></td>
</tr>
<tr>
<td>VCSFeatures</td>
<td>DR</td>
</tr>
<tr>
<td>VCSMode</td>
<td>VCS</td>
</tr>
</tbody>
</table>
Adding and removing cluster nodes

This chapter contains the following topics:

- About adding and removing nodes
- Adding a node to a cluster
- Removing a node from a cluster
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 16 nodes.

Adding nodes

You must add a node to VCS cluster before you add the same node to the VMware cluster. This prevents DRS from automatically moving a virtual machine to a host that does not have VCS.

Removing nodes

You must delete a node from the VMware cluster before you remove the same node from VCS cluster. This prevents DRS from automatically moving a virtual machine to a node that does not have VCS.

In order to remove a node from a DRS cluster, you need to put it into maintenance mode. You then remove it from the VMware DRS cluster. The ESXHost agent detects this state change and internally performs a VCS system freeze command with the evacuate option.

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 33.

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>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the hardware.</td>
<td>“Setting up the hardware” on page 101</td>
</tr>
<tr>
<td>Install the software manually.</td>
<td>“Installing VCS software manually” on page 119</td>
</tr>
<tr>
<td>Add a license key.</td>
<td>“Adding a license key” on page 103</td>
</tr>
<tr>
<td>Configure LLT and GAB.</td>
<td>“Configuring LLT and GAB” on page 103</td>
</tr>
</tbody>
</table>
### Adding a node to a cluster

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add the node to the existing cluster.</td>
<td>“Adding the node to the existing cluster” on page 105</td>
</tr>
<tr>
<td>Start VCS and verify the cluster.</td>
<td>“Starting VCS and verifying the cluster” on page 105</td>
</tr>
<tr>
<td>Add the node to the VMware cluster.</td>
<td>“Adding the node to the VMware cluster” on page 106</td>
</tr>
</tbody>
</table>

### 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 illustrates a new node being added to an existing three-node cluster using two independent switches or hubs.

Figure 6-1 Adding a node to a three-node cluster using two independent switches
Adding and removing cluster nodes

Adding a node to a cluster

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

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-4.3.26.9-9.1386.rpm
   # VRTSatServer-4.3.26.9-9.1386.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
   # VRTSjre15-1.5.1.3-3.i386.rpm
   # VRTSllt-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSgab-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSvcs-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSvcsmg-5.0.20.00-GA_GENERIC.noarch.rpm
   # VRTSvcsmag-5.0.20.00-GA_ESX30.i686.rpm
   ```
Adding and removing cluster nodes

Adding a node to a cluster

# VRTSvcsesx-5.1.20.00-GA_ESX30
# VRTSweb-5.0.1-GA4_GENERIC.noarch.rpm
# VRTSvcsmn-5.0.20.00-GA_GENERIC.noarch.rpm
# VRTScssim-5.0.20.00-GA_ESX30.i686.rpm
# VRTScmcs-5.0.00.00-GA_ESX.i686.rpm
# VRTScmccc-5.0.00.00-GA_ESX.i686.rpm
# VRTSvcsdns-5.0.20.00-GA_ESX30.i686.rpm
# VRTSvcs-5.0.20.00-GA_ESX30.i686.rpm
# VRTSvcsvmip-5.0.20.00-GA_ESX30.i686.rpm
# VRTSvcsvisdk-5.0.20.00-GA_ESX30.i686.rpm
# VRTSvcsctl-5.1.20.00-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
Adding and removing cluster nodes

Adding a node to a cluster

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 84.
   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 -nN 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 85.
     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 95.
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
   ```
Adding the node to the VMware cluster

From the VMware Infrastructure client add the exact node that you added to the VCS cluster.

For more information on adding a node to a VMware cluster, refer to the VMware documentation.

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>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Back up the configuration file.</td>
<td>“Verify the status of nodes and service groups” on page 107</td>
</tr>
<tr>
<td>■ Check the status of the nodes and the service groups.</td>
<td></td>
</tr>
</tbody>
</table>

Remove the node from the VMware cluster.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Switch or remove any VCS service groups on the node departing the cluster.</td>
<td>“Deleting the departing node from VCS configuration” on page 107</td>
</tr>
<tr>
<td>■ Delete the node from VCS configuration.</td>
<td></td>
</tr>
</tbody>
</table>

Modify the llthosts and gabtab files to reflect the change.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Modify startup scripts for LLT, GAB, and VCS to allow reboot of the node without affecting the cluster.</td>
<td>“Modifying configuration files on each remaining node” on page 109</td>
</tr>
<tr>
<td>■ Unconfigure and unload the LLT and GAB utilities.</td>
<td></td>
</tr>
<tr>
<td>■ Remove the VCS RPMs.</td>
<td>“Unloading LLT and GAB and removing VCS on the departing node” on page 110</td>
</tr>
</tbody>
</table>
Adding and removing cluster nodes

Removing a node from a cluster

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.

   ```bash
   # 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.

   ```bash
   # hastatus -summary
   ```

   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 node from the VMware cluster

From the VMware Infrastructure client delete the exact node that you deleted from the VCS cluster.

For more information on deleting a node to a VMware cluster, refer to the VMware documentation.

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
   ```
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
```

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

```
# hagrp -delete grp4
```

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
```

Delete the node from the cluster.

```
# hasys -delete C
```

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 -nN option, where N is the number of cluster systems.
   If the command has the form /sbin/gabconfig -c -nN, where N is the number of cluster systems, 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.
Removing a node from a cluster

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:

   # VRTSvcsstc-5.1.20.00-GA_ESX30.i686.rpm
   # VRTSvcsvisdk-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSvcsvmip-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSvcsams-5.0.20.00-GA_ESX30.i686.rpm
   # VRTScmccc-5.0.00.00-GA_ESX.i686.rpm
   # VRTScmscs-5.0.00.00-GA_ESX.i686.rpm
   # VRTScssim-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSvcsmm-5.0.20.00-GA_GENERICS.noarch.rpm
   # VRTSweb-5.0.1-GA4 GENERIC noarch.rpm
   # VRTSvcsesx-5.1.20.00-GA_ESX30
   # VRTSvcsag-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSvcsmsg-5.0.20.00-GA_GENERICS.noarch.rpm
   # VRTSvcs-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSgb-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSllt-5.0.20.00-GA_ESX30.i686.rpm
   # VRTSjre15-1.5.1.3-3.1386.rpm
   # VRTSjlic-3.02.18.0-0.1686.rpm
   # VRTSext-5.0.00.2-GA.noarch.rpm
   # VRTSperl-5.0.2.1-linux.i386.rpm
   # VRTSatServer-4.3.26.9-9.1386.rpm
   # VRTSatClient-4.3.26.9-9.1386.rpm
4 Remove the LLT and GAB configuration files.

# rm /etc/llttab
# rm /etc/gabtab
# rm /etc/llthosts
Removing a node from a cluster
Installing VCS on a single node

This chapter contains the following topics:

- About installing VCS on a single node
- Creating a single-node cluster using the installvcs program
- Creating a single-node cluster manually
- Adding a node to a single-node cluster
About installing VCS on a single node

You can install VCS 5.1 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 installvcs program or you can add it manually.

See “Creating a single-node cluster using the installvcs program” on page 114.
See “Creating a single-node cluster manually” on page 115.

Creating a single-node cluster using the installvcs program

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for installation.</td>
<td>“Preparing for a single node installation” on page 114</td>
</tr>
<tr>
<td>Install the VCS software on the system using the installvcs program.</td>
<td>“Starting the installvcs program for the single node cluster” on page 115</td>
</tr>
</tbody>
</table>

Preparing for a single node installation

You can use the installvcs 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 19.
Starting the installvcs program for the single node cluster

When you install VCS on a single system, follow the instructions in this guide for installing VCS using the installvcs program.

See “Starting the software installation” on page 52.

During the installation, you need to answer two questions specifically for single node installations. When the installvcs program asks:

- Enter the system names separated by spaces on which to install VCS:

Enter a single system name. The installvcs program 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 53.

Creating a single-node cluster manually

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the PATH variable</td>
<td>“Setting the PATH variable” on page 116</td>
</tr>
<tr>
<td>Install the VCS software manually and add a license key</td>
<td>“Installing VCS RPMs for a manual installation” on page 116 “Adding a license key” on page 117</td>
</tr>
<tr>
<td>Remove any LLT or GAB configuration files and rename LLT and GAB startup files.</td>
<td>“Renaming the LLT and GAB startup files” on page 117</td>
</tr>
</tbody>
</table>

A single-node cluster does not require the node-to-node communication service, LLT, or the membership communication service, GAB.
### Creating a single-node cluster manually

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the VCS startup file for single-node operation.</td>
<td>“Modifying the startup files” on page 118</td>
</tr>
<tr>
<td>Create and modify the VCS configuration files.</td>
<td>“Configuring VCS” on page 118</td>
</tr>
<tr>
<td>Start VCS and verify single-node operation.</td>
<td>“Verifying single-node operation” on page 119</td>
</tr>
</tbody>
</table>

### 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:
    ```bash
    $ PATH=/usr/sbin:/sbin:/opt/VRTS/bin:/opt/VRTSvcs/bin: \n    $PATH; export PATH
    ```
  - For the C Shell (csh or tcsh), type:
    ```bash
    % setenv PATH /usr/sbin:/sbin:/opt/VRTS/bin:
    /opt/VRTSvcs/bin:$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 (VRTSscw) 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-3.02.18.0-0.1686.rpm
#VRTSjre15-1.5.1.3-3.i386.rpm
#VRTSllt-5.0.20.00-GA_ESX30.i686.rpm
#VRTSgab-5.0.20.00-ESX30.i686.rpm
#VRTSvcs-5.0.20.00-ESX30.i686.rpm
#VRTSvcsag-5.0.20.00-ESX30.i686.rpm
#VRTSvcsesx-5.1.20.00-ESX30
#VRTSweb-5.0.1-GA GENERIC.noarch.rpm
#VRTSvcsesx-5.1.20.00-ESX30
#VRTSvcs-5.0.20.00-ESX30.i686.rpm
#VRTSvcs-5.0.20.00-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.
Installing VCS on a single node

Creating a single-node cluster manually

To rename the LLT and GAB startup files

- Rename the LLT and GAB startup files.
  
  ```bash
  # 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 `-onemode` 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:
   ```bash
   # 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:

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

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

```plaintext
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` with the `-onenode` option:
   ```bash
   # hastart -onenode
   ```

2. Verify that the had and hashadow daemons are running in single-node mode:
   ```bash
   # 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up Node B to be compatible with Node A.</td>
<td>“Setting up a node to join the single-node cluster” on page 121</td>
</tr>
<tr>
<td>■ Add Ethernet cards for private heartbeat network for Node B.</td>
<td>“Installing and configuring Ethernet cards for private network” on page 121</td>
</tr>
<tr>
<td>■ If necessary, add Ethernet cards for private heartbeat network for Node A.</td>
<td></td>
</tr>
<tr>
<td>■ Make the Ethernet cable connections between the two nodes.</td>
<td></td>
</tr>
<tr>
<td>Connect both nodes to shared storage.</td>
<td>“Configuring the shared storage” on page 122</td>
</tr>
<tr>
<td>■ Bring up VCS on Node A.</td>
<td>“Bringing up the existing node” on page 122</td>
</tr>
<tr>
<td>■ Edit the configuration file.</td>
<td>“Installing VCS RPMs for a manual installation” on page 116</td>
</tr>
<tr>
<td>■ Edit the startup scripts.</td>
<td>“Adding a license key” on page 117</td>
</tr>
<tr>
<td>If necessary, install VCS on Node B and add a license key.</td>
<td>“Installing VCS RPMs for a manual installation” on page 116</td>
</tr>
<tr>
<td>Make sure Node B is running the same version of VCS as the version on Node A.</td>
<td>“Adding a license key” on page 117</td>
</tr>
<tr>
<td>Edit the configuration files on Node B.</td>
<td>“Configuring LLT and GAB” on page 123</td>
</tr>
<tr>
<td>Start LLT and GAB on Node B.</td>
<td>“Starting LLT and GAB” on page 125</td>
</tr>
<tr>
<td>■ Start LLT and GAB on Node A.</td>
<td>“Reconfiguring VCS on the existing node” on page 125</td>
</tr>
<tr>
<td>■ Restart VCS on Node A.</td>
<td></td>
</tr>
<tr>
<td>■ Modify service groups for two nodes.</td>
<td></td>
</tr>
<tr>
<td>■ Start VCS on Node B.</td>
<td>“Verifying configuration on both nodes” on page 126</td>
</tr>
<tr>
<td>■ Verify the two-node cluster.</td>
<td></td>
</tr>
</tbody>
</table>
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

◆ Do one of the following:
  ■ 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 106.
  ■ If the node you plan to add as Node B is also currently a single VCS node, uninstall VCS. See “Uninstalling VCS 5.1” on page 79.
  ■ If you renamed the LLT and GAB startup files, remove them. See “Renaming the LLT and GAB startup files” on page 117.

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 37.

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.
Adding a node to a single-node cluster

Configuring the shared storage

Make the connection to shared storage from Node B. Reboot the node when you are prompted.

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 VCS on a single node

Installing the VCS RPMs and license key

Install the VCS 5.1 RPMs manually and install the license key.
See "Installing VCS RPMs for a manual installation" on page 116.
See "Adding a license key" on page 117.

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/llttab on each node in the cluster.

Setting up /etc/llthosts

The file llthosts 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/llttab

The /etc/llttab 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 llttab file in /opt/VRTSllt.
See "LLT directives" on page 124.
Using vi or another editor, create the file /etc/llttab that contains entries that resemble:

```
set-node north
set-cluster 2
link vswwifi1 eth-00:50:56:41:07:c1 - ether -
link vswwifi2 eth-00:50:56:58:54 - 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
Installing VCS on a single node

Adding a node to a single-node cluster

network cards that the LLT protocol uses. The order of directives must be the same as in the sample file /opt/VRTSlt/lttab.

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

<table>
<thead>
<tr>
<th>Table 7-4</th>
<th>LLT directives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directive</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>set-node</td>
<td>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/ljthosts file. Note that LLT fails to operate if any systems share the same ID.</td>
</tr>
<tr>
<td>link</td>
<td>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 lttstat output to identify the link. It may also be used in lttab 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 lttab(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.</td>
</tr>
<tr>
<td>set-cluster</td>
<td>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.</td>
</tr>
<tr>
<td>link-lowpri</td>
<td>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.</td>
</tr>
</tbody>
</table>

For more information about LLT directives, refer to the lttab(4) manual page.
Installing VCS on a single node

Adding a node to a single-node cluster

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 -n
```
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
   ```
Installing VCS on a single node

Adding a node to a single-node cluster

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
Upgrading to VCS 5.1

This chapter includes the following topics:

- About upgrading to VCS 5.1
- Upgrading VCS on ESX Server nodes
- Upgrading the Veritas Virtual Machine Tools on virtual machines
- Completing the VCS upgrade on the ESX Server nodes
About upgrading to VCS 5.1

Use the installvcs program to upgrade the ESX Server nodes where VCS runs. You must then use Veritas Virtual Machine Tools to upgrade the virtual machines. You need to then return the ESX Server nodes to start VCS and unfreeze service groups.

Figure 8-1 on page 128 illustrates a VCS for VMware ESX upgrade.

Figure 8-1 Recommended upgrade flow

- Upgrade VCS on ESX Server nodes.
- Upgrade the Veritas Virtual Machine Tools.
- Finish the ESX Server upgrade by unfreezing service groups.

Table 8-1 on page 128 describes where to look for the pertinent road map information.

Table 8-1 Installation road map

<table>
<thead>
<tr>
<th>Road map entry</th>
<th>Document or chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the VCS on ESX Server node upgrade.</td>
<td>See “Upgrading VCS on ESX Server nodes” on page 128.</td>
</tr>
<tr>
<td>Upgrade Veritas Virtual Machine Tools on each virtual machine.</td>
<td>See “Upgrading the Veritas Virtual Machine Tools on virtual machines” on page 133.</td>
</tr>
<tr>
<td>Complete the VCS on ESX Server node upgrade.</td>
<td>See “Completing the VCS upgrade on the ESX Server nodes” on page 135.</td>
</tr>
</tbody>
</table>

Upgrading VCS on ESX Server nodes

On a VCS cluster, or a VCS global cluster, you can run the installvcs program to upgrade to VCS 5.1. The program detects the current configuration and prompts you to indicate whether you want to upgrade. While the installation program is not able to verify the validity of the existing configuration, it is able to run extensive upgrade requirement checks. The example upgrade demonstrates how to upgrade VCS 5.1 on nodes north and south.

See “About the VCS installation program” on page 48.
Starting the upgrade

Start the installvcs program to automatically upgrade the cluster nodes.

To start the upgrade

1. Log in as superuser.
2. Mount the software disc.
3. Ensure that the VCS high-availability daemon (HAD) is running.
   
   ```
   # /bin/ps -ef | grep had
   ```
4. On the node where you mounted the disk, change directory to the cluster_server directory and start the installation program:
   
   ```
   # ./installvcs
   ```
   See “Starting the software installation” on page 52.
5. Review the copyright notice and note the location for the installation program log. You can use the tail command to monitor the upgrade as it progresses.
   
   For example, if the program created the log in this directory /var/tmp/ installer-abc. You change into the directory, start a new terminal window, and enter the following command:
   
   ```
   # tail -f installer-abc.log
   ```
6. After the installvcs program displays the current cluster information, review the report. This report includes the ClusterService group, if it is defined:
   
   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 XYZ_group
   ```
   No checks have been made to ensure the validity of the configuration.
   VCS version 5.0.10.00 is installed on this system
7. To upgrade to VCS 5.1, press the **Enter** key.
   
