

Veritas™ Cluster Server Release Notes

ESX

5.1

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.

Licensing and registration

Veritas Cluster Server is a licensed product. See the *Veritas Cluster Server Implementation 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) 5.1 for VMware ESX. Review this entire document before installing VCS.

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

<http://entsupport.symantec.com/docs/289940>

Features of Veritas Cluster Server

This release of Veritas Cluster Server offers the following features.

Support for Exchange Server and SAP NetWeaver

This release adds support for Exchange Server and SAP NetWeaver.

See “[Supported applications](#)” on page 10.

Support for virtual machines running Solaris 10 x64 Platform Edition

VCS supports confiding virtual machines running Solaris 10 x64 Platform Edition. This release does not support monitoring applications running inside virtual machines running Solaris 10 x64 Platform Edition.

Support for agents to manage replication

This release of VCS provides the following agents to manage replication:

- Veritas agent for EMC MirrorView
- Veritas agent for Hitachi TrueCopy

Support for monitoring NFS mounts in virtual machines

This release supports monitoring NFS mounts in virtual machines. Configure the Mount agent to monitor NFS mounts.

See the *Veritas Cluster Server Implementation Guide* for more information

Support for virtual machine datastores on NFS

This release supports configuring virtual machine datastores on NFS.

See the *Veritas Cluster Server Implementation Guide* for more information

Support for raw device mapping (RDM)

This release supports virtual machines with RDM disks. Use the Disk agent to configure RDM disks.

See the *Veritas Cluster Server Implementation Guide* for more information

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 shut down opposed to when an application has crashed. The purpose of this feature 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	Apache
Linux	Oracle
	SAP NetWeaver
Virtual machines running	Exchange Server
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.

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.

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.

Cluster Manager (Java Console)

This release includes Cluster Manager (Java Console.) See the *Veritas Cluster Server Implementation Guide* for more information.

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 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.

Requirements for VCS cluster nodes

VMware ESX

VCS supports ESX Server 3.0 and 3.0.1 plus all required VMware ESX patches.

- 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 operating systems in the virtual machines

Table 1-1 lists the architectures and operating systems that VCS for VMware ESX 5.1 supports for guest operating systems.

Table 1-1 Supported operating systems and architectures

Guest operating systems	Kernels	Architectures	File systems/ Volume managers
† Windows 2000 Server or Advanced Server with Service Pack 4	---	x86 (32-bit)	NTFS
† Windows Server 2003: Standard Edition or Enterprise Edition (SP1 required)	---	x86 (32-bit) x86 (64-bit)	NTFS
† Red Hat Enterprise Linux 4 (RHEL 4) Update 3	2.6.9-34.EL 2.6.9-34.smp 2.6.9-34.hugemem	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
† SUSE Linux Enterprise Server 9 (SLES 9) with SP3	2.6.5-7.244 2.6.5-7.244-smp 2.6.5-7.244-bigsm	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
SUSE Linux Enterprise Server 10 (SLES 10) with SP1	2.6.16-37-0.18-smp 2.6.16-37-0.18-bigsm	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
Solaris 10	---	x86	

† 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.

Note: The EMC CLARiiON series and Symmetrix series storage arrays do not support virtual machines running Solaris 10 U1 guest operating systems. See the VMware documentation for more information.

Supported applications

This section lists the applications supported in this release of VCS.

Table 1-2 Supported guest applications

Platform	Applications	Versions
Linux	Apache Web server	1.3, 2.0, and 2.2
“ “	IBM HTTP Server	1.3 and 2.0
“ “	Oracle	10g
“ “	SAP NetWeaver	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
Windows	Exchange	Exchange Server 2003
“ “	IIS	5.0 and 6.0
“ “	SQL	Microsoft SQL Server 2000 Standard Edition or Enterprise Edition (both require SP4) Microsoft SQL Server 2005, 32-bit (SP1 required)

Additionally, VCS provides the following agents to monitor other applications:

- Application agent on virtual machines running Linux
- GenericService agent on virtual machines running Windows

Supported operating systems for increasing allocated storage

VCS supports increasing allocated storage for the following guest operating systems.

Guest operating systems	32-bit	64-bit	Supported file systems
Windows 2000	Yes	No	NTFS
Windows Server 2003	Yes	No	NTFS
RHEL 4 Update 3 (*)	Yes	Yes	ext3
SLES 9 with SP3	Yes	Yes	reiserfs/LVM
SLES 10 with SP1	No	No	N.A.
Solaris 10	N.A.	No	N.A.

