

Veritas™ Cluster Server Release Notes

VMware ESX

5.0



Veritas Cluster Server Release Notes

Copyright © 2007 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be “commercial computer software” and “commercial computer software documentation” as defined in FAR Sections 12.212 and DFARS Section 227.7202.

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

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Veritas product. Such third-party software is licensed separately by its copyright holder.

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

Licensing and registration

Veritas Cluster Server is a licensed product. See the *Veritas Cluster Server Installation Guide* for license installation instructions.

Technical support

For technical assistance, visit:

http://www.symantec.com/enterprise/support/assistance_care.jsp.

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

Veritas Cluster Server Release Notes

- [Introduction](#)
- [Features of Veritas Cluster Server](#)
- [Veritas agents](#)
- [System requirements](#)
- [Installation notes](#)
- [Software limitations](#)
- [Known issues](#)
- [Documentation](#)
- [Third-party legal notices](#)
- [Getting help](#)

Introduction

This document provides important information regarding Veritas Cluster Server (VCS) 5.0 for ESX. Review this entire document before installing VCS.

For the latest information on updates, patches, and software issues regarding this release, see the following TechNote on the Symantec Technical Support website:

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

Features of Veritas Cluster Server

This release of Veritas Cluster Server offers the following features.

Support for monitoring applications running inside virtual machines

VCS provides the ability to monitor applications running inside virtual machines. You can configure VCS to fail over the entire virtual machine to another node in the cluster when the application faults. VCS provides agents to monitor the following applications running inside virtual machines:

Virtual machines running Linux	Apache Application Oracle
Virtual machines running Windows	Internet Information Services (IIS) SQL Server

VCS interface to trigger VMotion

Use the `hagrp -migrate` command to trigger VMotion for a virtual machine configured as a VCS resource. You can also run this command from Cluster Management Console.

Support for VMotion and Distributed Resource Scheduler

VCS recognizes virtual machine migration initiated by VMotion or DRS. VCS does not interpret this motion as a fault.

Support for detecting intentional offline for specific applications

Intentional Offline is a capability built into some application agents to allow the agent to identify when an application has been intentionally shutdown opposed to when an application has crashed. The purpose of Intentional offline is to allow administrators to manage the applications (start/stop) running inside their virtual machines without having to coordinate application start and stop with the cluster.

The following agents support detection of an intentional offline:

Virtual machines running Linux	Apache Oracle
Virtual machines running Windows	Internet Information Services (IIS) SQL Server

Note that Intentional Offline is not supported by all application agents. Refer to the agent documentation to verify whether Intentional offline is supported by the agent.

Dynamic increase of storage allocated to virtual machines

You can dynamically increase the size of your application mount points or file systems inside the virtual machine without having to reboot the virtual machine. See the *Veritas Cluster Server Implementation Guide* for more information

Cluster Management Console

Cluster Management Console enables administration and analysis for VCS clusters in your enterprise from a single console. You can install Cluster Management Console on a standalone system to manage multiple clusters or you can install the console on cluster nodes to manage a local cluster.

See “[Installing Veritas Cluster Management Console Management Server](#)” on page 13.

VCS privileges for operating system user groups

VCS 5.0 lets you assign VCS privileges to native users at an operating system (OS) user group level in secure clusters.

Assigning a VCS role to a user group assigns the same VCS privileges to all members of the user group, unless you specifically exclude individual users from those privileges.

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

Five levels of service group dependencies

VCS supports configuring up to five levels of service group dependencies. The exception is the online local hard dependency, for which only two levels are supported.

Enhancements to the hastop command

You can customize the behavior of the hastop command by configuring the EngineShutdown attribute for the cluster.

EngineShutdown Value	Description
Enable	Process all hastop commands. This is the default behavior.
Disable	Reject all hastop commands.
DisableClusStop	Do not process the hastop -all command; process all other hastop commands.
PromptClusStop	Prompt for user confirmation before running the hastop -all command; process all other hastop commands.
PromptLocal	Prompt for user confirmation before running the hastop -local command; reject all other hastop commands.
PromptAlways	Prompt for user confirmation before running any hastop command.