   Do you want to upgrade to version 5.1 on these systems using the current configuration? [y,n,q,?] (y) **y**

Checking upgrade requirements

The installation program verifies that your systems meet the requirements for upgrading.
To check upgrade requirements

1 Review the output as the program verifies that the upgrade can proceed on the nodes.

The installvcs program checks the operating system level and system-to-system communication. It also creates logs for the VCS update.

installvcs requires that ssh commands used between systems execute without prompting for passwords or confirmations. If installvcs hangs or asks for a login password or hangs, stop installvcs and run it again with the ssh configured for passwordless logins, or configure rsh and use the -rsh option.

Checking ssh communication with north......................Linux 2.4.21-37.0.2.ELvmunix
Checking VCS installation on north...................... 5.0.10.00
Checking kernel release on north...................... 5.0.10.00
.
.
.

2 Review the output as the installvcs program checks the licenses that are currently in place on the cluster nodes.

The program also prompts you to add additional license keys:

Checking system licensing

Installing licensing rpms

VCS license registered on north

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

VCS license registered on south

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

Upgrading VCS 5.0 packages to VCS 5.1 RPMs

The installation program is ready to remove the RPMs from VCS version 5.0 and install the 5.1 RPMs on each node after verifying the requirements.

To add 5.1 RPMs

1 Review the output as the installvcs program checks for existing RPMs.

Checking installed rpms on north
Checking installed rpms on south

2 The installvcs program lists the RPMs for the upgrade. Press Enter at the prompt.

VRTSperl Veritas Perl 5.8.8 Redistribution
VRTSvlic Veritas Licensing
VRTSatClient Symantec Product Authentication Service Client
VRTSatServer Symantec Product Authentication Service
Upgrading to VCS 5.1

Upgrading VCS on ESX Server nodes

VRTSspt  Veritas Software Support Tools
VRTSllt  Veritas Low Latency Transport
VRTSgab  Veritas Group Membership and Atomic Broadcast
VRTSvcs  Veritas Cluster Server
VRTSvcsmsg  Veritas Cluster Server Message Catalogs
VRTSvcsag  Veritas Cluster Server Bundled Agents
VRTSvcsmm  Veritas Cluster Server Man Pages
VRTSjre  Veritas Java Runtime Environment Redistribution
VRTSjre15  Veritas Java Runtime Environment Redistribution
VRTScssim  Veritas Cluster Server Simulator
VRTSwesb  Veritas Java Web Server
VRTScmcsc  Veritas Cluster Management Console for single cluster environments
VRTScmcc  Veritas Cluster Management Console cluster connector
VRTSvcsvmip  VERITAS Cluster Server Virtual Machine IP agent for VMware ESX
VRTSvcsdns  VERITAS Cluster Server DNS update agent for VMware ESX
VRTSvcsvisdk  Veritas Cluster Server Virtualization SDK for VMware ESX
VRTSvcs  VERITAS Clustering Support for Hitachi TrueCopy(tm)
VRTScsc  VERITAS Cluster Support for Hitachi TrueCopy(tm)
VRTSvcsesx  VERITAS Cluster ESX Host agent

Press [Enter] to continue:

3  The program can now upgrade VCS. Press Enter at the prompt to continue.

installvcs is now ready to upgrade VCS.
Are you sure you want to upgrade VCS? [y,n,q] (y) y
Updating gabtab on north............................ Done

installvcs must now make configuration updates and stop the cluster before upgrading VCS rpms
Are you ready to begin the Veritas Cluster Server upgrade at this time? [y,n,q] (y) y

4  Review the output as the program backs up the types.cf and main.cf and freezes the service group configured in the cluster.

Backing up types.cf and main.cf............................ Done
Freezing group XYZ_group................................. Done
Updating types.cf file ...................................... Done
Updating gabtab on north.................................... Done
Updating gabtab on south.................................... Done

The program then performs the following actions:

- It stops VCS and uninstalls the RPMs. Progress indicators show the status of these tasks.
- It installs VCS 5.1 RPMs. A progress indicator shows the status of the task.
Upgrading to VCS 5.1
Upgrading VCS on ESX Server nodes

- It configures the ESX service console firewall on the nodes by opening the required ports.
  See “Service console firewall ports that installvcs opens during installation” on page 46.

ESX network configuration

The installvcs program now generates keystore files for secure and password free agent communications.

To configure the ESX network configuration

1. The installvcs program asks if want to keep the default SSL certificate that is used to generate the keystore. Answer y to accept the default.
   Do you want to use default ssl cert to generate keystore on north? [y,n,q] (y)
   y

2. Enter a password for the keystore for the first system.
   Enter keystore password, not less than 6 characters:
   Re-type the password:

3. Enter the password for the root user on the first system:
   Enter the password for user root on host north:
   Re-type the password:

4. If you have the same root password on all the nodes in the cluster, answer y.
   The installvcs program generates the security credentials across all the systems in the cluster.
   Do you want to use the same root and keystore password on the other hosts? [y,n,q] (y)
   y
   If you use different root passwords on any of the nodes in the cluster, installvcs prompts you for those.
   Installvcs now generates the security credentials for VCS agents.
   Generating security credentials for VCS agents ............ Done

5. The installvcs program starts VCS and terminates. You are not done with the ESX Server cluster upgrade. You must now upgrade the virtual machines.
   After you upgrade the virtual machines, you must finish the upgrade for the ESX Server cluster unfreezing the service groups.
   See “Upgrading the Veritas Virtual Machine Tools on virtual machines” on page 133.
Upgrading the Veritas Virtual Machine Tools on virtual machines

After upgrading the VCS nodes to 5.1, upgrade each virtual machine.

Upgrading Linux virtual machines

You must upgrade each virtual machine individually.

To upgrade a virtual machine to VCS 5.1
1. Mount the product disc.
2. Navigate to the installvcsvm-tools location.
   cd /media/cdrom/installvcsvm-tools
3. On the virtual machine, enter the installvcsvm-tools -n command.
   ./installvcsvm-tools -n
4. You now must now finish the upgrade for the ESX Server cluster.
   See “Completing the VCS upgrade on the ESX Server nodes” on page 135.

Upgrading Windows virtual machines

You must upgrade each virtual machine individually.

The upgrade utility is on the disc inside the vcsvm_tools directory. It is in the ISO format:

- For x86 (32-bit) architectures, use:
  win-x86-vcsvm-tools.iso
- For x64 architectures, use:
  win-x64-vcsvm-tools.iso

To add the Tools .iso file
1. From a Windows client, click Start > Programs > Symantec > 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.
   The Add CD-ROM ISO window appears.
3. Click the OK button to add the .iso file.
   The ISO file is now available for your use.
To upgrade the Veritas Virtual Machine Tools

1. Once you have mounted the appropriate ISO file to your virtual machine, run the vcsvm-tools.exe file to upgrade the Tools.

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.
   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)

12 You now must now finish the upgrade for the ESX Server cluster.  
   See “Completing the VCS upgrade on the ESX Server nodes” on page 135.

Completing the VCS upgrade on the ESX Server nodes

Unfreeze the service groups.

To unfreeze and bring service groups online

1 After VCS has started on all nodes, verify all resources have been probed. On any node, type:  
   # hastatus -summary

2 Find the section that begins with:
   -- -- GROUPS FROZEN
   This section contains a list of all the frozen service groups. Note the frozen service groups.

3 Unfreeze all frozen service groups. On any node, type:
   # haconf -makerw
   # hagrp -unfreeze service_group1 -persistent
   # hagrp -unfreeze service_group2 -persistent
   # hagrp -unfreeze service_group3 -persistent
   .
   .
   .
   # haconf -dump -makero

4 Bring the service groups online, if necessary. On any node type:
   # hagrp -online service_group -sys node
Upgrading to VCS 5.1

Completing the VCS upgrade on the ESX Server nodes
Configuring VCS for virtual machines

This section contains the following chapters:

- Chapter 9, “Installing the Veritas Virtualization Manager (VVM)” on page 139
- Chapter 10, “Configuring virtual machines for high availability” on page 149
- Chapter 11, “Configuring virtual machines for disaster recovery” on page 155
Installing the Veritas Virtualization Manager (VVM)

This chapter contains the following topics:

■ About Veritas Virtualization Manager (VVM)
■ Installing the Veritas Virtualization Manager (VVM)
■ Preparing keystores
■ Starting the Veritas Virtualization Manager (VVM)
■ Removing the Veritas Virtualization Manager (VVM)
About Veritas Virtualization Manager (VVM)

The Veritas Virtualization Manager (VVM) is a user interface that enables you to configure virtual machines for high availability, disaster recovery, and to increase allocated storage for a virtual machine.

After you start the application, VVM presents a hierarchy of objects in the left side of the pane, 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 to perform the following tasks:

■ Configure virtual machines for high availability.
  See “Configuring virtual machines for high availability using the Veritas Virtualization Manager” on page 150.

■ Configure a virtual machine for disaster recovery.
  See “Configuring virtual machines for disaster recovery using the Veritas Virtualization Manager” on page 165.

■ Manage service groups using the Cluster Server (Java Console).
  Right-click a cluster and select Launch VCS Console. This full-featured Java Console is part of VVM. You cannot access this version of the Java Console through the Start menu.
  For a stand-alone Java Console that you can access through the Start menu, install the Java Console.
  See “Installing the Cluster Manager (Java Console)” on page 65.
  For information about using the Java Console, refer to the Veritas Cluster Server User's Guide.
Installing the Veritas Virtualization Manager (VVM)

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 a Pentium III at 400 MHz, with 256 MB RAM. Minimum hardware requirements follow:

- Pentium II 300 megahertz CPU
- 256 megabytes RAM
- 800 x 600 display resolution
- 8-bit color display depth
- Graphics card capable of 2D images
- Approximately 40 MB of free hard drive space

Installing the Veritas Virtualization Manager

Install the Veritas Virtualization Manager on a standalone Windows system that is outside of the cluster.

To install the Veritas Virtualization Manager

1. Insert the product disc into a drive on the client system.
2. Change directory to windows/vvm.
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 keystores

The Veritas Virtualization Manager (VVM) requires a VMware keystore (generated from a SSL certificate) to connect and communicate with the VirtualCenter Server. The keystore secures communication between the system where VVM runs and the VirtualCenter Server.

The following is an example of how to set up the required keystore. For each VirtualCenter Server that you have deployed, you need a keystore file on each system where you plan to run VVM. You must also copy this generated keystore file on to all of the ESX Server nodes that are in the VCS cluster.

**Figure 9-2** Preparing the keystore file (SSL Certificate)

1. 
   
   rui.crt + keytool.exe + **Server name** + **Keystore file**

2. **VirtualCenter Servers**
   
   **vc-server1**
   
   Move the keystore to the VVM system.
Finding the path information on the VirtualCenter Server

You need some basic information for the keytool.exe and the rui.crt files on the VirtualCenter Server.

To find and note the path to the keytool.exe executable

1. On the VirtualCenter Server (vc-server1), locate the keytool.exe executable. The keytool.exe file is commonly in: C:\Program Files\Common Files\VERITAS Shared\VRTS\jre1.5\bin. Some systems may have this file in a different directory. In this situation, use the Windows search feature to locate the file. If multiple jre directories exist, find the file that is in the version 1.5 directory.

2. On the VirtualCenter Server (vc-server1), copy the path information for the file to a temporary file. In this example, the path information resembles: "C:\Program Files\Common Files\VERITAS Shared\VRTS\jre1.5\bin\keytool.exe"
   Remember to add the file name—keytool.exe—and quotes at the beginning and end of the path.

To find and note the path to the rui.crt certificate file

1. On the VirtualCenter Server (vc-server1), locate the rui.crt certificate file. The rui.crt file is commonly in: C:\Program Files\VMware\VMware Server\SSL. Some systems may have this file in a different directory. In this situation, use the Windows search feature to locate the file.

2. On the VirtualCenter Server (vc-server1), copy the path information for the file to a temporary file. In this example, the path information resembles: "C:\Program Files\VMware\VMware Server\SSL\rui.crt"
   Remember to add the file name—rui.crt—and quotes at the beginning and end of the path. If for any reason, the rui.crt file does not exist, refer to VMware SDK documentation.

To generate (import) the keystore

1. On the VirtualCenter Server (vc-server1), open a command line prompt.

2. Click Start > Run.

3. In the Run dialog, enter cmd in the Open field. Click the OK button.

4. From the command line, make sure that you are at root. At the prompt, type:
   C:\>cd \

5. To make it easy to find the file that you generate, create a temporary directory and open it.
   C:\>mkdir \tempkeystore
   C:\>cd tempkeystore
At the prompt type the following command.

```
"path_to_keytool\keytool.exe" -import -file
"path_to_rui.crt" -alias server-name -keystore
"path_to_keystorefile\vmware.keystore"
```

A full command example is:

```
"C:\Program Files\Common Files\VERITAS Shared\VRTSjre\jre1.5\bin\keytool.exe" -import -file "C:\Program Files\VMware\VMware Server\SSL\rui.crt" -alias vc-server1 -keystore
vc-server1.keystore
```

- **path_to_keytool**: The pathname and the executable for the keytool (keytool.exe) is the path from root to the keytool.exe file that you found in the previous procedure. "C:\Program Files\Common Files\VERITAS Shared\VRTSjre\jre1.5\bin\keytool.exe" in this example. Start and end the path and file name with quotes.

- **path_to_rui.crt**: The pathname and the certificate file leads to the rui.crt certificate file ("C:\Program Files\VMware\VMware Server\SSL\rui.crt" in this example). Start and end this path and file name with quotes.

- **server-name**: The server-name is the name of the VirtualCenter Server (vc-server1 in this example).

- **vmware.keystore**: The certificate store that you are creating (vc-server1.keystore in this example). If you do not specify the absolute path to this file, it is created in the current directory.

When you enter the password for the keystore use the same password as the one that you use to log on to the VirtualCenter Server. Press the Enter key.

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

Creating the certificate store for the Veritas Virtualization Manager

The certificate store is a directory that you create to hold keystore files. For convenience’s sake, consider using identical certificate store names on each system where you plan to install and use VVM.

**To create the certificate store**

1. Where you have installed VVM, create the new certificate store directory.

2. Open a command prompt on the VirtualCenter Server. Click Start > Run.

3. In the Run dialog, enter cmd in the Open field. Click the OK button.
145

Installing the Veritas Virtualization Manager (VVM)