Note that file systems on raw device maps (RDMs) do not support the GrowFS feature.

* Supports increasing allocated storage once.

Supported hardware

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

See the documentation published by your array vendor for information about:

- Hardware compatibility with VMware ESX
- Supported microcode or firmware versions
- Supported versions of client software for the array
- Supported versions of the replication and mirroring software
- Recommended array settings

Installation notes

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

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

Merge updated type definitions after upgrade

After upgrading to VCS 5.1, you must merge the type definitions in the types.cf file.

To merge the type definitions

- 1 Stop VCS on the ESX nodes:
`hastop -all -force`
- 2 Merge the new types.cf with the old types.cf. If you have not added any new type definitions to your types.cf, you can replace the old types.cf file with the new one.
The new types.cf file is installed at: /etc/VRTSvcs/conf/default/
The old types.cf file is at: /etc/VRTSvcs/conf/config/
- 3 Start VCS on the node where you updated the types.cf file.:
`hastart`
Do not start VCS on other nodes at this time.
- 4 After VCS goes into running state on that node, start VCS on the other nodes.

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.

Installer does not recognize valid license keys in specific situations

This issue occurs if while installing VCS, you enter an invalid license key and terminate the install program.

If you run the install program again and enter a valid license key, the program prints a message saying the license key is not valid.

This may also occur if you run the installation program after the `/etc/vx` directory was inadvertently erased. [1076425]

Workaround: Uninstall the VRTSvlic package before running the `installvcs` program.

Installer may hang when restarting VMware management service

Because of a VMware ESX issue, the installation program may hang while trying to restart the VMware management service. [1111867]

Workaround: Manually stop and start the management service using the following commands:

```
service mgmt-vmware stop  
service mgmt-vmware start
```

You may need to stop and start the management service on each node during the install process.

Installing VCS with the response file does not work

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

Cannot attach virtual machine console from the VirtualCenter

After installing VCS, you cannot attach the virtual machine console from the VirtualCenter. [1107798]

Workaround: Follow this procedure:

- 1 Edit the file `/etc/vmware/config` file.
- 2 Set the value of `vmauthd.server.alwaysProxy` to `TRUE`.
`vmauthd.server.alwaysProxy=TRUE`
- 3 Reboot the ESX servers.

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. [1081009.]

For more information on obtaining the latest version, visit the VMware website.

Update MonitorTimeout for ESXHost agent

Symantec recommends that you set the MonitorTimeout attribute of the ESXHost resource type to 150 to avoid any monitor timeouts. [1114612]

Software limitations

The following limitations apply to this release.

VCS does not support cold migration of virtual machines

VCS supports migrating virtual machines by using VMotion or by running the `hagrp -migrate` command. VCS provides this support only if the service group configured for the virtual is in an online state. [1108005]

Do not freeze service groups without the evacuate option

Symantec recommends that you do not run either `hasys -freeze` or `hasys -freeze -persistent` commands without the `-evacuate` option to maintain compatibility between VCS and the VMware cluster.

VCS does not support raw devices in DR environments

VCS does not support raw device configurations in disaster-recovery environments.

VCS Replicated Data Clusters

Replicated data clusters are not supported in this release of VCS.

Wizards do not support modifying configurations

Every time you run a VCS configuration wizard on a Windows virtual machine, the process create a new configuration. To preserve your earlier configuration, you must recreate the configuration when running the wizard.

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]

To stop the website or virtual server, you must stop the corresponding service.

Exchange agent does not detect intentional offline of protocol virtual servers

The Exchange Protocol agent detects an intentional offline of protocol services. However, the agent does not detect an intentional offline of protocol virtual servers like the SMTP Virtual Server. If you stop an Exchange protocol server, the Exchange agent interprets the action as a resource fault and triggers a failover. [1052626]

To stop an Exchange protocol virtual server, you must stop the corresponding service.

Limitations related to LVM settings

VCS agents for Hitachi TrueCopy and EMC MirrorView rescan datastores using the following parameters:

- LVM.EnableResignature = 0
- LVM.DisAllowSnapshotLUN = 0

The agents set these values to detect datastores on the disaster recovery site.

The fire drill agents (HTCSnap and MirrorViewSnap) rescan datastores after temporarily setting the following parameters:

- LVM.EnableResignature = 1
- LVM.DisAllowSnapshotLUN = 0.

The agents set these values to detect snapshots that can be used for the fire drill.

These settings impose some limitations on VCS configuration and usage. VMware provides a global setting, which enables rescanning of all LUNs, as against a mechanism that can selectively rescan LUNs. See the VMware documentation for more information on ESX server behavior with these settings.