Backup of VCS configuration files

VCS backs up all configuration files (<config>.cf) including main.cf and types.cf to <config>.cf.autobackup. The configuration is backed up only if the BackupInterval is set and the configuration is writable.

When you save a configuration, VCS saves the running configuration to the actual configuration file (i.e. <config>.cf) and removes all autobackup files. This does away with the VCS behavior of creating .stale files.

If you do not configure the BackupInterval attribute, VCS does not save the running configuration automatically.

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

Separate logger thread for HAD

The VCS engine, HAD, runs as a high-priority process to send heartbeats to kernel components and to respond quickly to failures. In VCS 5.0, HAD runs logging activities in a separate thread to reduce the performance impact on the engine due to logging.

on a specific node. See the *Veritas Cluster Server User's Guide* for more information on running virtual fire drills.

Daemon Down Node Alive (DDNA)

Daemon Down Node Alive (DDNA) is a condition in which the VCS high availability daemon (HAD) on a node fails, but the node is running. When HAD fails, the hashadow process tries to bring HAD up again. If the hashadow process succeeds in bringing HAD up, the system leaves the DDNA membership and joins the regular membership. See the *Veritas Cluster Server User's Guide* for more information.

Use comma or semicolon as delimiter

VCS 5.0 does not support using spaces as delimiters to separate vector, association, or keylist values. You must use a comma or a semicolon as a delimiter.

Location of message catalogs and attribute pools

VCS stores binary message catalogs (BMCs) at the following location:

`/opt/VRTS/messages/language/module_name`

The variable *language* represents a two-letter abbreviation.

The attribute pools also move from `/var` to `/opt`.

Veritas agents

VCS bundles agents to manage key resources used in the cluster. The implementation and configuration of bundled agents vary by platform.

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

VCS also provides agents for the management of key enterprise applications.

In addition to the agents for enterprise applications provided with VCS, other agents are available through an independent Symantec offering called the Veritas Cluster Server Agent Pack. The agent pack includes the currently shipping agents and is re-released regularly to add new agents that are now under development.

Contact your Symantec sales representative for information about agents included in the agent pack, agents under development, and agents available through Symantec consulting services.

System requirements

System requirements for VCS are as follows.

Supported hardware

For the latest information on supported hardware, see the hardware compatibility list published by VMware.

Supported software for VCS cluster nodes

VCS supports ESX Server 3.0

Supported operating systems in the virtual machines

- Windows 2000, Windows Server 2003
- Red Hat Enterprise Linux 4 (RHEL 4) Update 3
- Suse Linux Enterprise Server 9 (SLES 9) Service Pack 3

Supported applications in the Linux guest OS

- Oracle 10g
- Apache Web server
 - Apache HTTP server 1.3, 2.0, and 2.2
 - IBM HTTP Server 1.3 and 2.0

Supported applications in the Windows guest OS

- Microsoft SQL Server 2000 Standard Edition or Enterprise Edition
- Microsoft SQL Server 2005, 32-bit
- Microsoft Internet Information Services (IIS) 5.0 and 6.0

Supported software for Cluster Management Console

You can install Cluster Management Console on a standalone system to manage multiple clusters or you can install the console on cluster nodes to manage a local cluster.

When you set up a management server to manage multiple clusters, you can connect to the clusters directly or install the cluster connector on cluster nodes to enable connection across firewalls.

See [“Installing Veritas Cluster Management Console Management Server”](#) on page 13.

Install Mode

Multi-cluster mode. To manage multiple clusters. Installed on a standalone system designated the *management server*.

Single cluster mode. To manage a single cluster. Installed on cluster nodes.

Supported software

- Solaris 8, 9, and 10, with patches indicated by Sun.
- Windows 2000 Server, Advanced Server, and Datacenter, with SP4 or patches as indicated by Microsoft.
- Windows Server 2003 Standard Edition, Datacenter Edition, Enterprise Edition, and Web Edition, with patches as indicated by Microsoft.