Preparing keystores

4 From the command line, make sure that you are at root. At the prompt, type:
   ```cmd
   C:\> cd \n   ```

5 Create a directory to hold the keystore file. For example, at the prompt type:
   ```cmd
   C:\> mkdir certificate-store
   ```
   Where certificate-store is the name of the new directory and the certificate
   store.

   Copying the keystore file from the VirtualCenter Server to the
   Veritas Virtualization Manager (VVM)

   You now need to copy the keystore file onto the system where you plan to use
   VVM. The certificate file must be on each client where you plan to use VVM.

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

   1 Copy the keystore file that you have created on the VirtualCenter Server to
      the new directory that you created on the system where you plan to run
      VVM.

   2 When you log into VVM, it asks for authentication information including
      the path to the certificate store (in the example,
      C:\certificate-store\vc-server1.keystore).

   Copying the keystore file from the VirtualCenter Server to each of
   the ESX Sever nodes in the VCS cluster

   For VMotion to work in a VCS environment, the VCS nodes need access to the
   keystore file. Copy the keystore file to the same location on each of the ESX
   Server nodes that are in the cluster. For example, place the keystore file in the
   /etc/VRTSvcs/conf/ directory. When you configure the ESXVirtualMachine
   agent, you must configure the sslcert attribute to point to this keystore file.

   Starting the Veritas Virtualization Manager (VVM)

   Figure 9-3 shows the VirtualCenter Server name, the username and password
   for the VirtualCenter Server, and the SSL certificate path to the keystore file.
To start the Veritas Virtualization Manager

1. From a Windows client, click **Start > Programs > Symantec > 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

1. Enter the path information to the keystore for the VirtualCenter Server. For example, enter: `C:\certificate-store\vc-server1.keystore`.
   See “Finding the path information on the VirtualCenter Server” on page 143.

For more information about the tasks that VVM can perform:

See “About Veritas Virtualization Manager (VVM)” on page 140.

### Removing the Veritas Virtualization Manager (VVM)

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

To remove the Veritas Virtualization Manager

1. From the Windows system, 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.
Upgrading the Veritas Virtualization Manager (VVM)

Use Windows Add or Remove program functionality to remove the previous version of VVM. Run the vcsvm.msi file to install the latest version of VVM.

See "Removing the Veritas Virtualization Manager (VVM)" on page 146.

See "Installing the Veritas Virtualization Manager (VVM)" on page 141.
Installing the Veritas Virtualization Manager (VVM)

Upgrading the Veritas Virtualization Manager (VVM)
Chapter 10

Configuring virtual machines for high availability

This chapter contains the following topics:

- About configuring virtual machines
- Configuring virtual machines for high availability using the Veritas Virtualization Manager
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.

Configuring virtual machines for high availability using the Veritas Virtualization Manager

You can take existing virtual machines that are part of a VMware cluster, and configure them into virtual machines that run under VCS. Use one of the following procedures:

- See “To configure one virtual machine for high availability” on page 151.
- See “To configure multiple virtual machines for high availability” on page 151.

Prerequisites for configuring virtual machines for high availability

Before you start, ensure that:

- The hardware for the cluster 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.
- You have disabled VMware HA on the target clusters.
- The nodes are part of a VMware cluster.
- The ESX nodes that form a VCS ESX cluster are present and configured in the VirtualCenter Server as a corresponding VC Server cluster.
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 keystores” on page 142.

To start the virtual machine deployment
1. From a Windows client, click Start > Programs > Symantec > 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 146.

To configure one 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. Review the next window, and click the Next button.
3. 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.
4. Choose to configure a new administrator. This user is the person who you want to administer the application and the service group that VVM creates when you complete this wizard. Note the name and password for future reference.
   Click the Next button to proceed.
5. Review the configuration summary.
   - Click on the summary item in the right-column 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 made the virtual machine highly available.

To configure multiple virtual machines for high availability
1. Right-click the cluster that contains the virtual machines that you want to make highly available.
   From the pull-down menu, select Configure HA.
2. Review the next window, and click the Next button.
3 Check the boxes next to the virtual machines that you want to configure. Click the Next button.

4 Review the names.
   - Click on an item to edit it. Note that some items cannot be edited.
   - Click the Back button to go back and change any values.
   - Click the Next button to finalize the configuration for the virtual machines.

You have now made the selected virtual machines 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 has an ESXVirtualMachine resource that depends on its storage and network 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:

- “Configuring applications and resources in Windows virtual machines” on page 217
- “Configuring applications and resources in Linux virtual machines” on page 177

In Figure 10-1, you can see a basic example of a resource dependency graph for a service group.

**Figure 10-1** 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, Veritas Cluster Management Console, Cluster Server (Java 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, refer to 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.
Configuring virtual machines for high availability using the Veritas Virtualization Manager
Configuring virtual machines for disaster recovery

This chapter contains the following topics:

- About VCS global clusters
- Setting up a global cluster manually
- Configuring virtual machines for disaster recovery using the Veritas Virtualization Manager
- Verifying virtual machine failover
- Fire drills
About VCS global clusters

Local clustering provides local failover for each site or building. Local clusters do not, however, provide protection against large-scale disasters for an entire city or region.

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

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 11-1 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.

**Note:** You cannot use raw device mapping (RDM) in a disaster recovery-enabled environment.

---

**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, refer to 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 Veritas 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
Configuring virtual machines for disaster recovery
Setting up a global cluster manually

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.
Configuring virtual machines for disaster recovery

Setting up a global cluster manually

Sample configuration

```bash
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.
Configuring the second cluster

1. Configure the ClusterService group in the second cluster. See “Configuring the ClusterService group” on page 160.

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. Provide cluster connection information:
   - 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.
5. Click Finish.
   The cluster icon changes to indicate that the cluster is a global cluster.

Creating the global service group

Use the 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 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.
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**.

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.

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 **Existing 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).

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

Click **Next**.

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 158.
Overview of tasks

Table 11-1 Configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review prerequisites.</td>
<td>See “Prerequisites for configuring virtual machines for disaster recovery” on page 167.</td>
</tr>
<tr>
<td>Set up secure DNS update.</td>
<td>See “Setting up secure DNS update” on page 167.</td>
</tr>
<tr>
<td>Use VVM to configure virtual machines for disaster recovery.</td>
<td>See “Using Veritas Virtualization Manager to configure virtual machines for disaster recovery” on page 168.</td>
</tr>
<tr>
<td>On the primary site, deploy the Tools and applications.</td>
<td>See “Deploying VCS components on the virtual machines in the primary site” on page 170.</td>
</tr>
<tr>
<td>Confirm the availability of the service group.</td>
<td>See “Confirming service group availability” on page 170.</td>
</tr>
<tr>
<td>Reverse the direction of replication.</td>
<td>See “Reversing the direction of replication” on page 170.</td>
</tr>
<tr>
<td>On the secondary site, use VVM to configure the virtual machines.</td>
<td>See “Using VVM to configure virtual machines for disaster recovery on the secondary site” on page 170.</td>
</tr>
<tr>
<td>Deploy VCS components.</td>
<td>See “Deploying VCS components on virtual machines in the secondary site” on page 171.</td>
</tr>
<tr>
<td>Verify the service group and use the Global Wizard.</td>
<td>See “Verifying the service group on the secondary site and using the Global Wizard” on page 171.</td>
</tr>
<tr>
<td>Perform post-failover actions.</td>
<td>See “Post-failover actions” on page 171.</td>
</tr>
<tr>
<td>Review the service group that VVM creates.</td>
<td>See “Reviewing the generated service groups” on page 172.</td>
</tr>
<tr>
<td>Work with the service groups.</td>
<td>See “Accessing the service groups” on page 173.</td>
</tr>
<tr>
<td>Verify machine fail over functionality.</td>
<td>See “Verifying virtual machine failover” on page 173.</td>
</tr>
</tbody>
</table>
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 your 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.
- You have disabled VMware HA on the VMware clusters.
- The nodes are part of a VMware cluster.
- Ensure that all the ESX nodes that form a VCS ESX cluster are present and configured in the VirtualCenter Server as a corresponding VC Server cluster.

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 keystores" on page 142.

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 > Symantec > 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 146.
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 Tools and configure the applications on the virtual machine. Perform the procedures in the following chapter depending on operating system:

- Chapter 12, “Configuring applications and resources in Linux virtual machines” on page 177.
- Chapter 13, “Configuring applications and resources in Windows virtual machines” on page 217.

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 173.

Reversing the direction of replication

You now need to reverse the direction of replication between your primary and secondary arrays. Make sure that the service group for this virtual machine is offline on the primary site. 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.
Deploying VCS components on virtual machines in the secondary site

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

- For Linux:
  - See “Configuring the Veritas Virtual Machine Tools” on page 209.
  - See “Validating the configuration of Veritas Virtual Machine Tools” on page 209.

- For Windows:
  - See “Configuring Veritas Virtual Machine Tools” on page 240.
  - See “Validating the configuration of Veritas Virtual Machine Tools” on page 241.

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 164.

Post-failover actions

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

- For Linux:
  - See “Configuring the Veritas Virtual Machine Tools” on page 209.
  - See “Validating the configuration of Veritas Virtual Machine Tools” on page 209.
Configuring virtual machines for disaster recovery

Configuring virtual machines for disaster recovery using the Veritas Virtualization Manager

- Apply the changes to the configuration by running the vcsag_config.pl program with the -apply option, as follows:
  
  ```bash
  # /opt/VRTSvcs/bin/vcsag_config.pl -apply
  ```

- For Windows:
  - See “Configuring Veritas Virtual Machine Tools” on page 240.
  - See “Validating the configuration of Veritas Virtual Machine Tools” on page 241.
  - Apply the changes to the configuration by running the vcsag_config.pl program with the -apply option, as follows:
    
    ```cmd
    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 11-3, you can see a basic example of a resource dependency graph for a service group.
Accessing the service groups

Although the Veritas Virtualization Manager creates a service group for you, use command line tools, Veritas Cluster Management Console, Cluster Server (Java 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 the 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.
- Enter a `hagrp -online` command to boot the virtual machine through VCS. 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.

### Fire drills

A disaster recovery fire drill mimics a failover from a primary site to a secondary site. The fire drill tests the fault-readiness of a configuration. Configuring fire drills for supported arrays, and performing the fire drills are described in detail in the following guides:

- *The Veritas Cluster Server User’s Guide*
- The applicable VCS agent configuration guide
Configuring applications in virtual machines

This section contains the following chapters:

- Chapter 12, “Configuring applications and resources in Linux virtual machines” on page 177
- Chapter 13, “Configuring applications and resources in Windows virtual machines” on page 217
Configuring applications in virtual machines
Configuring applications and resources in Linux virtual machines

This chapter contains the following topics:

- About VCS components for virtual machines running Linux
- How VCS monitors applications and resources on virtual machines
- Installing the applications
- Installing the Veritas Virtual Machine Tools
- Configuring application and resource monitoring inside of virtual machines
- Applying the configuration and creating the corresponding GuestOSApp resource
- Removing the Veritas Virtual Machine Tools
VCS for VMware ESX provides agents to monitor applications that run inside virtual machines. When the agent detects and application or resource fault, the agent takes actions to communicate the state of the resource to VCS running on the ESX Server node.

Certain VCS agents also support the ability to detect administrative intervention. When an administrator gracefully shuts down an application, VCS correctly does not initiate failover.

VCS provides agents to monitor the following applications that run on virtual machines running Linux:

<table>
<thead>
<tr>
<th>Application</th>
<th>Agent information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>■ Monitors Oracle instances.</td>
</tr>
<tr>
<td></td>
<td>■ Detects a graceful administrative shutdown of Oracle.</td>
</tr>
<tr>
<td></td>
<td>■ See “About the VCS agent for Oracle” on page 179.</td>
</tr>
<tr>
<td>Apache Web Server</td>
<td>■ Monitors Apache processes.</td>
</tr>
<tr>
<td></td>
<td>■ Detects a graceful administrative shutdown of Apache processes.</td>
</tr>
<tr>
<td></td>
<td>■ See “About the VCS agent for the Apache Web server” on page 188.</td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td>■ Monitors SAP NetWeaver instances.</td>
</tr>
<tr>
<td></td>
<td>■ Detects a graceful administrative shutdown of SAP NetWeaver processes.</td>
</tr>
<tr>
<td></td>
<td>■ See “About the VCS agent for SAP NetWeaver” on page 192.</td>
</tr>
</tbody>
</table>

VCS provides the following agents to monitor mount points and applications:

<table>
<thead>
<tr>
<th>Agent</th>
<th>Agent information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount</td>
<td>■ Monitors mount points.</td>
</tr>
<tr>
<td></td>
<td>■ See “About the Mount agent” on page 202.</td>
</tr>
<tr>
<td>Application</td>
<td>■ Monitors applications.</td>
</tr>
<tr>
<td></td>
<td>■ See “About the Application agent” on page 198.</td>
</tr>
</tbody>
</table>

If a monitored resource or application fails, the corresponding agent communicates this state change to VCS on the ESX Server node. VCS can then fails over the virtual machine that runs the application onto another node.
About monitoring levels

VCS agents provide two levels of monitoring:

- Basic monitoring
  Checks for running processes.

- Detailed monitoring
  Performs application-specific tasks to check the application’s health. For example, the VCS agent for Oracle performs a transaction on the database and checks to see if the transaction succeeds.

All VCS agents provide basic monitoring capabilities. Some agents provide detailed monitoring capabilities.

Supported software

VCS 5.1 for VMware ESX supports the following software for virtual machines:

- **Guest operating systems**
  - Red Hat Enterprise Linux 4 (Update 3)
  - SUSE Linux Enterprise Server 9 with SP3
  - SUSE Linux Enterprise Server 10 with SP1

- **Applications**
  - Oracle 10g
  - Apache Web server:
    - Apache HTTP server 1.3, 2.0, and 2.2
    - IBM HTTP Server 1.3 and 2.0
  - SAP R/3-4.6C with a 4.6D Kernel, 4.6D, 4.7 Enterprise Version
    - SAP Web AS-6.20, 6.40, 7.00
    - SAP NetWeaver-2004, 2004s

About the VCS agent for Oracle

The VCS agent for Oracle contains two agents:

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

Both agents work together to make Oracle highly available.

VCS agent for Oracle detects graceful shutdown for Oracle 10g only. When an administrator brings down Oracle 10g gracefully, the agent does not trigger a resource fault even though Oracle is down. The agent provides this intentional offline functionality only when the Health check monitoring is enabled.
Agent functions
The VCS agent for Oracle supports the Monitor agent function.

- Oracle agent
  The Monitor agent function verifies the status of the Oracle processes. The Oracle agent provides two levels of monitoring: basic and detailed. By default, the agent performs basic monitoring. Set the DetailMonitor attribute to 1 to enable detailed monitoring for Oracle.
  The basic monitoring mode has two options: Process and Health check. Depending on the mode you want to use, you must set the value of the MonitorOption attribute.

<table>
<thead>
<tr>
<th>MonitorOption value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>Health check (supported on Oracle 10g and later) You must set the value of this attribute to 1 to enable intentional offline functionality. The agent uses the Health Check APIs from Oracle to monitor the SGA and retrieve the information about the instance.</td>
</tr>
</tbody>
</table>

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

- Netlsnr agent
  The Monitor agent function verifies the status of the listener process. The Netlsnr agent provides two levels of monitoring: basic and detailed.
  - In the basic monitoring mode, which is the default behavior, the agent scans the process table for the tnslsnr process to verify the listener process is running.
  - In the detailed monitoring mode, the agent uses the Lsnrctl status $LISTENER command to verify the status of the Listener process.
How the agent handles Oracle error codes during detail monitoring

The VCS agent for Oracle handles Oracle errors during detail monitoring. The agent classifies Oracle errors according to their severity and associates predefined actions with each error code.

The agent includes a reference file called oraerror.dat, which lists Oracle errors and the action to be taken when the error is encountered.

The file stores information in the following format:
Oracle_error_string:action_to_be_taken

For example:
01035:WARN
01034:FAILOVER

Table 12-1 lists the predefined actions that the agent takes when an Oracle error is encountered.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGNORE</td>
<td>Ignores the error. When the VCS Agent for Oracle encounters an error that does not have a matching error code in the oraerror.dat file, then the agent ignores the error.</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>Marks the resource state as UNKNOWN and sends a notification if the Notifier resource is configured. See the <em>Veritas Cluster Server User’s Guide</em> for more information about VCS notification. This action is typically associated with configuration errors or program interface errors.</td>
</tr>
<tr>
<td>WARN</td>
<td>Marks the resource state as ONLINE and sends a notification if the Notifier resource is configured. This action is typically associated with errors due to exceeded quota limits, session limits/restricted sessions so on.</td>
</tr>
<tr>
<td>FAILOVER</td>
<td>Marks the resource state as OFFLINE. This faults the resource. The GuestOSApp agent fails over the virtual machine. This is agent’s default behavior. If the file oraerror.dat is not available, the agent assumes this default behavior for every Oracle error encountered.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNKNOWN</td>
<td>Marks the resource state as UNKNOWN and sends a notification if the Notifier resource is configured. See the <em>Veritas Cluster Server User’s Guide</em> for more information about VCS notification. This action is typically associated with configuration errors or program interface errors.</td>
</tr>
<tr>
<td>WARN</td>
<td>Marks the resource state as ONLINE and sends a notification if the Notifier resource is configured. This action is typically associated with errors due to exceeded quota limits, session limits/restricted sessions so on.</td>
</tr>
<tr>
<td>FAILOVER</td>
<td>Marks the resource state as OFFLINE. This faults the resource. The GuestOSApp agent fails over the virtual machine. This is agent’s default behavior. If the file oraerror.dat is not available, the agent assumes this default behavior for every Oracle error encountered.</td>
</tr>
</tbody>
</table>
TABLE 12-1  Predefined agent actions for Oracle errors

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOFAILOVER</td>
<td>Freezes the service group temporarily and marks the resource state as OFFLINE. The agent also sends a notification if the Notifier resource is configured. This action is typically associated with errors that are not system-specific. For example, if a database does not open from a node due to corrupt Oracle files, failing it over to another node does not help.</td>
</tr>
</tbody>
</table>

State definitions

- **ONLINE**
  Indicates that Oracle is running.

- **OFFLINE**
  Indicates that Oracle is not running.
  Can also indicate that the administrator stopped Oracle gracefully. The Oracle agent can detect that the administrator has gracefully stopped it when the MonitorOption attribute is set to 1 (when health check monitoring is enabled).

- **FAULTED**
  Indicates that the application crashed or unexpectedly went offline.

- **UNKNOWN**
  Indicates that a problem exists with the configuration.

Oracle agent attributes

**Table 12-2** lists the required attributes for Oracle agent.

**Table 12-2**  Oracle agent required attributes

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sid</td>
<td>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</td>
</tr>
<tr>
<td>Owner</td>
<td>The Oracle user, as the defined owner of executables and database files in /etc/passwd. Type and dimension: string-scalar</td>
</tr>
</tbody>
</table>
Configuring applications and resources in Linux virtual machines

About VCS components for virtual machines running Linux

Table 12-2
Oracle agent required attributes

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 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 12-3 lists the optional attributes for Oracle agent.