Remote fire drill limitation

Before running a remote fire drill on the secondary site, make sure that the secondary site does not have any global service groups in the online state. This restriction applies to service groups that may have failed over or switched to the secondary site. If this restriction is not met, running a fire drill may cause undesirable resignaturing of other unrelated datastores.

Local fire drill limitation

Do not run a local fire drill on the secondary site, even if the secondary site has become the new primary site after a failover. If this restriction is not met, running a fire drill may cause undesirable resignaturing of other unrelated datastores.

Run fire drills on dedicated node and make snapshot LUNs visible to only that node

Symantec recommends dedicating one node in the cluster for fire drills. Configure fire drill service groups on this node. Do not configure replication resources (for example HTC or MirrorView) on this node. Configure your array such that snapshot LUNs are visible to this node only; the other nodes must not see snapshot LUNs.

The restriction occurs because other nodes in the cluster may have LVM settings `LVM.EnableResignature = 0` and `LVM.DisAllowSnapshotLUN = 0` set by the replication agents, in which case VMWare recommends that no snapshot LUNs should be exposed to such ESX hosts.

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 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 this release of VCS.

Service group does not come online in some scenarios

This issue occurs if VCS is not running and the ExternalStateChange attribute of the ESXVirtualMachine resource has the OnlineGroup token. If you try to bring the service group online, VCS detects that the ESXVirtualMachine resource is online, but does not bring the service group online. [1110943]

Cannot add ISO image for virtual machines on some platforms

The Veritas Virtualization Manager does not support adding an ISO image for virtual machines on some platforms. On SLES 10 systems, Veritas Virtualization Manager mounts the ISO image meant for SLES 9 systems.

See “[Supported operating systems in the virtual machines](#)” on page 9.

Workaround: Mount the correct ISO image using the VirtualCenter client. The images are available at /vmimages/tools-isomages.

VCS may report incorrect status of applications in some situations

This issue occurs if you attempt to configure a resource after intentionally stopping the corresponding application inside a virtual machine. The issue applies to agents that support detecting intentional offline of applications.

In this scenario, VCS incorrectly reports the status of the application as waiting to go online. [1109924]

Workaround: Flush the service group before attempting to bring it online again.

VCS does not support VMotion if ESX hosts are configured using IP addresses

VCS does not support running the hagr -migrate command to trigger VMotion if you have configured ESX hosts in VMware VirtualCenter using IP addresses instead of fully qualified hostnames. You can run VMotion using the VirtualCenter client. [922540]

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.

Issues related to virtual machines running Windows

Configuration wizards require VCS_HOME to be set correctly

If the VCS_HOME environment variable is not set or is set incorrectly in a Windows virtual machine, the VCS configuration wizards may not work correctly. [1112622]

Workaround: Reboot the virtual machine. If that does not solve the problem, reinstall Veritas Virtual Machine Tools in the Windows virtual machine and reboot the virtual machine.

SQL Configuration wizard requires all SQL Server instances to be running

Before running the SQL configuration wizard, make sure that all SQL instances are running. If all instances are not running, the configuration wizard may not correctly detect one or more instances. [1112400]

Issues related to Veritas Virtualization Manager

Veritas Virtualization Manager does not detect missing ISO files.

If ISO files for the guest virtual machine are missing on host, in some situations, VVM does not detect that the files are missing. [1001263]

Workaround: Restore the missing ISO files from the product media. The ISO files are located at the following path: /cluster_server

/vcsvm_tools directory.

Copy the ISO images to the following directory on the ESX server:

/vmimages/tools-isoimages.

Veritas Virtualization Manager requires Java Access Bridge

Veritas Virtualization Manager displays errors when run on a system that does not have the Java Access Bridge installed. [1087820]

Workaround: Download and install the Java Access Bridge from <http://java.sun.com/products/accessbridge/>

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.

Cannot configure disaster recovery if LUNs are in PSUS state

This issue applies to configurations that use Hitachi TrueCopy for replication.

If you have configured Shadow Image and the LUNs is in the PSUS state, the datastore gets imported on shadow LUNS s and not on the original LUNs.

In this scenario, if you try to configure disaster recovery, Veritas Virtualization Manager displays a message saying the LUNs are not replicated.

Workaround: Follow this procedure:

- 1 Set `/proc/vmware/config/LVM/EnableResignature = 1`.
- 2 Rescan the storage from the Virtual Infrastructure Client.
The datastore gets imported on the LUNS at the primary site.
- 3 Configure disaster recovery using Veritas Virtualization Manager.