Note: Windows Management Instrumentation (WMI) must be installed on Windows 2003 systems prior to installing Cluster Management Console.

You can install Cluster Management Console in this mode only with VCS 5.0 in a fresh install or upgrade scenario. See [“Supported software for VCS cluster nodes”](#) on page 11.

Supported browsers

Veritas Cluster Management Console is supported on the following browsers:

- Microsoft Internet Explorer 6.0 with SP2 or later
- Firefox 1.5 or later

Veritas Cluster Management requires the Macromedia Flash Plugin v8.0.

Installation notes

Refer to the *Veritas Cluster Server Implementation Guide* for instructions on how to install VCS 5.0. The guide is in the `cluster_server/docs` directory of the software disc.

The following information includes guidelines, tips, and other considerations for installing the product.

Do not configure Security Services when installing VCS

This release of VCS does not support configuring the Symantec Product Authentication Service. Do not configure the service when installing VCS.

Change default password after installing VCS

When you install and configure VCS, if you do not choose the secure mode, the `installvcs` program creates a user *admin* with the password *password*. The user has administrative privileges to the cluster.

Symantec recommends you change the password of the user after installing and configuring VCS.

Installing VCS with the response file does not work

This release does not support installing VCS using the response file. [802303]

Installing Veritas Cluster Management Console Management Server

If you plan to set up a management server to administer your clusters, install the Veritas Cluster Management Console on a system outside of the managed clusters.

To install Veritas Cluster Management Console

- 1 Go to <http://www.symantec.com/enterprise/products/index.jsp>.
- 2 In the **Product Finder** box, click **Select Product/Service** and selected **High Availability>Veritas Cluster Server**.
- 3 In the **Learn about this product** box, click **Trialware**.
- 4 Click Storage Foundation and High Availability Solutions.
- 5 On the Trialware Download page, click **Download Now**.
- 6 Accept the export restrictions agreement.
- 7 Enter your credentials or create a new user account.

- 8 On the **Software Download** page, click the link for **Storage Foundation and HA Solutions, Solaris, v5.0** to begin the download process.
Note that the Solaris package contains installers for setting up a management server on Solaris or Windows systems.
- 9 After the download completes, extract the files.
- 10 Install the console by following the instructions in the *Veritas Cluster Server Installation Guide*. The guide is available in the `cluster_server/docs` directory of the extracted image.
For information on administering clusters using the console, see the *Veritas Cluster Management Console Implementation Guide*.

Software limitations

The following limitations apply to this release.

IIS agent does not detect intentional offline of websites or virtual servers

The IIS agent detects an intentional offline of IIS services. However, the agent does not detect an intentional offline of IIS websites or the FTP, NNTP, and SMTP virtual servers. If you stop a virtual server or a website, the IIS agent interprets the action as a resource fault and triggers a failover. [809217]

If you need to stop the website or virtual server, then you need to stop the corresponding service.

Cluster address for global cluster requires resolved virtual IP

The virtual IP address must have a DNS entry if virtual IP is used for heartbeat agents.

Systems in a cluster must have same system locale setting

VCS does not support clustering of systems with different system locales. All systems in a cluster must be set to the same locale.

Networking agents do not support IPv6 protocol

The bundled networking agents for VCS 5.0 do not support the IPv6 enhanced IP protocol.

Undocumented commands, command options, and libraries

VCS contains undocumented commands and command options intended for development use only. Undocumented commands are not supported.

Known issues

The following issues are open for VCS version 5.0.

Newly-added disk not detected by virtual machine running Windows

When you increase the storage allocated to a virtual machine running Windows, the first rescan of the SCSI adapters inside the virtual machine does not detect the newly-added disk. [898182]

Workaround: The ESX administrator must run the action entry point manually in the ESX cluster. This resets the SCSI ID and the drive letter. When the monitor routine runs again and rescans, it finds the newly-added disk and completes the task of increasing allocated storage.

```
hares -actiooutn ESXVirtualMachineResourceName growfs -  
actionargs SCSI_ID DriveLetter -sys system_name
```

where *system_name* represents the node where the ESXVirtualMachine resource is online.