Table 12-3
Oracle agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartUpOpt</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>ShutDownOpt</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
</tbody>
</table>
| EnvFile             | The full path name of the file that is sourced by the agent function 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 |
<p>| AutoEndBkup         | This attribute is disabled. Accept the default setting. |</p>
<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 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  
| Note:              | You must set the value of this attribute to 1 to enable the intentional offline functionality of the agent.  
|                     | See "Agent functions" on page 180.  
|                     | Type and dimension: integer-scalar |
| DetailMonitor       | Setting this attribute to a non-zero value enables detailed monitoring for Oracle. The value indicates the number of monitor cycles after which the agent monitors Oracle in detail. For example, the value 5 indicates that the agent monitors Oracle in detail every five monitor intervals. The monitor interval is 60 seconds by default.  
|                     | Default: 0  
|                     | Type and dimension: integer-scalar |
| MonScript           | Pathname to the script provided for detailed monitoring. The default, basic monitoring, monitors the database PIDs only.  
|                     | Note: Detailed 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 |
Configuring applications and resources in Linux virtual machines
About VCS components for virtual machines running Linux

Table 12-3  Oracle agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pword</td>
<td>Encrypted password for internal database-user authentication. You must encrypt passwords using the VCS Encrypt utility before you configure this attribute. See “Prerequisites for configuring Oracle and Netlsnr resources” on page 211. <strong>Note:</strong> The VCS Encrypt utility is installed as part of the Veritas Virtual Machine tools. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>Table</td>
<td>Table for update by User/ Pword. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>Encoding</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>AgentDebug</td>
<td>Additional debug messages are logged when this flag is set. Default: 0 Type and dimension: boolean-scalar</td>
</tr>
</tbody>
</table>

Table 12-4 lists the internal attribute for Oracle agent. This attribute is for internal use only. Symantec recommends that you do not modify the value of this attribute.

Table 12-4  Oracle agent internal attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentDirectory</td>
<td>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</td>
</tr>
</tbody>
</table>
### Netlsnr agent attributes

Table 12-5 lists the required attributes for Netlsnr agent.

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 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 12-6 lists the optional attributes for Netlsnr agent.

<table>
<thead>
<tr>
<th>Optional attributes</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 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 |
| 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.  
You must encrypt passwords using the VCS Encrypt utility before you configure this attribute.  
See “Prerequisites for configuring Oracle and Netlsnr resources” on page 211.  
**Note:** The VCS Encrypt utility is installed as part of the Veritas Virtual Machine tools.  
Type and dimension: string-scalar |
Table 12-6  Netlsnr agent optional attributes

<table>
<thead>
<tr>
<th>Optional attributes</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnvFile</td>
<td>Specifies the full path name of the file that is sourced by the agent function 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</td>
</tr>
<tr>
<td>MonScript</td>
<td>Pathname to the script provided for detail monitoring. The default (basic monitoring) is to monitor the listener process only. <strong>Note:</strong> 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 &quot;./&quot;, as in the path ./bin/Netlsnr/LsnrTest.pl. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>Encoding</td>
<td>Specifies operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. Default: &quot;&quot; Type and dimension: string-scalar</td>
</tr>
<tr>
<td>AgentDebug</td>
<td>Additional debug messages are logged when this flag is set. Default: 0 Type and dimension: boolean</td>
</tr>
</tbody>
</table>
Table 12-7 lists the internal attribute for Netlsnr agent. This attribute is for internal use only. Symantec recommends that you do not modify the value of this attribute.

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentDirectory</td>
<td>Specifies the location of binaries, scripts, and other files related to the Netlsnr agent. Default: /opt/VRTSagents/ha/bin/Netlsnr</td>
</tr>
</tbody>
</table>

About the VCS agent for the Apache Web server

The Apache Web server agent monitors the Apache server processes. The agent can detect when Apache is brought down gracefully by an administrator. 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. Can also indicate that the administrator stopped the Apache server gracefully. Note that the agent uses the PidFile attribute for the intentional offline detection.

- **FAULTED**
  - Indicates that the Apache server unexpectedly went offline.

- **UNKNOWN**
  - Indicates that a problem exists with the configuration.
Apache Web server attributes

Table 12-8 lists the required attributes for the Apache agent.

Table 12-8
Apache Web server agent required attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 <httpd.conf> option. If the httpd process is not started with the specified option, modify the OPTIONS attribute in Apache startup file to specify the full 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" |
| **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.  
                    Type and dimension: string-scalar  
                    Example: /var/run/httpd.pid |
Table 12-8  Apache Web server agent required attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>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: &quot;80&quot;</td>
</tr>
<tr>
<td>ResLogLevel</td>
<td>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: &quot;TRACE&quot;</td>
</tr>
<tr>
<td>User</td>
<td>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: &quot;apache1&quot;</td>
</tr>
</tbody>
</table>

Table 12-9 lists the optional attributes for the Apache agent.

Table 12-9  Apache Web server agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectiveAfter</td>
<td>A list of directives that httpd processes after reading the configuration file. Type and dimension: string-association Example: DirectiveAfter{} = { KeepAlive=On }</td>
</tr>
</tbody>
</table>
### Table 12-9 Apache Web server agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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) to exclude 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. 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).  
Type and dimension: boolean-scalar  
Default: 0  
Example: "1" |
| SharedObjDir       | Full path of the directory in which the Apache HTTP shared object files are located. 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" |
Table 12-9  Apache Web server agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| SecondLevelTimeout | Number of seconds the Monitor agent function waits for the second-level monitor to complete. If the second-level monitor program does not respond within the SecondLevelTimeout value, the Monitor agent function stops blocking on the program sub-process and reports that the resource is offline. The value for the attribute must be less than 60 seconds.  
Type and dimension: integer-scalar  
Default: 30 |

About the VCS agent for SAP NetWeaver

The Veritas agent for SAP NetWeaver provides high availability for SAP R/3 and SAP NetWeaver in a cluster. The SAP NetWeaver agent supports a wide range of SAP environments, including the traditional Basis architecture and the SAP J2EE Web Application Server architecture (NetWeaver). The agent also supports Standalone Enqueue Servers in a distributed SAP installation.

The SAP components are:

- Central instance
- Dialog instance
- Standalone Enqueue Server
  Standalone Enqueue Server is also known as SAP Central Services (SCS).

The agent supports the following SAP Web Application Server architectures:

- ABAP
- Java
- Java Add-In (ABAP + Java)

The sample resource configurations for SAP NetWeaver agent are shown in the following figures. In these configurations, three SAP components are configured in three different virtual machines.

Figure 12-1 shows the resource configuration for SCS instance.
Configuring applications and resources in Linux virtual machines

About VCS components for virtual machines running Linux

Figure 12-2 shows the resource configuration for Central instance.

Figure 12-2 Resource configuration for Central instance

Figure 12-3 shows the resource configuration for Dialog instance.

Figure 12-3 Resource configuration for Dialog instance

VCS supports detection of graceful shutdown for SAP instances. When SAP NetWeaver is brought down gracefully, the agent does not trigger a resource fault even though SAP NetWeaver is down.
Agent functions

The SAP NetWeaver agent supports the Monitor function, which is described as follows:

- **Monitor**
  The monitor operation monitors the state of the SAP instance on all nodes in the cluster. The operation performs the following tasks:
  - Depending upon the search criteria that the ProcMon attribute specifies, the monitor operation scans the process table to verify that the SAP instance processes are running. Review the information for setting the ProcMon attribute.
    See “SAP NetWeaver agent attributes” on page 195.
  - If the SecondLevelMonitor attribute is greater than 0, the monitor operation performs a thorough check of the Application instance.
    - For Central or Dialog instances, the operation uses the following utilities to perform this check:

<table>
<thead>
<tr>
<th>Server architecture</th>
<th>SAP utility used</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Web Application Server as ABAP</td>
<td>sapinfo</td>
</tr>
<tr>
<td>SAP Web Application Server as Java</td>
<td>jcmon</td>
</tr>
<tr>
<td>SAP Web Application Server as Java Add-In</td>
<td>sapinfo and jcmon</td>
</tr>
</tbody>
</table>

- For Enqueue Server instances, the operation uses the ensmon utility for all the architectures (ABAP, Java, and Java Add-In).
- The monitor operation can also execute a custom monitor utility that the MonitorProgram attribute specifies.

State definitions

- **ONLINE**
  Indicates that the SAP server is running.

- **OFFLINE**
  Indicates that the SAP server is not running.
  Can also indicate that the administrator has intervened to stop the SAP server.

- **FAULTED**
  Indicates that the SAP server unexpectedly went offline.

- **UNKNOWN**
  Indicates that a problem exists with the configuration.
SAP NetWeaver agent attributes

Table 12-10 shows the required attributes for the SAP NetWeaver agent.

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EnvFile</strong></td>
<td>The absolute path to the file that must be sourced with the UNIX shell. You must source this file to set the environment before executing the SAP scripts for monitor operation. Supported shell environments are ksh, sh, and csh. <strong>Note:</strong> Ensure that the syntax of this file is in accordance with the user shell that the SAPAdmin attribute specifies. Symantec recommends that you store this file on shared disk so that the file is always available to an online system. Type and dimension: string-scalar Default: “” Example: <code>/usr/sap/EC1/DVEBMGS00/envfile</code></td>
</tr>
<tr>
<td><strong>InstName</strong></td>
<td>Identifies a SAP server instance. Type and dimension: string-scalar Default: DVEBMGS00 Example: DVBGS01</td>
</tr>
</tbody>
</table>
| **InstType**        | An identifier that classifies and describes the SAP server instance type. Valid values are:  
  - CENTRAL: SAP Central Services instance  
  - DIALOG: SAP Dialog instance  
  - ENQUEUE: Standalone Enqueue instance  
  - AENQUEUE: ABAP SAP Standalone Enqueue instance  
  - JENQUEUE: Java SAP Standalone Enqueue instance  
  **Note:** The value of this attribute is not case sensitive. Type and dimension: string-scalar Default: CENTRAL Example: DIALOG |
| **ProcMon**         | The list of SAP processes to monitor. Use a space to separate the entities in this list. The entities can appear in any order. Type and dimension: string-scalar Default: “” Example: dw se jc |
### Table 12-10  
**SAP NetWeaver agent required attributes**

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 operations.  
Type and dimension: string-scalar  
Default: INFO  
Example: TRACE |
| SAPAdmin            | UNIX user, as the defined administrator of executables of application directories and executables. This user name is usually a concatenation of the SAPSID attribute and the adm string.  
One or more system naming services store this user name, for example, NIS, NIS+, and LDAP servers. The agent functions use this user name to execute their respective core subroutines.  
Type and dimension: string-scalar  
Default: ““  
Example: ec1adm |
| SAPMonHome          | The location of the directory that contains the binary used for second level monitoring process.  
Type and dimension: string-scalar  
Default: ““  
Example: /usr/sap/${SAPSID}/SYS/exe/runU |
| SAPSID              | SAP system name.  
The value of this attribute is three characters in length, and must begin with an alphabetical character. The value of this attribute is defined during the SAP installation.  
Type and dimension: string-scalar  
Default: ““  
Example: EC1 |
About VCS components for virtual machines running Linux

Table 12-10  SAP NetWeaver agent required attributes

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| StartProfile        | The full path and file name of the StartProfile instance. The StartProfile instance is found in /usr/sap/SAPSID/SYS/profile directory. The value of the instance is START.InstName_hostname. The hostname must resolve into a valid IP address that is used to cluster the SAP instance.  
Type and dimension: string-scalar  
Default: “”  
Example: /usr/sap/EC1/SYS/profile/START_DVEBMGS01_sunaabap |

Table 12-11 lists the optional attributes for the SAP NetWeaver agent.

Table 12-11  SAP NetWeaver agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| MonitorProgram     | Absolute path name of an external, user-supplied monitor executable.  
Type and dimension: string-scalar  
Default: “”  
Example 1: /usr/sap/EC1/DVEBMGS00/work/myMonitor.sh  
Example 2: /usr/sap/EC1/DVEBMGS00/work/myMonitor.sh arg1 arg2 |
Table 12-11  SAP NetWeaver agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| SecondLevelMonitor   | Used to enable second-level monitoring. Second-level monitoring is a deeper, more thorough state check of the SAP instance.  
                        | By default, the agent performs basic monitoring. If the value of the SecondLevelMonitor attribute is greater than 0, then the agent performs detailed monitoring. The numeric value specifies how often the monitoring routines must run. For example, if you set the value of this attribute as 2, then the agent monitors the SAP instance in detail every second monitor interval. The monitor interval is 60 seconds by default.  
                        | **Note:** Exercise caution while setting SecondLevelMonitor to large numbers. For example, if you set the value of SecondLevelMonitor to 100, then sapinfo is executed every 100 minutes, which may not be as often as intended. For maximum flexibility, no upper limit is defined for SecondLevelMonitor.  
                        | Type and dimension: integer-scalar  
                        | Default: 0  
                        | Example: 1 |

About the Application agent

The Application agent monitors the status of applications. An application runs in the default context of root. Configure the User attribute to run the application in that user’s context (for example jsmith and not root).

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

Agent functions

- 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.

- **FAULTED**
  Indicates this resource state if an application process terminates.

- **UNKNOWN**
  Indicates an indeterminable application state or invalid configuration.

**Application agent attributes**

Table 12-12 lists the required attributes for the Application agent.

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least one of the following attributes:</td>
<td>See “Application agent optional attributes” on page 200.</td>
</tr>
<tr>
<td>- MonitorProcesses</td>
<td></td>
</tr>
<tr>
<td>- MonitorProgram</td>
<td></td>
</tr>
<tr>
<td>- PidFiles</td>
<td></td>
</tr>
<tr>
<td>StartProgram</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>StopProgram</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
</tbody>
</table>
Table 12-13 lists the optional attributes for the VCS agent for the Application agent.

### Table 12-13  Application agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CleanProgram</td>
<td>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</td>
</tr>
<tr>
<td>MonitorProcesses</td>
<td>A list of processes that you want monitored and cleaned. Each process name is the name of an executable. If the executable requires the complete path to start, specify the complete path. The process name must be the name displayed by the <code>ps -ef</code> command for the process. Type and dimension: string-vector Example: “nmbd”</td>
</tr>
<tr>
<td>MonitorProgram</td>
<td>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</td>
</tr>
</tbody>
</table>
### Table 12-13 Application agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PidFiles</td>
<td>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. Type and dimension: string-vector</td>
</tr>
<tr>
<td>User</td>
<td>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</td>
</tr>
</tbody>
</table>
About the Mount agent

Use the Mount agent to monitor a mount point. If the mount point fails, VCS detects the fault, and fails over the service group to another node.

Agent functions

- **Monitor**
  Determines if the file system is mounted.

State definitions

- **ONLINE**
  Indicates that the file system is properly mounted on the given mount point.

- **OFFLINE**
  Indicates that the file system is not mounted properly on the mount point.

- **FAULTED**
  Indicates that the file system unexpectedly unmounted.

- **UNKNOWN**
  Indicates that a problem exists either with the configuration or the ability to determine the status of the resource.
Mount agent attributes

Table 12-14 lists the required attributes for the Mount agent.

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlockDevice</td>
<td>The block device for the mount point. Type and dimension: string-scalar. Examples: /dev/sdc1. If the device is an LVM2 volume, specify the BlockDevice as: /dev/mapper/volume-group-logical-volume. For example: /dev/mapper/voldg-lvol0. If the file system type is NFS, then specify the BlockDevice as: server:/path/to/share. NFS device example: vcslnx1.veritas.com:/usr/share1.</td>
</tr>
<tr>
<td>FsckOpt</td>
<td>Specify -n for this value.</td>
</tr>
<tr>
<td>FSType</td>
<td>Type of file system. Supports ext2, ext3, nfs, or reiserfs. Type and dimension: string-scalar.</td>
</tr>
<tr>
<td>MountPoint</td>
<td>Directory for mount point. Type and dimension: string-scalar. Example: &quot;/mnt/apache1&quot;.</td>
</tr>
</tbody>
</table>
Table 12-15 lists the optional attributes for the Mount agent.

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CkptUmount</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>MountOpt</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>SecondLevelMonitor</td>
<td>This attribute is only applicable to NFS client mounts. If set to 1, this attribute enables detailed monitoring of a NFS mounted file system. Type and dimension: boolean-scalar Default: 0</td>
</tr>
<tr>
<td>SecondLevelTimeout</td>
<td>This attribute is only applicable for a NFS client mount. This is the timeout (in seconds) for the SecondLevelMonitor/Detail monitoring of NFS Mounts. Number of seconds the Monitor agent function waits for the second-level monitor to complete. If the second-level monitor program does not respond within the SecondLevelTimeout value, the Monitor agent function stops blocking on the program sub-process and reports that the resource is offline. The value for the attribute must be less than sixty. Type and dimension: integer-scalar Default: 30</td>
</tr>
<tr>
<td>SnapUmount</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
</tbody>
</table>
Table 12-15  Mount agent optional attributes

<table>
<thead>
<tr>
<th>Optional attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessPermissionChk</td>
<td>If the value of this attribute is 1, the monitor verifies that the values of the MntPtPermission, MntPtOwner, and the MntPtGroup attributes for the mount point are the same as the actual mount point. If any of these do not match the user-specified values, a message is logged. Use the same mount permissions, the same owner, and the same group for both the mount point directory and the file system to be mounted. Failure to use the same information for both can cause mount point permission changes after the file system is mounted. Type and dimension: boolean-scalar Default: 0</td>
</tr>
<tr>
<td>CreateMntPt</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>MntPtGroup</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>MntPtOwner</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>MntPtPermission</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>OptCheck</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>RecursiveMnt</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
<tr>
<td>ReuseMntPt</td>
<td>This attribute is disabled. Accept the default setting.</td>
</tr>
</tbody>
</table>

Sample configuration
You can use the Mount agent to monitor an application that uses a network file system. For example, Oracle uses a network file system that is mounted at /mnt/oracle. The Mount agent monitors /mnt/oracle. If /mnt/oracle goes offline, then the Mount resource would fault, and the virtual machine would fail
over to another cluster node. Like all other applications that VCS monitors in virtual machines, the Mount agent is represented as a GuestOSApp resource at the VMware ESX Server level.