Fire drill resource fails due to incorrect pairedisplay output

The fire drill agent uses the pairedisplay output. In some situations, pairedisplay returns an incorrect device file for a LUN. When this occurs, the fire drill resource fails to come online and faults.[1104350]

Workaround: Shut down and restart both the HORCM instances (shadow instances).

When running a fire drill, different virtual machine may boot up

This issue occurs if the configuration has a single datastore that contains multiple virtual machine configuration files.

In this scenario, when running a fire drill, VCS detects an incorrect virtual machine configuration file, which leads to the wrong virtual machine getting booted on the system.

Workaround: Configure the correct CfgFile attribute of the ESXVirtualMachine resource and bring the ESXVirtualMachine resource online manually.

Misleading error message when reversing the direction of replication

This issue occurs if you attempt to reverse the replication direction of arrays from the secondary site in a disaster recovery configuration. In a VCS environment, replicated arrays at the secondary site have read only permissions.

If you do try to reverse the direction of replication, VCS logs the following error:
`There are no replicated LUNS on the clariion array`

Workaround: Ignore the error. Symantec recommends that you do not attempt to reconfigure the arrays or reverse the direction of replication from the secondary site.

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.

Erroneous message in the testVCConnect 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:
...
...
```

Misleading error message when running vcsag_config.pl

When you run the vcsag_config.pl utility to configure an agent, the utility adds a resource of type GuestOSApp to the VCS cluster and waits for the resource to get probed. The utility displays a message saying the resource is not probed. [1112757]

```
ERROR : Resource apache_vm1 is not getting probed on the ESX
cluster. Contact your ESX Server Administrator.
```

Workaround: Ignore the error. To verify that resources have been probed, run the following command:

```
[virtual-machine-prompt]# hares -display apache_vm1 |grep Probed
```

The command returns:

```
apache_vm1 Probed          esxnode1  1
apache_vm1 Probed          esxnode2  1
```

The value 1 indicates that resources have been probed.

Naming issue with VCS resources

In some situations, VCS resources display incorrect behavior when the resource name contains a 0 followed by another number. [851277]

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

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]

Unexpected results 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]

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.

The hagetcf script reports an error

Running the hagetcf script to gather information about the VCS cluster generates the following error:

```
tar: cannot stat ./var/VRTSvcs/log/*.A.log. Not dumped.
```

Workaround: This message may be safely ignored.

Segmentation fault occurs if UTF8 encoding is used

The `halog` command results in a core dump if utf8 encoding is used.

For example, if you issue the command:

```
# $VCS_HOME/bin/halog -add "test debug msg" -dbg 1 -sys -msgid  
10000 -encoding utf8 -parameters "test"
```

The following error occurs:

```
Unknown trailer  
Segmentation fault (core dumped)
```

Make sure you specify the encoding as utf-8.

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 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.

Fixed Issues

The following issues are fixed in this release of VCS.

855817	Issue with the Browse button in the SQL Agent Configuration wizard.
838275	ESXVirtualMachine agent may not detect virtual machine fault
764018	Virtual machine may remain in a stuck state during boot process Switching a service group that contains ESX virtual machine resources may not work.
898182	Newly-added disk not detected by virtual machine running Windows.
793819	GuestOSApp agent may fault during VMotion

Documentation

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

VCS documentation set

VCS 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 Configuration Guide</i>	<code>vcs_mirrorview_config.pdf</code>
<i>Veritas Cluster Server Agent for Hitachi TrueCopy Configuration Guide</i>	<code>vcs_truecopy_config.pdf</code>

The manual pages for `VRTSvcs` are installed in `/opt/VRTS/man`. Manual pages are divided into sections 1, 1m, 3n, and 4. Edit the `man(1)` configuration file `/etc/man.config` to view these pages.

To edit the `man(1)` configuration file

- 1 If you use the `man` command to access manual pages, set `LC_ALL` to "C" in your shell to ensure that the pages are displayed correctly.

```
# export LC_ALL=C
```

 See incident 82099 on the Red Hat Linux support website for more information.

- 2 Add the following line to `/etc/man.config`:

```
MANPATH /opt/VRTS/man
```

 where other man paths are specified in the configuration file.

- 3 Add new section numbers. Change the line:

```
MANSECT      1:8:2:3:4:5:6:7:9:tc1:n:l:p:o
```

 to

```
MANSECT      1:8:2:3:4:5:6:7:9:tc1:n:l:p:o:3n:1m
```

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
- 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.