For example:

```
hares -action ESXVM1_Res growfs -actionargs 0:3 E: -sys node1
```

The GUI may not run the action to increase allocated storage on the correct node

When you use Veritas Virtualization Manager to increase allocated storage, sometimes the GUI picks up the wrong node to fire the growfs action. Due to this, the action does not succeed.

Workaround: The ESX administrator must run the growfs action entry point manually on the ESX cluster. This will ensure that the action is run on the correct ESX node.

```
hares -action <ESXVirtualMachineResourceName> growfs -actionargs  
SCSI_ID MountPoint -sys system_name
```

where *system_name* represents the node where the ESXVirtualMachine resource is online.

For example, for virtual machines running Linux:

```
hares -action ESXVM1_Res growfs -actionargs 0:3 \mnt\app -sys  
node1
```

For example, for virtual machines running Windows:

```
hares -action ESXVM1_Resgrowfs -actionargs 0:3 E: -sys node1
```

Erroneous message in the testVCVconnect utility

The testVCConnect action entry point for the ESXVirtualMachine agent prints the following output when the connection to the VC Server is successfully established:

```
Successfully connected to the VirtualCenter Server
Error: Virtual Machine (/path/filename.vmx) not found in
repository
Successfully Disconnected to the VC Server
```

Workaround: Ignore the message about the virtual machine not being found in the repository. The following string indicates that the attributes are configured properly for the ESXVirtualMachine agent:

```
Successfully connected to the VirtualCenter Server"
```

If any of the attributes are not configured correctly, the output of this action entry point will be a Java trace, similar to:

```
Exception in thread "main" AxisFault
  faultCode: {http://schemas.xmlsoap.org/soap/envelope/
}Server.userException
  faultSubcode:
  faultString: java.net.UnknownHostException:
DR51.enterprise.veritas.com
  faultActor:
  faultNode:
  faultDetail:
...
...
```

Issue with the Browse button in the SQL Agent Configuration wizard

The detailed monitoring page of the SQL Agent configuration wizard has a Browse button to locate *.sql files. The button does not work when you click it the first time. [855817]

Workaround: Click the button twice to browse for *.sql files.

Naming issue with resources of type VMIP

The VMIP resource displays incorrect behavior when the resource name contains a 0 followed by another number. [851277]

Workaround: Rename the VMIP resource such that it does not include a 0 followed by a number.

ESXVirtualMachine agent may not detect virtual machine fault

In some situations, the ESXVirtualMachine agent may not detect the correct status of a faulted virtual machine. For example, the agent may not detect the blue -screen of a virtual machine and may report that the ESXVirtualMachine resource is online. [838275]

Remote failover does not work with auto-generated MAC addresses

If you use auto-generated MAC addresses, switching service groups multiple times may cause the MAC address associated with the virtual machine to change. [850148]

Workaround: Do not use auto-generated MAC addresses. Assign static MAC addresses to virtual machines configured as VCS resources.

Set the MAC address by adding the following line to a virtual machine's configuration file:

```
ethernet0.addressType = "static"  
ethernet0.Address = "00:50:56:XX:YY:ZZ"
```

Make sure you choose hex values that are unique among your hard-coded addresses to prevent conflicts between the automatically assigned MAC addresses and the manually assigned ones.

The values of XX must be between 00 to 3F.

The values of YY and ZZ must be between 00 to FF.

See the VMware documentation for more information.

Virtual machine may remain in a stuck state during boot process

Switching a service group that contains ESX virtual machine resources may not work. [764018]

Workaround: Make sure the vmx config files for the virtual machine have the following entry:

```
uuid.action = "keep"
```

When the virtual machine goes to the stuck state, go to the virtual machine console in the Virtual Infrastructure Client. When prompted to resolve the UUID conflict, choose the Keep Always option.

VCS does not detect Vmotion in a multi-VM environment

VCS does not support the migration of multiple virtual machines that are configured in a single service group. [789348]

Workaround: If you plan to migrate virtual machines, make sure that you configure a service group for each virtual machine.