How VCS monitors applications and resources on virtual machines

The VCS agent management daemon (vcsagmd) is a very light-weight daemon that resides in the virtual machine. It manages the agents that monitor virtual machine resources. While the agents monitor the resources, the daemon monitors the agents. The daemon sends heartbeats to VCS on the ESX Server layer. The heartbeats inform VCS at the ESX Server layer if VCS at the virtual machine layer is functioning properly or not. In cases where the guest operating system does not boot, heartbeats are interrupted. An interrupted heartbeat can result in an UNKNOWN state and can also result in a failover.

When a resource (like Oracle or a mount point) fails, the resource in the virtual machine reports an OFFLINE state. The OFFLINE state is reported to VCS at the ESX Server layer. VCS at the ESX Server layer then decides where the application’s virtual machine needs to move to re-continue services.

Figure 12-4  State information passing between the virtual machine and the VCS node where the machine resides
Installing the applications

Install the application on the virtual machine. This is the application that you want VCS to monitor in the virtual machine. Refer to the application’s instructions for installation information. Note that you can install VCS for VMware ESX on virtual machines that already contain applications. You must set up the application to automatically start when the virtual machine starts. VCS only monitors the application—it does not start or stop the applications. In case of a failover, VCS moves the entire virtual machine. When the virtual machine starts on the other node, the application must start automatically when the virtual machine boots.

Installing the Veritas Virtual Machine Tools

Install Veritas Virtual Machine Tools on a virtual machine where you want to monitor resources for high availability. These tools contain different programs that enable high availability and monitoring. The tools installation is in a .iso file that you can mount as a disc on the virtual machine using the Veritas Virtualization Manager (VVM).

See “Mounting the Veritas Virtual Machine Tools” on page 207.

Mounting, installing, and configuring Veritas Virtual Machine Tools on the virtual machine

Before you install Veritas Virtual Machine Tools, you need to mount the .iso file for the virtual machine. Before you mount or install the tools, prepare the following information:

- The virtual IP address for the cluster.
- The username and password required to administer the service group.
- The name of the ESXVirtualMachine resource that is associated with the virtual machine.
- In disaster recovery environment only, you need the device path for the location of the pagefile datastore on another storage device.

Mounting the Veritas Virtual Machine Tools

VVM can make the Veritas Virtual Machine Tools installation program available to you for easy access.
To mount the tools .iso file

1. From a Windows client, click Start > Programs > Symantec > Veritas Virtualization Manager.
2. Right-click the virtual machine where you want to mount the .iso file. Select Add VCSVM-Tools ISO.
   If you receive this message, “This virtual machine has the ISO image mounted already,” perform the following troubleshooting task:
   “To resolve the “virtual machine has the ISO image mounted already” error” on page 208
3. Click the OK button to add the .iso file.
   The Add CD-ROM ISO window appears. The .iso file is now available for your use.

To resolve the “virtual machine has the ISO image mounted already” error

1. Open the VMware Infrastructure Client.
2. Click the virtual machine, and go to the Summary tab.
3. On the Summary tab, click Edit Settings.
4. Check Client Device in the Device Type section, and click OK to save.
5. In VVM, right-click the virtual machine and select Add VCSVM-Tools ISO.

Installing the Veritas Virtual Machine Tools

Install the Veritas Virtual Machine Tools.

To install the Veritas Virtual Machine Tools

1. Navigate to the installvcsvm-tools program location.
   `# cd /media/cdrom`
2. On the virtual machine, enter the installvcsvm-tools -i command.
   `# ./installvcsvm-tools -i`
3. When you are prompted to install the tools, press the y key to proceed.
4. The installvcsvm-tools program prints some information and asks if you want to configure the tools. Press the y key to configure the tools.
Configuring the Veritas Virtual Machine Tools

Configure the Veritas Virtual Machine Tools.

To configure the Veritas Virtual Machine Tools

1. On the virtual machine, enter the `installvcsvm-tools -c` command.
   ```bash
   ./installvcsvm-tools -c
   ``
   On a virtual machine that already has the tools mounted, use the full path for the command. At the prompt, enter:
   ```bash
   /opt/VRTSvcs/bin/installvcsvm-tools -c
   ``
2. When asked if you are ready to configure the tools, 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 one virtual machine for high availability” on page 151.
   - See “To configure a virtual machine for disaster recovery” on page 169.
5. Enter the name of the ESXVirtualMachine resource that is associated with the virtual machine.
6. In a disaster recovery environment, enter the device path for the location of the pagefile datastore on the secondary storage device. Note that this step is not required for a high availability environment.

Veritas Virtual Machine Tools configuration is now complete.

Validating the configuration of Veritas Virtual Machine Tools

You can verify that the tools are properly configured.

To validate the tools' configuration

1. Get the virtual machine resource's name, which is in the file `/etc/VRTSvcs/vcsvmresname`. To get the name, type:
   ```bash
   # 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 and resource monitoring inside of virtual machines

After you have installed the Veritas Virtual Machine Tools, configure resources within a virtual machine. You must use the resource configuration (vcsag_config.pl) program to configure 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.

For the Oracle and Netlsnr agents, see the following attributes:

- See “Oracle agent attributes” on page 182.
- See “Netlsnr agent attributes” on page 186.
- See “Apache Web server attributes” on page 189.
- See “SAP NetWeaver agent attributes” on page 195.
- See “Application agent attributes” on page 199.
- See “Mount agent attributes” on page 203.

## Prerequisites

These prerequisites are to make sure the high availability setup in the virtual machine is correct. Review the following:

- Before you configure your applications on the virtual machine, ensure that the applications are running.
- Each virtual machine has VMware Tools installed on it.
- The guestinfo interfaces of the VMware Virtual Machine tools are enabled. Note that these interfaces are enabled by default.
- The virtual machine or application administrator has VCS privileges to configure the application resources.
■ The ESX Server administrator has provided you with the username and password credentials for the service group that contains the virtual machine resource.

■ Set up the applications to automatically start when the virtual machine starts. VCS only monitors the applications. VCS does not start or stop the applications. In case of a failover, VCS moves the entire virtual machine to another node in the cluster.

■ Symantec recommends that you configure one virtual machine in one service group. You can configure multiple virtual machines in one service group if you have a multi-tier application that required the multiple virtual machines to fail over together.

Prerequisites for configuring Oracle and Netlsnr resources

You must encrypt the Pword attribute in the Oracle agent and the LsnrPwd attribute in the Netlsnr agent before configuring these attributes.

Encrypting passwords for VCS agent for Oracle

VCS provides a utility to encrypt the Oracle database user passwords and listener passwords.

Oracle provides the option of storing the listener password in the listener.ora file, in both clear text and encrypted formats. Irrespective of the format in which the password is stored in Oracle, you must encrypt the password using the vcsencrypt utility before configuring the LsnrPwd attribute. If you encrypted the listener password using the Oracle lsnrctl utility, make sure that you pass the encrypted password to the vcsencrypt utility. You can find the Oracle lsnrctl encrypted password from the following line in the listener.ora file:

```
PASSWORDS_ENCRYPTED = Xxxxxxxx
```

When the agent decrypts this password, the decrypted password for the listener must be of the same format as stored in the listener.ora file.
Configuring applications and resources in Linux virtual machines

Configuring application and resource monitoring inside of virtual machines

To encrypt passwords

1. From the path $VCS_HOME/bin/, run the vcsencrypt utility.
   - Type the following command:
     
     ```
     # vcsencrypt -agent
     ```
   - Enter the password and confirm it by entering it again. Press Enter.
     
     ```
     # Enter New Password:
     # Enter Again:
     ```

2. Review as the utility encrypts the password and displays the encrypted password.

3. Enter this encrypted password as the value for the attribute.


Configuring resources inside virtual machines

You need to configure the resources 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 resource or application that you want to monitor. Your choices are:
   - Apache
   - Application
   - Mount
   - Netlsnr
   - Oracle
   - SAPNW04

   The program lists the configured resources. 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 of the displayed resources.

5. To configure a new resource, enter a name for that resource.

6. When prompted, enter a value for each attribute.
You need to enter these values in the formats requested. For definitions for these data types:
See “Resource data types” on page 213.

Enter information for each attribute.
■ See “Oracle agent attributes” on page 182.
■ See “Netlsnr agent attributes” on page 186.
■ See “Apache Web server attributes” on page 189.
■ See “SAP NetWeaver agent attributes” on page 195.
■ See “Application agent attributes” on page 199.
■ See “Mount agent attributes” on page 203.

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

You can now choose to configure more resource 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.

If for any reason step 10 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
```

Resource data types

Table 12-16 shows the data types for information that you need to enter when running vcsag_config.pl.

<table>
<thead>
<tr>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>integer</td>
<td>Integer values include the numbers 0 through 9.</td>
</tr>
</tbody>
</table>
Table 12-16  Resource data types and acceptable values

<table>
<thead>
<tr>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boolean</td>
<td>Boolean values include 0 and 1. Zero is false, or off. One is true, or on.</td>
</tr>
</tbody>
</table>
| 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. |

Verifying that VCS is running

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

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

Grep for the agent name, for example: oracle, netlsnr, apache, or sapnw04.

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 resource configuration utility 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 Deaemon (vcsagmd) on the virtual machine. This restart applies the newly created configuration.
Removing the Veritas Virtual Machine Tools

To remove the Veritas Virtual Machine Tools

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

2. When asked if you are ready to uninstall the tools, answer `y`.
   
   The `installvcsvm-tools` program prints some information and the location of the log files.
Removing the Veritas Virtual Machine Tools
Configuring applications and resources in Windows virtual machines

This chapter contains the following topics:

- About VCS components on virtual machines running Windows
- How VCS monitors applications and resources on virtual machines
- Installing the applications
- Installing Veritas Virtual Machine Tools
- Configuring application monitoring
- Applying the configuration and creating the corresponding GuestOSApp resource
- Removing Veritas Virtual Machine Tools from the virtual machine running Windows
About VCS components on virtual machines running Windows

VCS for VMware ESX provides agents to monitor applications that run inside virtual machines. When the agent detects and application or resource fault, the agent takes actions to communicate the state of the resource to VCS running on the ESX Server node.

Certain VCS agents also support the ability to detect administrative intervention. When an administrator gracefully shuts down an application, VCS does not initiate failover.

VCS provides agents to monitor the following applications that run on virtual machines running Windows:

<table>
<thead>
<tr>
<th>Application</th>
<th>Agent information</th>
</tr>
</thead>
</table>
| SQL Server                    | ■ Monitors SQL Server instances.  
                                 | ■ Detects a graceful shutdown of SQL Server.  
                                 | ■ See “About the VCS agents for SQL Server” on page 220. |
| Internet Information Services (IIS) | ■ Monitors IIS servers and services  
                                | ■ Detects a graceful shutdown of IIS servers.  
                                | ■ See “About the VCS agent for Internet Information Services (IIS)” on page 227. |
| Exchange Server               | ■ Monitors Exchange services and protocol servers.  
                                | ■ Detects a graceful shutdown of Exchange protocol servers.  
                                | ■ See “About the VCS agent for Exchange Server 2003” on page 230. |

Additionally, VCS provides the following agent to monitor generic services:

<table>
<thead>
<tr>
<th>Agent</th>
<th>Agent information</th>
</tr>
</thead>
</table>
| GenericService      | ■ Monitors generic services  
                                 | ■ See "About the VCS agent for generic services" on page 234. |

If a monitored resource or application fails, the corresponding agent communicates this state change to VCS on the ESX Server node. VCS can then fail over the virtual machine that runs the application onto another node.

About monitoring levels

VCS agents provide two levels of monitoring:
Basic monitoring
Checks for running processes.

Detailed monitoring
Performs application-specific tasks to check the application’s health. For example, the VCS agent for Oracle performs a transaction on the database and checks to see if the transaction succeeds.

All VCS agents provide basic monitoring capabilities. Some agents provide detailed monitoring capabilities.

Supported software

VCS 5.1 for ESX supports the following software for virtual machines:

**Guest operating systems**
- Windows 2000 Server or Advanced Server with Service Pack 4
- Windows Server 2003: Standard Edition or Enterprise Edition (SP1 required) on either x86 (32-bit) or x86 (64-bit)

**Required software**
- Microsoft .NET Framework version 1.1 with SP1 or higher
- VMware Tools
- Veritas Virtual Machine Tools

**Required software for Veritas Virtual Machine Tools on Windows 2000**
Veritas Virtual Machine Tools requires the sc.exe utility. It is a separate download for Windows 2000 Server. To download it, perform the following steps:
1. Download the sc.exe utility:
2. Extract the sc.exe file to the system folder (C:\WINNT is the default).

**Microsoft SQL servers and their operating systems**
- Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (both require SP4) with
  Windows Server 2003: Standard Edition or Enterprise Edition (SP1 required) on either x86 (32-bit) or x86 (64-bit)
- Windows 2000 Server or Windows 2000 Advanced Server (both require SP4)
- Microsoft SQL Server 2005 (SP1 required) on either x86 (32-bit) or x86 (64-bit) with
  Windows Server 2003: Enterprise Edition (SP1 required) on either x86 (32-bit) or x86 (64-bit)

**Applications**
- Internet Information Services (IIS) 5.0 and 6.0
- Microsoft Exchange Server 2003
About the VCS agents for SQL Server

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.

See “Configuring the SQL Server agents” on page 242.

VCS 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.

Agent functions

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

State definitions

- **ONLINE**
  Indicates the configured SQL Server instance is available.

- **OFFLINE**
  Indicates the configured SQL Server instance is not available.
  Can also indicate that the administrator gracefully stopped the SQL Server instance.
About VCS components on virtual machines running Windows

Configuring applications and resources in Windows virtual machines

SQL Server agent attributes

Review the following information to familiarize yourself with the various agent attributes. This information will assist you during the agent configuration.

Agent for SQL Server 2000

The agent for SQL Server 2000 is represented by the SQLServer2000 resource type. The attributes for this agent are as follows:

<table>
<thead>
<tr>
<th>Required attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of instance to monitor. If the attribute is blank, the agent monitors the default instance. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>The Lanman resource name on which the SQL Server 2000 resource depends. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>MountResName</td>
<td>The mount resource name on which the SQL Server 2000 resource depends. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>SQLOnlineTimeout</td>
<td>Number of seconds that can elapse before the Online agent function aborts. Default is 90. Type and dimension: integer-scalar</td>
</tr>
<tr>
<td>SQLOfflineTimeout</td>
<td>Number of seconds that can elapse before Offline agent function aborts. Default is 90. Type and dimension: integer-scalar</td>
</tr>
<tr>
<td>IsGuestOS</td>
<td>A flag that indicates whether SQL is deployed in a VCS for VMware environment. This attribute controls the agent behavior. Set this attribute to 1 (True) if you have installed SQL on a VMware virtual machine in a VCS for VMware cluster environment. Default value is 1 (True). Type and Dimension: boolean-scalar</td>
</tr>
</tbody>
</table>
Table 13-2  SQL Server 2000 agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DetailMonitor</td>
<td>Defines whether the agent performs detail monitoring of SQL Server 2000 database. The value 0 indicates the agent does not monitor the database in detail. The value 1 indicates the agent does. Default = 0 &lt;br&gt; <strong>Note:</strong> If the attribute is set to 1, the attributes Username, Password, Domain, SQLDetailMonitorTimeOut, and SQLFile must be assigned appropriate values. Type and dimension: boolean-scalar</td>
</tr>
<tr>
<td>FaultOnDMScriptFailure</td>
<td>Defines whether the agent fails over the service group if the detail monitoring script execution fails. Default = 1 &lt;br&gt; The value 1 indicates that the agent fails over the service group if detail monitoring script fails to execute. The value 0 indicates that it does not. Type and dimension: boolean-scalar</td>
</tr>
<tr>
<td>SQLDetailMonitorTimeout</td>
<td>Number of seconds that can elapse before the detail monitor routine aborts. Default is 30. Type and dimension: integer-scalar</td>
</tr>
<tr>
<td>Username</td>
<td>The Microsoft Windows authentication name when logging in to a database for detail monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain for the user account. This attribute is used to create a trusted connection to the SQL Server 2000 instance if “DetailMonitor” attribute is set to 1. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>Password</td>
<td>Password for logging in to a database for detail monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1. Type and dimension: string-scalar</td>
</tr>
</tbody>
</table>
Table 13-2  SQL Server 2000 agent optional attributes (continued)

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLFile</td>
<td>The location of the SQLFile executed during a monitor cycle. This attribute must not be null if the &quot;DetailMonitor&quot; attribute is set to 1. Type and dimension: string-scalar</td>
</tr>
</tbody>
</table>

Agent for MSSearch service
The agent for MSSearch service is represented by the MSSearch resource type. The attribute for this agent is as follows:

Table 13-3  MSSearch service agent required attribute

<table>
<thead>
<tr>
<th>Required Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppName</td>
<td>The name of MSSearch instance to be monitored. Type and dimension: string-scalar</td>
</tr>
</tbody>
</table>