Localized attributes not supported on Windows virtual machines

This release does not support configuring localized attributes for VCS resources in virtual machines running Windows. [794789]

VSwitch agent does work well with long switch names

The monitor entry point of the VSwitch agent may cause unexpected results when used to monitor switches with long names. [779190]

Misleading error message when running installvcsvm-tools

When you specify a device for the swap and page file location, installvcsvm-tools displays the following error. [896474]

```
No such file or directory
```

Workaround: Ignore the error. The utility completes the configuration successfully.

Saving large configuration results in very large file size for main.cf

If your service groups have a large number resources or resource dependencies, and if the PrintTree attribute is set to 1, saving the configuration may cause cause the configuration file to become excessively large in size and may impact performance. [616818]

Workaround: Disable printing of resource trees in regenerated configuration files by setting the PrintTree attribute to 0.

AutoStart may violate limits and prerequisites load policy

The load failover policy of Service Group Workload Management may be violated during AutoStart when all of the following conditions are met:

- More than one autostart group uses the same Prerequisites.
- One group, G2, is already online on a node outside of VCS control, and the other group, G1, is offline when VCS is started on the node.
- The offline group is probed before the online group is probed.

In this scenario, VCS may choose the node where group G2 is online as the AutoStart node for group G1 even though the Prerequisites load policy for group G1 is not satisfied on that node.

Workaround: Persistently freeze all groups that share the same Prerequisites before using `hastop -force` to stop the cluster or node where any such group is online. This workaround is not required if the cluster or node is stopped without the force option.

Trigger not invoked in REMOTE_BUILD state

In some situations, VCS does not invoke the injeopardy trigger if the system is a REMOTE_BUILD state. VCS fires the trigger when the system goes to the RUNNING state.

Some alert messages do not display correctly

The following alert messages do not display correctly [612268]:

- 51030 Unable to find a suitable remote failover target for global group %s. administrative action is require
- 51031 Unable to automatically fail over global group %s remotely because local cluster does not have Authority for the group.
- 50913 Unable to automatically fail over global group %s remotely because clusters are disconnected and ClusterFailOverPolicy is set to %s. Administrative action is required.
- 50914 Global group %s is unable to failover within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required.
- 50916 Unable to automatically failover global group %s remotely due to inability to communicate with remote clusters. Please check WAN connection and state of wide area connector.
- 50761 Unable to automatically fail over global group %s remotely because ClusterList values for the group differ between the clusters. Administrative action is required.
- 50836 Remote cluster %s has faulted. Administrative action is required.
- 51032 Parallel global group %s faulted on system %s and is unable to failover within cluster %s. However, group is still online/partial on one or more systems in the cluster
- 51033 Global group %s is unable to failover within cluster %s and AutoFailOver is %s. Administrative action is required.

Issues related to the VCS engine

Engine may hang in LEAVING state

When the command `hares -online` is issued for a parent resource when a child resource faults, and the `hares -online` command is followed by the command `hastop -local` on the same node, then the engine transitions to the LEAVING state and hangs.

Workaround: Issue the command `hastop -local -force`.

Timing issues with AutoStart policy

Consider a case where the service group is offline and engine is not running on node 1. If you restart the engine on node 1 after HAD is killed on node 2 *and* before the engine is restarted on node 2, then VCS does not initiate the autostart policy of the group.

Issues related to global service groups

Switch across clusters may cause concurrency violation

If you try to switch a global group across clusters while the group is in the process of switching across systems within the local cluster, then the group may go online on both the local and remote clusters. This issue affects only global groups. Local groups do not experience this behavior.

Workaround: Ensure that the group is not switching locally before attempting to switch the group remotely.

Global service group does not go online on AutoStart node

At cluster startup, if the last system where the global group is probed is not part of the group's AutoStartList, then the group does not AutoStart in the cluster. This issue affects only global groups. Local groups do not display this behavior.

Workaround: Ensure that the last system to join the cluster is a system in the group's AutoStartList.

Declare cluster dialog may not display highest priority cluster as failover target

When a global cluster fault occurs, the Declare Cluster dialog enables you to fail groups over to the local cluster. However, the local cluster may not be the cluster assigned highest priority in the cluster list.