Agent for SQL Server 2005
The agent for SQL Server 2005 is represented by the SQLServer2005 resource type. The attributes for this agent are as follows:

Table 13-4  SQL Server 2005 agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of instance to monitor. If the attribute is blank, the agent monitors the default instance. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>The Lanman resource name on which the SQL Server 2005 resource depends. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>SQLOnlineTimeout</td>
<td>Number of seconds that can elapse before Online agent function aborts. Default is 90. Type and dimension: integer-scalar</td>
</tr>
<tr>
<td>SQLOfflineTimeout</td>
<td>Number of seconds that can elapse before Offline agent function aborts. Default is 90. Type and dimension: integer-scalar</td>
</tr>
</tbody>
</table>
### Table 13-4  SQL Server 2005 agent required attributes (continued)

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| IsGuestOS           | A flag that indicates whether SQL is deployed in a VCS for VMware environment. This attribute controls the agent behavior. Set this attribute to 1 (True) if you have installed SQL on a VMware virtual machine in a VCS for VMware cluster environment.  
Default value is 1 (True).  
Type and Dimension: boolean-scalar |

### Table 13-5  SQL Server 2005 agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| DetailMonitor       | Defines whether the agent performs detail monitoring of SQL Server 2005 database. The value 0 indicates the agent will not monitor the database in detail. The value 1 indicates the agent will.  
Default = 0.  
Note: If the attribute is set to 1, the attributes Username, Password, Domain, SQLDetailMonitorTimeOut, and SQLFile must be assigned appropriate values.  
Type and dimension: boolean-scalar |
| FaultOnDMScriptFailure | Defines whether the agent fails over the service group if the detail monitoring script execution fails.  
Default = 1  
The value 1 indicates that the agent fails over the service group if detail monitoring script fails to execute. The value 0 indicates that it does not.  
Type and dimension: boolean-scalar |
| SQLDetailMonitorTimeout | Number of seconds that can elapse before the detail monitor routine aborts. Default is 30.  
Type and dimension: integer-scalar |
| Username            | The Microsoft Windows authentication name when logging in to a database for detail monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1.  
Note: This attribute can take localized values.  
Type and dimension: string-scalar |
Configuring applications and resources in Windows virtual machines

About VCS components on virtual machines running Windows

Table 13-5  SQL Server 2005 agent optional attributes (continued)

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| Domain              | Domain for the user account. This attribute is used to create a trusted connection to the SQL Server 2005 instance if “DetailMonitor” attribute is set to 1.  
  **Note:** This attribute can take localized values.  
  Type and dimension: string-scalar |
| Password            | Password for logging in to a database for in-depth monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1.  
  Type and dimension: string-scalar |
| SQLFile             | The location of the SQLFile executed during a monitor cycle. This attribute must not be null if the “DetailMonitor” attribute is set to 1.  
  **Note:** This attribute can take localized values.  
  Type and dimension: string-scalar |

Agent for SQL Server 2005 Agent service

The agent for SQL Server 2005 Agent service is represented by the SQLAgService2005 resource type. The attributes for this agent are as follows:

Table 13-6  SQL Server 2005 Agent service agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| SQLServer2005ResName    | The name of the SQLServer2005 resource on which the SQL Server 2005 Agent service resource depends.  
  Type and dimension: string-scalar |
| LanmanResName           | The Lanman resource name on which the SQL Server 2005 resource depends.  
  Type and dimension: string-scalar |
Agent for SQL Server 2005 Analysis service
The agent for SQL Server 2005 Analysis service is represented by the SQLOlapService2005 resource type. The attributes for this agent are as follows:

Table 13-7  SQL Server 2005 Analysis service agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLServer2005ResName</td>
<td>The name of the SQLServer2005 resource on which the SQL Server 2005 Analysis service resource depends. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>The Lanman resource name on which the SQL Server 2005 resource depends. Type and dimension: string-scalar</td>
</tr>
</tbody>
</table>

MSDTC agent
The MSDTC agent is represented by the MSDTC resource type. The attributes for this agent are as follows:

Table 13-8  MSDTC agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LanmanResName</td>
<td>Name of the Lanman resource on which the MSDTC resource depends. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>MountResName</td>
<td>The mount resource name on which the MSDTC resource depends. Type and dimension: string-scalar</td>
</tr>
<tr>
<td>LogPath</td>
<td>The path for MSDTC logs. This attribute can take localized values. Type and dimension: string-scalar</td>
</tr>
</tbody>
</table>
About the VCS agent for Internet Information Services (IIS)

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.

See “Configuring the IIS agent” on page 245.

Agent functions

- Monitor
  Verifies the configured sites or application pools are running.

State definitions

- ONLINE
  Indicates the configured site or application pool is available.

- OFFLINE
  Indicates the configured site or application pool is not available.
  Can also indicate that the administrator gracefully stopped the application.

- UNKNOWN
  Indicates the agent could not determine the status of the resource.
**Internet Information Services (IIS) agent attributes**

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 13-9  Internet Information Services (IIS) required attributes**

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
| 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 |
Configuring applications and resources in Windows virtual machines

About VCS components on virtual machines running Windows

Table 13-10  Internet Information Services (IIS) optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 does not monitor the application pool associated with the Web site.  
  - DEFAULT: Indicates that the agent monitors 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 starts all application pools associated with the Web site, but monitors and stops the root application pool only. |
| DetailMonitor       | A flag that defines whether the agent monitors the site in detail. The value 1 indicates the agent monitors each site in detail by attempting an actual socket connection to the port. |
| DetailMonitorInterval | The number of monitor cycles after which the agent attempts detail monitoring. For example, the value 5 indicates that the agent monitors the resource in detail after every 5 monitor cycles. |

Type and dimension: integer-scalar
About the VCS agent for Exchange Server 2003


The VCS for VMware agent for Microsoft Exchange contains two agents:

- Exchange Service agent
  Monitors core Exchange services.

- Exchange Protocol agent
  Monitors Exchange protocol servers configured under the Exchange protocol services.

The agents for Microsoft Exchange monitor the configured Exchange services and Exchange protocol servers. Both agents work in conjunction to provide high availability for Microsoft Exchange.

See “Configuring the Exchange agents” on page 247.

Exchange Service agent

The Exchange Service agent monitors the status of the following Exchange services:

- Microsoft Exchange Information Store (MSExchangeIS)
  The Exchange storage used to hold messages in users’ mailboxes and in public folders.

- Microsoft Exchange System Attendant (MSExchangeSA)
  The Exchange component responsible for maintenance and ensuring that operations run smoothly.

- Microsoft Exchange Message Transfer Agent (MSExchangeMTA)
  The Exchange component responsible for routing messages.

- Microsoft Exchange Routing Engine (RESvc)
  The Exchange routing engine service.

- Microsoft Exchange Management Service (MSExchangeMGMT)
  Provides Exchange management information through WMI.

Each Microsoft Exchange service is configured as a VCS resource of type ExchService.
Agent functions

- Monitor
  Determines the state of the configured Exchange service by querying the Service Control Manager (SCM).

**Note:** The agent verifies the state of the enabled databases (databases that are automatically mounted when the service starts up). If an enabled database is dismounted, the agent returns **UNKNOWN** state. The VCS for VMware agent for Microsoft Exchange monitors only the enabled databases. To enable databases, run Microsoft Exchange System Manager and clear the **Do not mount this store at start-up** check box in database properties. If the agent detects that an enabled database is not mounted, it returns an **UNKNOWN** state. So, to disable the database, check the **Do not mount this store at start-up** check box if you want to dismount a database.

State definitions

- **ONLINE**
  Indicates the configured Exchange service is available.

- **OFFLINE**
  Indicates the configured Exchange service is not available.
  Can also indicate that the administrator gracefully stopped the Exchange service.

- **UNKNOWN**
  Indicates the agent could not determine the status of Exchange service.

Exchange Protocol agent

The Exchange Protocol agent monitors the protocol servers configured under the following Exchange protocols:

- **Post Office Protocol (POP3SVC)**
  Internet messaging protocol used to access email from a remote location.

- **Simple Mail Transfer Protocol (SMTPSVC)**
  TCP/IP protocol used to transfer email over the internet, which is also the native mail transport in Microsoft Exchange.

- **Internet Message Access Protocol (IMAP4SVC)**
  Internet messaging protocol used to access email messages stored on a remote server.
About VCS components on virtual machines running Windows

- World Wide Web (W3SVC)
  World Wide Web service.

Each protocol server to be monitored is configured as a VCS resource of type ExchProtocol.

Agent functions

- Monitor
  Determines the state of the configured Exchange protocol servers.

State definitions

- ONLINE
  Indicates the configured Exchange protocol service is available.

- OFFLINE
  Indicates the configured Exchange protocol service is not available. Can also indicate that the administrator gracefully stopped the Exchange protocol service.

- UNKNOWN
  Indicates the agent could not determine the status of Exchange protocol service.

Exchange Server agent attributes

Review the following information to familiarize yourself with the Exchange agent attributes. Use this information during the agent’s configuration.
**Exchange service agent attributes**

Review the following information to familiarize yourself with the required agent attributes for an ExchService resource type. This information assists you during the agent configuration.

Table 13-11  Exchange Service agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| Service            | The name of the Exchange service to be monitored. By default this attribute takes the following values:  
  - MSExchangeIS  
  - MSExchangeSA  
  - RESvc  
  Additionally, you can also configure the following services:  
  - MSExchangeMTA  
  - MSExchangeMGMT  
  Type and Dimension: string-scalar |

| LanmanResName      | Do not modify this attribute. For internal use only. |

Table 13-12  Exchange Service agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attribute</th>
<th>Definition</th>
</tr>
</thead>
</table>
| DetailMonitor      | A flag that determines whether the agent monitors the MSExchangeIS service in detail. The value 1 indicates that the agent monitors the service in detail; the value 0 indicates it does not.  
  Set this attribute only for resources configured to monitor the MSExchangeIS service; the attribute is ignored for other services.  
  Type and Dimension: integer-scalar |
Exchange protocol agent attributes
Review the following information to familiarize yourself with the required agent attributes for an ExchProtocol resource type. This information will assist you during the agent configuration.

Table 13-13  Exchange Protocol agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualServer</td>
<td>The name of the Exchange protocol server to be monitored. This attribute can take localized values. Type and Dimension: string-scalar</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>Do not modify this attribute. For internal use only.</td>
</tr>
</tbody>
</table>
| Protocol           | The Exchange protocol for which the Exchange protocol server is configured. This attribute could take any of the following values:
  - POP3SVC
  - W3SVC
  - IMAP4SVC
  - SMTPSVC
  Type and Dimension: string-scalar |

Table 13-14  Exchange Protocol agent optional attribute

<table>
<thead>
<tr>
<th>Optional Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DetailMonitor</td>
<td>Do not modify this attribute. For internal use.</td>
</tr>
</tbody>
</table>

About the VCS agent for generic services
The GenericService agent monitors the status of a service. Note that a service is an application type supported by Windows that conforms to the interface rules of the Service Control Manager (SCM).

Services are defined as resources of type GenericService. You can configure the GenericService agent to monitor multiple services by defining a resource for each service to be monitored. You can monitor a service in a user-context by specifying the user name, password, and domain.

**Note:** The service to be configured using the GenericService agent must have the status as Started and the startup type as Automatic.

See “Configuring the GenericService agent” on page 249.
Agent functions

- **Monitor**
  - Retrieves the current state of the configured service. It also verifies the user context, if applicable.

State definitions

- **ONLINE**
  - Indicates the service being monitored is online.

- **OFFLINE**
  - Indicates the service being monitored is offline.

- **UNKNOWN**
  - Indicates the service operation is in a pending state, or that the agent could not determine the state of the resource.

GenericService agent attributes

Review the following information to familiarize yourself with the agent attributes for the GenericService resource type. Use this information during the agent’s configuration.

**Table 13-15**  
GenericService agent required attribute

<table>
<thead>
<tr>
<th>Required Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| ServiceName            | Name of the service to be monitored. The service name can be the Service Display Name or the Service Key Name.  
  **Note:** This attribute can take localized values.  
  Type and dimension: string-scalar |

**Table 13-16**  
GenericService agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| DelayAfterOffline          | Number of seconds the offline routine waits for the service to go offline. Default is 10 seconds.  
  Type and dimension: integer-scalar |
| DelayAfterOnline           | Number of seconds the online routine waits for the service to go online. Default is 10 seconds.  
  Type and dimension: integer-scalar |
<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| Domain              | The domain name to which the user specified in the UserAccount attribute belongs.  
  **Note:** This attribute can take localized values.  
  Type and dimension: string-scalar |
| Password            | The password of the user, in whose context, the service would be started. If the UserAccount attribute is empty or contains a built-in service account, this attribute is ignored.  
  Type and dimension: string-scalar |
| service_arg         | An array of arguments passed to the service.  
  Type and dimension: string-vector |
| UserAccount         | A valid user account in whose context the service will be monitored. Username can be of the form username@domain.com or domain.com\username.  
  If you do not specify a value for this attribute, then the user account of the service in the SCM is ignored.  
  To monitor service under built-in accounts, you must provide explicit values. For example:  
  - On Windows 2000: UserAccount='LocalSystem'  
  - On Windows 2003: UserAccount='LocalSystem', 'Local Service', or 'Network Service'. Domain='NT Authority'.  
  The 'NT Authority' domain is not applicable for the 'LocalSystem' account.  
  **Note:** This attribute can take localized values.  
  Type and dimension: string-scalar |
| UseVirtualName      | Do not modify this attribute. For internal use only. |
| LanmanResName       | Do not modify this attribute. For internal use only. |
How VCS monitors applications and resources on virtual machines

The VCS agent management daemon (vcsagmd) is a very light-weight daemon that resides in the virtual machine. It manages the agents that monitor virtual machine resources. While the agents monitor the resources, the daemon monitors the agents. The daemon sends heartbeats to VCS on the ESX Server layer. The heartbeats inform VCS at the ESX Server layer if VCS at the virtual machine layer is functioning properly or not. In cases where the guest operating system does not boot, heartbeats are interrupted. An interrupted heartbeat can result in an UNKNOWN state and can also result in a failover.

When a resource (like Exchange) fails, the resource in the virtual machine reports an OFFLINE state. The OFFLINE state is reported to VCS at the ESX Server layer. VCS at the ESX Server layer then decides where the application’s virtual machine needs to move to re-continue services.

**Figure 13-1** State information passing between the virtual machine and the VCS node where the machine resides
Installing the applications

Install the application on the virtual machine. This is the application that you want VCS to monitor in the virtual machine. Refer to the application’s instructions for installation information. Note that you can install VCS for VMware ESX on virtual machines that already contain applications.

You must set up the application to automatically start when the virtual machine starts. VCS only monitors the application—it does not start or stop the applications. In case of a failover, VCS moves the entire virtual machine. When the virtual machine starts on the other node, the application must start automatically when the virtual machine boots.

Installing Veritas Virtual Machine Tools

Install Veritas Virtual Machine Tools 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 tools .iso file

1. From a Windows client, click Start > Programs > Symantec > Veritas Virtualization Manager.
2. Right-click the virtual machine where you want to add the .iso file. Select Add VCSVM-Tools ISO. VVM automatically selects the proper .iso file to match the operating system.
4. Click the OK button to add the .iso file.
   The ISO file is now available for your use.

To install Veritas Virtual Machine Tools

1. Once you have mounted the appropriate ISO file to your virtual machine, run the vcsvm-tools.exe file to install the tools.
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 Veritas Virtual Machine Tools
If you skipped the configuration of the tools, you can return to configure it.

To configure Veritas Virtual Machine Tools
1. On the virtual machine, open the Control Panel and go to Add or Remove Programs.
2. Select the Veritas Virtual Machine Tools 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 Veritas Virtual Machine Tools

Use the following procedure to verify that the tools are properly configured.

**To validate Veritas Virtual Machine Tools 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.

### Configuring application monitoring

After you have installed Veritas Virtual Machine Tools, configure resources within a virtual machine. You use the configuration wizards to configure the resources inside virtual machines.

Before you run the configuration wizards, make sure that you review the attributes for the agent that you want to configure.

- See “**SQL Server agent attributes**” on page 221.
- See “**Internet Information Services (IIS) agent attributes**” on page 228.
Configuring applications and resources in Windows virtual machines

Configuring application monitoring

- See “Exchange Server agent attributes” on page 232.
- See “GenericService agent attributes” on page 235.

Once you have reviewed the agent attributes, use the configuration wizard for your application. Use the following wizards:

- See “Configuring the SQL Server agents” on page 242.
- See “Configuring the IIS agent” on page 245.
- See “Configuring the Exchange agents” on page 247.
- See “Configuring the GenericService agent” on page 249.

**Note:** Every time you run a VCS configuration wizard on a virtual machine, the process creates a new configuration. To preserve your earlier configuration, you must recreate it when running the wizard.

---

**Prerequisites**

- Each guest operating system must have VMware Tools installed on it.
- The guestinfo interfaces of the VMware Virtual Machine tools must be enabled. Note that these interfaces are enabled by default.
- The Veritas Virtual Machine Tools must be installed on a virtual machine running Windows.
- The virtual machine or application administrator needs VCS privileges to configure 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.

**Configuring the SQL Server agents**

The SQL Server agents can be configured using the SQL Server Configuration wizard.
Prerequisites for configuring the SQL Server agents

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.

To configure 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 13-17  List of SQL Server services and agents in Instance Selection screen

<table>
<thead>
<tr>
<th>Microsoft SQL Server Services</th>
<th>SQL Server Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server [instance name]</td>
<td>SQL Server (2000 or 2005) instance selected for monitoring</td>
</tr>
<tr>
<td>Is either SQL Server 2000 or 2005</td>
<td></td>
</tr>
<tr>
<td>SQL Server (2005) Full-Text Search</td>
<td>Search</td>
</tr>
<tr>
<td>Creates full-text indexes on content and properties of structured and semi-structured data</td>
<td>Monitors the SQL Server Full-Text Search function</td>
</tr>
<tr>
<td>SQL Server (2005) Agent</td>
<td>SQLAgent</td>
</tr>
<tr>
<td>Executes jobs, monitors SQL Server, fires alerts, and allows some automation of administrative functions</td>
<td>Monitors the SQL Server Agent</td>
</tr>
<tr>
<td>SQL Server (2005) Analysis Services</td>
<td>Analysis</td>
</tr>
<tr>
<td>Provides online analytical processing (OLAP) and data mining functionality</td>
<td>Monitors the Server Analysis Services</td>
</tr>
</tbody>
</table>
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 13-18** List of chosen SQL Server services

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

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.

Configuring the IIS agent

The IIS agent can be configured using the IIS Configuration wizard.

Prerequisites for configuring the IIS agent

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.

To configure the IIS agent

1 Navigate to the configuration wizard by clicking Start > Programs > Symantec > Veritas Cluster Server > Configuration Wizards > IIS Configuration Wizard.

2 Review the Welcome screen and click Next.

3 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.

4 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.

5 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.

6 The Failure Action screen lists the IIS services that you have chosen to monitor.

7 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

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

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

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

11 Repeat step 7 through step 10 for each of the Sites listed. Click Next when you are done.
12 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.

13 When you are done reviewing the resources, click Next.

14 Click Finish to close the configuration wizard.

Configuring the Exchange agents

The Exchange agents can be configured using the Exchange Server Configuration wizard.

Prerequisites for configuring the Exchange agents

Before configuring the Exchange agents, make sure the Exchange Server services and the Protocol Virtual Servers are running, or in the “Started” state. If they are not running, you will not successfully configure the Exchange services or the Protocol virtual servers.

To check the status of the Exchange Server services

1 Open the Control Panel, select Administrative Tools, and click Services.

2 In the Services window, scroll down the list of services until you reach the Microsoft Exchange services and verify that their status is “Started”.

3 If the Exchange services are not in the “Started” state, right-click each non-started service and click Start.

In addition, the Exchange Protocol virtual servers must be enabled.

To check the status of the Exchange Protocol virtual servers

1 Open the Microsoft Exchange System Manager (Start > Microsoft Exchange > System Manager).

2 In the left panel of the window (treeview), select the appropriate Exchange Server that you plan to configure and expand its subdirectory.

3 The Protocols folder contains the folders for each of the virtual servers. Double click each folder and then right click the virtual server inside.

4 Click Start to start the virtual server, if it is not already running.

Once you have verified that the Exchange Server services and the Protocol virtual servers are enabled you can configure the Exchange agents.
To configure the Exchange agents

1. Navigate to the configuration wizard by clicking **Start > Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Exchange Server Agent Configuration Wizard**.

2. Review the Welcome screen and click **Next**.

3. In the Detailed Monitoring screen, specify the Exchange Server services that you want to monitor and configure. By default, the "Monitor the Microsoft Exchange services in detail" box and the "Configure Exchange Management service" box are checked.
   - If you select the Detailed Monitoring check box, Microsoft Exchange Information Store is the only Exchange service that is monitored in detail.
   - You can choose to configure either the Exchange Management service or the Exchange MTA service, both services, or neither service (deselect both check boxes).
   - If you choose not to monitor the two services, the other three Exchange services — Information Store, System Attendant, and Routing Engine — are automatically configured by the wizard. In addition, the wizard automatically checks the state of these three services to ensure that they are running.
   - Click **Next** when done.

4. In the Protocol Configuration screen, the four protocol servers — POP3, SMTP, IMAP4, and W3 — are selected by default. If you do not want to configure any of the protocol servers, deselect it.
   - Note that if any of the protocol servers are not running, the corresponding selection will be grayed out and not available for selection.
   - Click **Next** when done.

5. The Failure Action screen lists the Exchange services and protocol servers that you have chosen to monitor.

6. 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

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 7 through step 10 for each of the services listed. Click Next when you are done.

11 The Summary screen lists the 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. Double-click the selected resource and type the new name. If you choose to change the name, make sure that the new name is unique. Click Next.

12 Click Finish to close the wizard.

Configuring the GenericService agent

You can use the GenericService Agent configuration wizard to configure the GenericService Agent. The GenericService Agent can configure all of the services listed in the Services panel (Control Panel > Administrative Tools > Services). However, for the SQL Server, Exchange, and IIS services, you should use the individual configuration wizards provided for detailed configuration and monitoring, as the GenericService Agent configuration wizard only provides minimal configuration and monitoring.

In addition, you must run the GenericService Agent configuration wizard locally.

To configure the GenericService agent

1 From the Start menu, select All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > GenericService Agent.

2 Review the prerequisites listed in the Welcome screen and then click Next.

3 From the list provided, select the services that you want to configure. Click Next. You can click the Check All button to select all services or the Uncheck All button to deselect all the services.

4 The Failure Action screen lists the services that you have chosen to monitor. 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

5 Specify when to reset the fail count (after 1 day is the default value).
6. Specify the script path name. You can accept the default value, or click 
   Browse to select a different path name.

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

8. Repeat step 4 through step 7 for each of the services listed. Click Next when 
   you are done.

9. The Summary screen lists the 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. Double 
   click the selected resource and type the new name. If you choose to change 
   the name, make sure that the new name is unique. 
   Click Next.

10. Click Finish to close the wizard.

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, 
Exchange, 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.

  **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(PRSP0OL) is ONLINE

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 node. 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.

Removing Veritas Virtual Machine Tools from the virtual machine running Windows

This section describes steps for uninstalling Veritas Virtual Machine Tools.

1. Open the Windows Control Panel and click Add or Remove Programs.
2. Select Veritas Virtual Machine Tools 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 Tools are complete, you can close the Add or Remove Programs screen.
Configuring applications and resources in Windows virtual machines

Removing Veritas Virtual Machine Tools from the virtual machine running Windows
Administering VCS for VMware ESX

This section contains the following chapter:

- Chapter 14, "Administration" on page 255.
Administration

This chapter contains the following topics:

- Administering a VCS cluster
- Using VMware features and commands in a VCS environment
- Increasing allocated storage
- Preserving the last-known good copy of your configuration
- Using raw devices for the virtual machine’s boot image
- Performing maintenance on virtual machines and applications in virtual machines
Administering a VCS cluster

Use the following tools to administer a VCS cluster:

- The command line interface
- Cluster Manager (Java Console)
- Cluster Management Console (web-based)

See the *Veritas Cluster Server User's Guide* for more information about administering clusters.

To launch the Java Console from the Veritas Virtualization Manager

1. From the Veritas Virtualization Manager (VVM), right-click the cluster that you want to manage.
2. Right-click a cluster icon and select **Launch VCS Console**.

Using VMware features and commands in a VCS environment

VCS is compatible with VMware’s VMotion, DRS, and maintenance mode. The ESXHost agent, which VCS automatically configures during installation, ensures compatibility with these features.

See the following topics for more information:

- “Using VMotion in a VCS environment” on page 256
- “Using maintenance mode in VCS environment” on page 260
- “Using DRS in a VCS environment” on page 259

Using VMotion in a VCS environment

You can use VMotion in a VCS environment. When you trigger VMotion through the Virtual Infrastructure Client, VCS accommodates the state changes that occur to the virtual machine.

You can also trigger VMotion through VCS using the service group migration feature. You can use all of the standard VCS management clients to perform service group migrations.
Prerequisites for accommodating VMotion triggered through the VirtualCenter Infrastructure

For VMotion to work properly in a VCS environment, make sure that you have met the following prerequisites:

- You have installed and configured VCS on all nodes in the VCS cluster.
- You have installed and configured VMware clustering on the exact same nodes that are in the VCS cluster.
- You have enabled the VMware's VMotion feature.
- You have disabled VMware's HA feature.
- You have configured a VCS service group for the virtual machine to ensure the machine's high availability.

Prerequisites for setting up service group migration

You must meet the prerequisites from the previous section and the following prerequisites for service group migration:

- Ensure that you have set the following attributes for the ESXVirtualMachine resource in the service group for a virtual machine:
  - username
  - password
  - esxhostdomain
  - vmname
  - sslcert

For more information on the above ESXVirtualMachine agent attributes, refer to the *Veritas Cluster Server Bundled Agents Reference Guide*. For more information on using the Cluster Manager (Java Console) to set attributes for the ESXVirtualMachine resource, see the *Veritas Cluster Server User’s Guide*.

- You need to set the sslcert attribute above to point to a keystore file. To create and copy the keystore file, refer to:
  - See “Preparing keystores” on page 142.
  - See “Copying the keystore file from the VirtualCenter Server to each of the ESX Sever nodes in the VCS cluster” on page 145.
Verifying if a service group can be migrated

Use the testVCConnect action to verify the connectivity from the cluster nodes to the VirtualCenter Server.

Run the testVCConnect action on each node in the cluster. You can use any of the standard VCS management clients to invoke an Action function a particular VCS resource. The following example uses a command line interface.

Run the testVCConnect on each node of the cluster:

```
# hares -action resname 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.

Migrating service groups

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 from the command line

◆ Enter the following command on any VCS node:

```
# hagrp -migrate service_group -to system
```

Where the service_group variable is the name of the service group that you want to move, and the system variable is the node where you want the service group to move to.

To migrate a service group from the Cluster Manager (Java Console)

1. From the Veritas Virtualization Manager (VVM), right-click the cluster that you want to migrate.
2. Right-click a cluster icon and select Launch VCS Console.
3. In the Service Groups tree, right-click the service group that you want to migrate.
4. Select bring your mouse down to Migrate to, and select the server where you want to migrate the service group.
Restrictions for service group migration
A few restrictions exist for service group migration. These restrictions follow:

- You can only migrate a service group that is completely online. VCS does not support cold migration.
- The `-migrate` option is not supported for migrating parallel service groups, for migrating hybrid service groups across system zones or across clusters.
- The `-migrate` option is not supported if the VCS service group contains more than one ESXVirtualMachine resource that can be migrated.
- The ability of VMotion to migrate virtual machines (either using the hagrp `-migrate` command or through the VirtualCenter Server) is not supported when you have multiple virtual machines that are configured in a single service group. VMotion is not supported if you have tiered applications configured in a single VCS service group. Tiered applications that are configured in different service groups are acceptable.
- VCS does not support running the hagrp `-migrate` command to trigger VMotion if you have configured ESX hosts in VMware VirtualCenter using IP addresses instead of fully qualified host names.

Using DRS in a VCS environment
You can use DRS in a VCS environment. See the following topics for more information:

- “Enforcing compatibility between VCS and VMware features (DRS and ESX Server maintenance mode)” on page 65
- “Restrictions for DRS in a VCS environment” on page 260
- “About adding and removing nodes” on page 100

Prerequisites for DRS in a VCS environment
For DRS to properly work in a VCS environment, make sure that you have met the following prerequisites:

- You have installed and configured VCS on all nodes in the VCS cluster.
- You have installed and configured VMware clustering on the exact same nodes that are in the VCS cluster.
- You have enabled the VMware’s DRS feature.
- You have disabled VMware’s HA feature.
Restrictions for DRS in a VCS environment
A few restrictions exist for DRS in a VCS environment. Adding and removing nodes from a cluster require special consideration in a DRS environment. Review the following restrictions:

- You must add a node to the VCS cluster before you add the same node to the VMware cluster. This prevents DRS from moving a virtual machine to a host that does not have VCS. If you add a node to VMware cluster with DRS enabled, it needs to added to the VCS SystemList attribute and vice-versa.
- You must delete a node from VMware cluster before you remove the same node from VCS cluster. This prevents DRS from moving a virtual machine to a host that does not have VCS.
- In order to remove a node from DRS cluster, you need to put it into maintenance mode. You then remove it from VMware DRS cluster. The ESXHost agent detects this state change and internally performs a VCS system freeze command with the evacuate option. No automatic way exists to delete a node that is deleted from DRS cluster and vice-versa.

Using maintenance mode in VCS environment
The VCS equivalent of maintenance mode is to perform a VCS system freeze command with the evacuate option (hasys -freeze -evacuate sysname). Evacuate fails over all the service groups that are online or active on a node to other nodes of the cluster. VCS then prevents service groups from coming online or failing over to a system that is already frozen. The sum of this command is to move service groups off the selected node, and to prevent further service groups from failing back to this node.

You can run the VCS system freeze command with the evacuate option from all of the standard VCS management clients. For more information on performing a system freeze command with the evacuate option, refer to the Veritas Cluster Server User’s Guide.

Maintenance mode notes
Review the following notes about using maintenance mode:

- The ESXHost agent, which VCS automatically creates, exists to maintain parity between a VMware DRS cluster and VCS.
- When you put a VMware node into maintenance mode with the Virtual Infrastructure Client, maintenance mode eliminates that virtual machine from being a virtual machine target under DRS. As soon as the ESXHost agent detects this mode, it performs a VCS system freeze with the evacuate option.
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 file systems, for more information on supported file systems:

See "Supported guest operating systems" on page 29.

Prerequisites

- The virtual machine must be configured for VCS.
- VMware Tools must be installed in the virtual machine.
- Veritas Virtual Machine Tools must be installed on the virtual machine.
Increasing allocated storage

- 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** > **Symantec** > **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 146.
3. Right-click the virtual machine where you want to increase storage. Select **Grow filesystem**.
4. Review this screen and click the **Next** button.
5. Select the amount of storage that you want to add, note that you can use small number such as 0.03.
6. Enter the mount point for the storage (for example /apache). Click the **Next** button.
7. Click a datastore to select it. If the current LUN does not have space for a new datastore, select an available LUN for a new datastore. Click the **Next** button.
8. Review the summary. Click the **Back** button to return and change settings.
9. Click the **Finish** button to increase the allocated storage.
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.

Using raw devices for the virtual machine’s boot image

VMware provides the ability to create virtual machines that uses a shared raw device for its boot image. The VMware infrastructure leverages its raw device mapping (RDM) feature to provide this functionality. VCS supports this use of raw devices and raw device mapping in certain high-availability configurations with some limitations.

Although VMotion is supported in this configuration, the possibility of data corruption can exist. This can occur when two virtual machines try to access the same shared raw device at the same time on two different physical nodes.

For more information about RDM, refer to the VMware Infrastructure Documentation.

**Note:** You cannot use raw device mapping (RDM) in a disaster recovery-enabled environment.

Setting up shared raw device storage under VCS

After you have set up a VCS for VMware ESX cluster, you can configure virtual machines to use raw devices. In this configuration, VMotion is allowed. When you set up the virtual machine, you need to configure the shared raw device as a Disk resource in a service group.

Figure 14-1 shows a two-node cluster. Each system has its own local VMFS mounted storage. The first system, sys1, has the virtual machine vm1. Virtual machine vm1’s configuration files, and its raw device mapping (RDM) file are
Using raw devices for the virtual machine's boot image

The service group for the shared raw device

For more information on creating and using service groups refer to the Veritas Cluster Server User’s Guide.
Performing maintenance on virtual machines and applications in virtual machines

When you need to perform maintenance on a virtual machine, or an application that does not have the ability to perform a graceful shutdown, use following procedures.

Performing maintenance on a virtual machine

You can perform maintenance on a virtual machine by temporarily freezing the service group that contains the ESXVirtualMachine resource.

Perform the following steps from inside the virtual machine that runs these resources.

To perform virtual machine maintenance

1. For Linux, open a terminal window, find the home/install directory of the VCS Virtual Machine Tools, and make sure it is in the PATH.
   # export PATH=$PATH:/opt/VRTSvcs/bin

2. Find the VCS resource name and the service group name that is associated with this virtual machine.
   - To find the resource name on Windows, type the following command:
     C:\> type "%VCS_HOME%\..vcsvmsresname"
   - To find the resource name on Linux, type the following command:
     # cat /etc/VRTSvcs/.vcsvmsresname
   - To find the service group that the resource resides in, type the following command at the prompt:
     hares -value vcs_vm_res_name Group
     Where vcs_vm_res_name is the name of the resource that you found.
     Record the output of the hares command, you need to use this service group name in the following step.

3. Freeze the service group. At the prompt, type:
   # hagrp -freeze service_group_name
   Where service_group_name is the name of the service group that the resource resides in.

4. Perform the virtual machine maintenance.

5. Unfreeze the service group. At the prompt, type:
   # hagrp -unfreeze service_group_name
   Where service_group_name is the name of the service group that the resource resides in.
Performing maintenance on applications inside the virtual machine

For VCS agents that have the ability to detect a graceful shutdown, you can directly shut down the application, perform maintenance, and then re-start it. For agents that do not have the ability to detect a graceful shut down (the Mount and Application agents) use the following procedure.

Perform the follow steps from inside the virtual machine that runs the Application or Mount resources.

**To bring down the Mount or Application resource for maintenance**

1. For Linux, open a terminal window, find the home/install directory of the VCS Virtual Machine Tools, and make sure it is in the PATH.
   
   ```
   export PATH=$PATH:/opt/VRTSvcs/bin
   ```

2. Find the VCS resource name and the service group name that is associated with this virtual machine.
   - To find the resource name on Windows, type the following command:
     ```
     C:\> type "%VCS_HOME%\.vcsvmresname"
     ```
   - To find the resource name on Linux, type the following command:
     ```
     # cat /etc/VRTSvcs/.vcsvmresname
     ```
   - To find the service group that the resource resides in, type the following command at the prompt:
     ```
     hares -value vcs_vm_res_name Group
     ```
     Where vcs_vm_res_name is the name of the resource that you found.
     Record the output of the `hares` command, you need to use this service group name in the following step.

3. Freeze the service group. At the prompt, type:
   ```
   # hagrp -freeze service_group_name
   ```
   Where service_group_name is the name of the service group that the resource resides in.

4. Stop the VCS agent management daemon. At the prompt, type:
   - On Windows:
     ```
     C:\> net stop vcsagmd
     ```
   - On Linux:
     ```
     # /etc/init.d/vcsagmd stop
     ```

5. Perform the application maintenance on the Mount or the Application resource.

6. Start the VCS agent management daemon. At the prompt, type:
   ```
   # /etc/init.d/vcsagmd start
   ```
Performing maintenance on virtual machines and applications in virtual machines

7  Unfreeze the service group. At the prompt, type:

    # hagrp -unfreeze service_group_name

Where service_group_name is the name of the service group that the resource resides in.

Troubleshooting maintenance

If you find that the commands from the preceding procedures do not work correctly or return errors, reconfigure the Veritas Virtual Machine Tools.

For Linux virtual machines:

See “Configuring the Veritas Virtual Machine Tools” on page 209.

For Windows virtual machines:

See “Configuring Veritas Virtual Machine Tools” on page 240.
Performing maintenance on virtual machines and applications in virtual machines
A

about
  global clusters 156
  Veritas Virtualization Manager 140
accessing service groups 153, 173
adding
  users 57
adding node
  to a cluster 99
  to a one-node cluster 120
administering
  tools 256
agent
  GenericService 234
  SQL Server 2000 service 220
  SQL Server 2005 Agent service 220
  SQL Server 2005 Analysis service 220
  SQL Server 2005 Search service 220
  SQL Server 2005 service 220
agent functions
  Application agent 198
  GenericService 235
  Mount agent 202
  VCS agent for Apache Web server 188
  VCS agent for Oracle 180
  VCS agent for SAP NetWeaver 194
agent operations
  ExchProtocol agent 232
  ExchService agent 231
agents
  Application 198
  DNS 158
  Exchange agents, agent
    Exchange 230
  GenericService 234
  Mount 202
  VCS agent for Apache Web server 188
  VCS agent for Oracle 179
  VCS agent for SAP NetWeaver 192
allocated storage
  prerequisites for increasing 261
Apache agent attributes
  ConfigFile 189
  DirectiveAfter 190
  DirectiveBefore 191
  EnableSSL 191
  EnvFile 191
  HostName 189
  httpdDir 189
  PidFile 189
  Port 190
  ResLogLevel 190
  SecondLevelMonitor 191
  SecondLevelTimeout 192
  SharedObjDir 191
  User 190
Application agent
  about 198
  agent functions 198
  state definitions 199
application monitoring 206, 237
attribute definitions
  GenericService agent 235
  IIS agent 228
  MSDTC agent 226
  MSSearch agent 223
  SQL Server 2000 agent 221
  SQL Server 2005 agent 223
  SQL Server 2005 Agent service agent 225
  SQL Server 2005 Analysis service agent 226
attributes
  for ExchProtocol agent 234
  for ExchService agent 233
  Mount agent 203
B

basic monitoring
  health check 180
  process 180
bundled agents
  types.cf file 118
Index

C

cables
  cross-over Ethernet 101
  cables, crossover Ethernet 37
  centralized cluster management 57
cluster
  creating a single-node cluster, installer 114
  creating a single-node cluster, manual 115
  four-node configuration 17
  removing a node from 106
  verifying 67
  verifying operation 96
  cluster connector
    uninstalling, UNIX 81
  cluster management 59
  Cluster Manager
    installing Java Console 65
ClusterService group
  configuring 160
  sample configuration 161
command-line options 77
commands
  gacconfig 95, 125
  hastart 105
  hastatus 96
  hasys 96
  lltconfig 84
  llstat 93
  vxlicinst 76, 103, 117
  vxlicrep 75, 103, 117
communication channels 19
communication disk 19
configuration files
  main.cf 85
  types.cf 85, 119
configuring
  disaster recovery 155, 165
  GAB 125
  GenericService agent 249
  hardware 26
  LLT, manual 123
  private network 37
configuring application monitoring
  Linux guest operating system 210
  Windows guest operating system 241
configuring replication 161
configuring VCS 54
  adding users 57
  Cluster Connector 57

Cluster Management Console 59
  event notification 60, 61
  global clusters 62
  overview 50
  Veritas Cluster Management Console 57
configuring virtual machines
  disaster recovery 168
  disaster recovery, prerequisites for 167
  for high availability 150
  secure DNS update 167
creating
  global service group 164
  service groups, disaster recovery 172
  service groups, high availability 152
  crossover cables 37

D
DetailMonitor attribute
  ExchProtocol agent 234
  ExchService agent 233
directives, LLT 124
disaster recovery 155
  global clusters 156
  service groups 172
disk space
  directories 26
disk space, required 26
DNS agent 158
DRS 259
  prerequisites 259

E
encrypting passwords 211
Ethernet controllers 102
Exchange agent
  supported protocols 231
  supported services 230
Exchange agents
  about 230
Exchange Protocol agent 231
Exchange Service agent 230
ExchProtocol agent
  attributes 234
  operations 232
  state definitions 232
ExchProtocol agent attributes
- DetailMonitor 234
- LanmanResName 234
- Protocol 234
- VirtualServer 234

ExchService agent attributes
- operations 231
- state definitions 231

ExchService agent attributes
- DetailMonitor 233
- LanmanResName 233
- Service 233

F
- fibre channel 26
- file system
  - grow 261
  - fire drill
    - last-known copy 263

G
- GAB
  - description 19
  - manual configuration 125
  - port membership information 95
  - verifying 95
- gabconfig command 95, 125
- -a (verifying GAB) 95
- in gabtab file 85
- gabtab file
  - creating 125
  - verifying after installation 85
- GenericService agent attributes
  - attribute definitions 235
  - configuring 249
  - description 234
  - state definitions 235
- GenericService agent attributes
  - DelayAfterOffline 235
  - DelayAfterOnline 236
  - Domain 236
  - LanmanResName 236
  - Password 236
  - service_arg 236
  - ServiceName 235
  - UserAccount 236
  - UseVirtualName 236
- Global Cluster option 35
- global clusters 35
  - about 156
  - ClusterService group 159, 160
  - framework 158
  - management 157
  - overview 156
  - prerequisites for 158
  - resiliency 158
  - setting up 159
  - wide-area heartbeats 158
- global clusters service groups
  - service groups
    - global clusters 157
- global clusters, cluster set up 158
- global clusters, configuration 62
- global service group
  - creating 164
  - growing file system 261
  - GuestOSApp agent 214, 250

H
- hardware
  - configuration 18
  - configuring network and storage 26
  - hastart 105
  - hastatus -summary command 96
  - hasys -display command 96
  - health check APIs 180
  - health check monitoring 180
  - heartbeats
    - wide area 158
  - high availability
    - service groups 152
  - hubs 37
  - hubs, independent 101

I
- IIS agent
  - attribute definitions 228
  - configuring 245
  - prerequisites 245
- IIS agent attributes
  - AppPoolMon 229
  - DetailMonitor 229
  - DetailMonitorInterval 229
  - IPResName 229
  - IPAddress 228
  - PortNumber 228
SiteName 228
SiteType 228
increasing
allocated storage 261
installing
required disk space 26
using installvcs program 48
Veritas Virtual Machine Tools 238
Veritas Virtualization Manager 139
VVM 208
installing and configuring VCS
overview 50
installing applications
Linux guest operating system 207
Windows guest operating system 238
installing VCS
checking systems 51
choosing packages 54
licensing 53
overview 50
required information 43
starting 52
utilities 48
installing VCS, example 50
installing Veritas Virtual Machine Tools
Linux guest operating system 207
installvcs 48
options 49
installvcs prompts
b 49
n 49
y 49
intentional offline
requirement for Oracle agent 179

J
Java Console
installing 65
installing on UNIX 65
installing on Windows workstation 66

L
LanmanResName attribute
ExchProtocol agent 234
ExchService agent 233
last-known good copy 263
launch
Java Console 256
license keys
adding with vxlicinst 76, 103, 117
obtaining 42
replacing demo key 76
licenses, information about 75
licenses, showing information 103, 117
licensing commands
vxlicinst 42
vxlicrep 42
vxlictest 42
licensing VCS 53
links, private network 37, 84
Linux applications
supported software 179
Linux guest operating system
about 178
application monitoring 210
installing applications 207
installing Veritas Virtual Machine Tools 207
removing Veritas Virtual Machine Tools 215
supported software 179
Linux guest operating system application
monitoring
prerequisites 210
Linux guest operating system applications
verifying 214
LLT
description 19
directives 124
interconnects 39
manual configuration 123
verifying 93
LLT directives
link 124
link-lowpri 124
set-cluster 124
set-node 124
lltconfig command 84
llthosts file, verifying after installation 84
llttstat command 93
llttab file, verifying after installation 84

M
main.cf file 85
example 85
maintenance
applications 265
applications in VMs 266
virtual machine 265
virtual machines 265
maintenance mode 260
managing
global clusters 157
managing clusters, centrally 57
MANPATH variable, setting 37
manual installation
preparing 102
media speed 39
optimizing 39
membership information 96
migrating service groups 258
monitoring
applications 206, 237
monitoring levels 179
Mount agent
agent functions 202
attributes 203
description 202
MSDTC agent
attributes 226
MSDTC agent attributes
LanmanResName 226
LogPath 226
MountResName 226
MSSearch agent
attributes 223
MSSearch agent attribute
AppName 223

N
Netlsnr agent attributes
AgentDebug 187
AgentDirectory 188
Encoding 187
EnvFile 187
Home 186
Listener 186
LsnrPwd 186
MonScript 187
Owner 186
TnsAdmin 186
network partition
protecting against 18
Network partitions
protecting against 19

O
operations
ExchProtocol agent 232
ExchService agent 231
optimizing
media speed 39
Oracle
error handling 181
Oracle agent attributes
AgentDebug 185
AgentDirectory 185
AutoEndBkup 183
DetailMonitor 184
Encoding 185
EnvFile 183
Home 183
MonitorOption 184
MonScript 184
Owner 182
Pfile 183
Pword 185
ShutDownOpt 183
Sid 182
StartUpOpt 183
Table 185
User 184
overview
Veritas Virtualization Manager 140

P
passwords, encrypting 211
PATH variable
setting 37, 116
VCS commands 93
performing
maintenance 260
port a
membership 95
port h
membership 95
port membership information 96
Preparing 33
preparing
manual installation 102
Prerequisites
Windows guest OS 220
prerequisites
  DRS 259
  Linux guest operating system application monitoring 210
  service group migration 257
  VMotion 257
private network, configuring 37
process monitoring 180
Protocol attribute 234

R
RAM, installation requirement 26
raw devices 263
RDM 263
  using 263
removing
  Veritas Virtual Machine Tools 251
  Veritas Virtualization Manager 146
removing a system from a cluster 106
removing Veritas Virtual Machine Tools
Linux guest operating system 215
replication
  configuring 161
  configuring, second cluster 163
  linking clusters 163
  reversing 170
  solutions 28
replication agents
  agents
  replication 158
replication setup 159
replication solutions 28
required servers 27
requirements
  Ethernet controllers 26
  fibre channel 26
  hardware 26
  RAM Ethernet controllers 26
  SCSI host bus adapter 26
  Veritas Virtualization Manager 141
  VMware components 28
resources
  GuestOSApp 214, 250
restrictions
  DRS 260
  service group migration 259
rpm -e command 110
rsh 39, 52, 67, 79

S
sample configuration
  ClusterService group 161
SAP NetWeaver agent attributes
  EnvFile 195
  InstName 195
  InstType 195
  MonitorProgram 197
  ProcMon 195
  ResLogLevel 196
  SAPAdmin 196
  SAPMonHome 196
  SAPSID 196
  SecondLevelMonitor 198
  StartProfile 197
SCSI host bus adapter 26
secure DNS update
  configuration 167
See 39, 171
servers, required 27
Service attribute 233
service group migration
  prerequisites 257
  restrictions 259
  verifying 258
service groups
  disaster recovery 172
  high availability 152
  migration, restrictions for 259
setting
  MANPATH variable 37
  PATH variable 37, 116
setting up
  replication 159
single-node cluster
  adding a node to 120
single-system cluster
  creating 114, 115
  modifying startup files 118
SMTP email notification 60
SMTP notifications 35
SNMP notifications 35
SNMP trap notification 61
SQL Server 2000 agent attributes
  DetailMonitor 222
  Domain 222
  FaultOnDMScriptFailure 222
  Instance 221
  IsGuestOS 221
LanmanResName 221
MountResName 221
Password 222
SQLDetailMonitorTimeout 222
SQLFile 223
SQLOfflineTimeout 221
SQLOnlineTimeout 221
Username 222

SQL Server 2005 agent attributes 223
SQL Server 2005 agent attributes
DetailMonitor 224
Domain 225
FaultOnDMScriptFailure 224
Instance 223
IsGuestOS 224
LanmanResName 223
Password 225
SQLDetailMonitorTimeout 224
SQLFile 225
SQLOfflineTimeout 223
SQLOnlineTimeout 223
Username 224

SQL Server 2005 Agent service agent attributes 225
SQL Server 2005 Agent service agent attributes
LanmanResName 225
SQLServer2005ResName 225
SQL Server 2005 Analysis service agent attributes 226
SQL Server 2005 Analysis service agent attributes
LanmanResName 226
SQLServer2005ResName 226
SQL Server agent attributes 221

SQL Server agents
about 220
agent for SQL Server 2000 service 220
agent for SQL Server 2005 Agent service 220
agent for SQL Server 2005 Analysis service 220
agent for SQL Server 2005 Search service 220
agent for SQL Server 2005 service 220

ssh 39, 52, 67
start
Java Console 256
starting installation
installvcs program 52
starting VCS 64

state definitions
Application agent 199
ExchProtocol agent 232
ExchService agent 231
GenericService agent 235
Mount agent 202
VCS agent for Apache Web server 188
VCS agent for Oracle 182
VCS agent for SAP NetWeaver 194

storage
fully shared vs. distributed 18
shared 18

storage, increase 261
supported applications, detailed monitoring 30
supported protocols 231
supported services 230
supported software 28
detailed application monitoring 30
guest operating systems 29
Linux applications 179
Linux guest operating system 179

system communication using rsh, ssh 39
system state attribute value 96

T

types.cf 118
bundled agents 118
types.cf file 119
included in main.cf 85

U

uninstalling
cluster connector, UNIX 81
uninstalling, VCS 79
uninstallvcs 79
using RDM 263

V

validating
Veritas Virtual Machine Tools 241
variables
MANPATH 37
PATH 37, 116

VCS
command directory path variable 93
configuration files
main.cf 85
types.cf 85
example installation 50
global clusters 35
installation example 50
installing 50
installing using program 48
replicated states on each system 18
VCS agent for Apache Web server
about 188
agent functions 188
state definitions 188
VCS agent for Oracle
about 179
agent functions 180
detecting intentional offline 179
state definitions 182
VCS agent for SAP NetWeaver
about 192
agent functions 194
monitor function 194
state definitions 194
VCS Agent Management Daemon 250
VCS Agent Management Deaemon 214
vcsagmd 214, 250
vcsencrypt utility 211
verifying
  cluster 67
  Linux guest operating system applications 214
  service group migration 258
  virtual machine failover 173
verifying the configuration
  Windows guest OS 250
Veritas Virtual Machine Tools
configuring 238
installing 238
installing and configuring 207
removing 215
removing from Windows guest operating system 251
validating 241
Veritas Virtual Machine Tools ISO file
mounting 207
Veritas Virtualization Manager
disaster recovery configuration 165
installation 139
removing 146
requirements 141
virtual machine fail over
verification 173
virtual machines
  high availability, prerequisites for 150
  maintaining 265
  running Linux 178
virtual machines, creation 168
virtual machines, high availability 150
VirtualServer attribute 234
VMotion 256
  prerequisites 257
VMware requirements 28
vswif1 50
VVM
  disaster recovery 168
  installing 208
vxlicinst 42
vxlicinst command 76, 103, 117
vxlicrep 42
vxlicrep command 75, 103, 117
vxlictest 42
W
Windows guest operating system
  application monitoring 241
  installing applications 238
  installing Veritas Virtual Machine Tools 238
  prerequisites 220
  removing Veritas Virtual Machine Tools from 251
  verifying the configuration 250