Workaround: To bring a global group online on a remote cluster, do one of the following:

- From the Java Console, right-click the global group in the Cluster Explorer tree or Service Group View, and use the Remote Online operation to bring the group online on a remote cluster.
- From the Web Console, use the Operations links available on the Service Groups page to bring the global group online on a remote cluster.

Issues related to VCS bundled agents

Problem in failing over the IP resource

When a system panics, the IP address remains plumbed to the system for a while. In such a case, VCS may not succeed in failing over the IP resource to another system. This can be observed when a system panics during I/O Fencing.

Workaround: Increase the value of the OnlineRetryLimit attribute for the IP resource type.

Issues related to the Oracle agent

Health check may not work

If you set MonitorOption to 1, health check monitoring may not function when the following message is displayed [589934]:

Warning message - Output after executing Oracle Health Check is:
GIM-00105: Shared memory region is corrupted.

Workaround: Set MonitorOption to 0 to continue monitoring the resource.

Health check does not work in a csh environment

Health check monitoring is not supported for the csh shell.

Issues related to Cluster Management Console

Cluster connector installation requires Symantec Product Authentication Service 4.3.x

You must install cluster connector from a system that has Symantec Product Authentication Service 4.3.x, or at least the authentication broker installed. You can also install cluster connector from a cluster node, provided that you are installing cluster connector on nodes that are part of the same cluster. [611353]

Cluster Management Console controls not immediately active

In some versions of Internet Explorer, you may need to click a GUI control (buttons, drop-down menus, radio buttons, and so on) once before the control becomes active. [603415]

This happens only with flash screens, pop-ups or wizards. Controls that require this activating click show the following message when you roll over them with your mouse pointer:

`Press SpaceBar or Click to activate this Control`

Login screen may not display after inactivity timeout

If your Cluster Management Console is inactive and the session times out, your next action in the console should return you to the login screen. However, if your next action is to request a sort or a new page, the console does not sort the data or load the page.

Workaround: Use the browser refresh feature to display the login screen.

Documentation

Symantec recommends copying installation guides and release notes, from the disc to your system directory `/opt/VRTS/docs` for reference.

VCS 5.0 documentation set

VCS 5.0 includes the following documents.

Title	File Name
<i>Veritas Cluster Server Implementation Guide</i>	<code>vcs_implementation.pdf</code>
<i>Veritas Cluster Server Release Notes</i>	<code>vcs_notes.pdf</code>
<i>Veritas Cluster Server User's Guide</i>	<code>vcs_users.pdf</code>
<i>Veritas Cluster Server Bundled Agents Reference Guide</i>	<code>vcs_bundled_agents.pdf</code>
<i>Veritas Cluster Server Agent Developer's Guide</i>	<code>vcs_agent_dev.pdf</code>
<i>Veritas Cluster Server Agent for EMC MirrorView Installation and Configuration Guide</i>	<code>vcs_mirrorview_install.pdf</code>

Documentation errata: Veritas Cluster Server User's Guide

The accompanying documentation includes information about the following features that are either unsupported or not shipped with this release:

- I/O fencing
- Cluster Manager (Java Console)
- Symantec Product Authentication Service

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to clustering_docs@symantec.com.

Include the title and part number of the document (located in the lower left corner of the title page), and chapter and section titles of the text on which you are reporting.

Third-party legal notices

Certain third-party software may be distributed, embedded, or bundled with this Symantec product, or recommended for use in conjunction with Symantec product installation and operation. Such third-party software is separately licensed by its copyright holder.

For the license agreements that govern the use of third-party software and its copyright holder's proprietary notices, see `vcs_third-party_copyrights.pdf` in the docs directory of the software disc.

Use of the third-party software must be in accordance with its license terms. Symantec makes no representation or warranty of any kind regarding such third-party software. Symantec offers no support for such third-party software and shall have no liability associated with its use.

Getting help

For technical assistance, visit:

http://www.symantec.com/enterprise/support/assistance_care.jsp.

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

