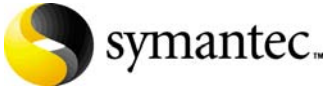
Veritas™ Cluster Server Release Notes

ESX

5.1 Maintenance Pack 2



Veritas Cluster Server
Release Notes

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

Third-party legal notices

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

Technical support

For technical assistance, visit:
http://www.symantec.com/business/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
- Changes in the 5.1 MP1 release
- Features
- Veritas agents
- Requirements
- Installation notes for VCS 5.1
- Software limitations
- Known issues
- Fixed issues
- Documentation
- Third-party legal notices
- Getting help

Introduction

This document provides important information regarding Veritas Cluster Server (VCS) 5.1 MP2 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

Changes in the 5.1 MP2 release

This section lists the changes in this release of VCS.

Support for ESX 3.5

VCS for ESX now supports VMware ESX Server 3.5.

Support for Windows Server 2008

VCS for ESX now supports Microsoft Windows Server 2008 as a guest operating system.

Updated support for EMC SRDF

This release of VCS adds support for the VCS agent for EMC SRDF. For more information, refer to the *Veritas Cluster Server Agent for EMC SRDF Configuration Guide*.

VCS agent support for replicated data clusters in an ESX environment

The following Veritas Cluster Server agents support replicated data clusters in an ESX environment:

- VCS agent for IBM MetroMirror
- VCS agent for EMC MirrorView
- VCS agent for EMC SRDF
- VCS agent for Hitachi TrueCopy

Exchange 2007

VCS for ESX now supports Microsoft Exchange 2007.

VCS Management Console 5.1

A newer version of Veritas Cluster Server (VCS) Management Console is available manage VCS clusters. VCS Management Console was earlier known as Cluster Management Console.

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

For information on updates and patches for VCS Management Console 5.1, see http://entsupport.symantec.com/docs/290657

To download the most current version of VCS Management Console, go to www.symantec.com, browse to the Cluster Server page and click **Utilities**.

Support for iSCSI

VCS for ESX now support iSCSI.

Changes in the 5.1 MP1 release

This section lists the changes in this release of VCS.

Support for IBM Metro Mirror

This release of VCS adds support for the VCS agent for IBM Metro Mirror. For more information, refer to the *Veritas Cluster Server Agent for IBM MetroMirror Configuration Guide*.

Support for EMC SRDF

This release of VCS adds support for EMC SRDF. For more information, refer to the *Veritas Cluster Server Application Note: SRDF replication in a VCS for VMware environment*.

http://entsupport.symantec.com/docs/295185

For updated support for EMC SRDF, see “Updated support for EMC SRDF” on page 6.

Updates to the VMIP agent

The NICConf attribute for the VMIP resource has been added. The attribute helps support configuration of multiple network interfaces using a single resource of type VMIP. The updated attribute type takes the MAC address of the NIC as the key value and the IP address as the data. You can append a non-standard netmask in decimal notation to the IP address with a “:” as separator.

The updated type definition of the VMIP agent follows:

```
    type VMIP (
        static int MonitorInterval = 300
        static str ArgList[] = { "VMwareResName:CfgFile", IPAddress,
        MACAddress, NetMask, Gateway, DNS, NICConf }
        str VMwareResName
        str IPAddress
        str MACAddress
        str NetMask
        str Gateway
        str DNS[]
        str NICConf{}
    )
```

A sample main.cf with the NICConf attribute, and its use follows:

```
VMIP vmIP_rhel4_32bit_vm (
    VMwareResName = esxVM_rhel4_32bit_vm
     IPAddress = "10.100.90.18"
     MACAddress = "00:50:56:94:57:05"
     NetMask = "255.255.248.0"
     Gateway = "10.100.88.1"
     DNS = { "10.100.88.20", "192.168.1.3" }
     NICConf {
     "00:50:56:94:06:5D " = "10.100.90.16:255.255.248.0",
     "00:50:56:94:64:B1" = "192.168.1.18" }
)
```

Changes in the installvcs program with the -configure option

The installvcs program with the -configure option has some modifications in the firewall configuration prompt and the VI3 login credentials prompt.

New attributes IntentionalOffline, ExternalStateChange, and OnlineAtUnfreeze

VCS uses a combination of these three attributes to make sure that the service group does not show a fault. For more information, refer to the *Veritas Cluster Server Implementation Guide*.

Virtual machine display name attribute is mandatory for the migrate and testVCConnect actions

The Vmname attribute for the ESXVirtualMachine resource is mandatory for the migrate and testVCConnect action agent functions for ESXVirtualMachine resources.

Features

Support for monitoring applications in virtual machines

VCS provides agents to monitor the following applications running inside virtual machines.

- Linux: Apache Web server; IBM HTTP Server; Oracle; SAP NetWeaver; WebLogic Server
- Windows: Exchange; Internet Information Services (IIS); SQL; WebSphere Application Server; SharePoint Portal Server

See "Supported applications" on page 16.

Support for virtual machines running Solaris 10 x64 Platform Edition

VCS supports configuring 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.

See "Supported operating systems" on page 14.

Support for agents to manage replication

This release of VCS supports the following replication technologies:

- EMC MirrorView
- EMC SRDF
- Hitachi TrueCopy
- IBM Metro Mirror

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.

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 the VCS 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.

VCS Management Console (formerly the Cluster Management Console)

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

Contact your Symantec sales representative for information about Veritas agents under development, and agents available through Symantec consulting services.

Requirements

System requirements for VCS and VMware ESX Server components follow:

- "VMware ESX Server software and infrastructure" on page 12
- "Patches" on page 13
- "Supported operating systems" on page 14
- "Supported applications" on page 16
- "Support for detecting intentional offline for specific applications" on page 18
- "Supported hardware" on page 18
- "Veritas Cluster Server hardware requirements" on page 19
- "Veritas Cluster Server required disk space" on page 20
- "VMware ESX components and configuration requirements" on page 20

VMware ESX Server software and infrastructure

VCS 5.1 MP2 supports the following:

- ESX Server 3.0.1, 3.0.2, 3.5, 3.5 Update 1, and later
- VirtualCenter Server 2.0, 2.5, and later
- VMotion
- Datastores on VMFS 3 (SAN-attached)
- When you do not have VMotion, you lose the following VMotion actions triggered from VCS:
  - From the command line, you cannot perform the `hagrp -migrate` command
  - From the Veritas Virtualization Manager, you cannot right-click a service group and order it to migrate
  - Other VCS Management interfaces like VCS Cluster Management Console, VCS APIs, etc.
- VCS supports the following VMware infrastructure offerings:
  - Foundation
  - Standard
  - Enterprise

Veritas products will operate on subsequent kernel and patch releases provided the operating systems maintain kernel ABI (application binary interface) compatibility. For the ESX Server in addition to the above kernel ABI information, VCS will operate on subsequent releases provided that the Virtual Infrastructure API and ESX Host CLI compatibility is maintained.

Patches

Review the following patch recommendations, apply the patches where necessary.

Patch for ESX Server 3.0.x when VCS agents hang and return UNKNOWN states

Patches the ESX Server and the VirtualCenter Server for incomplete SOAP messages. This patch fixes situations where VCS agents hang due to monitor timeouts, or start to return UNKNOWN states.

Review the VMware knowledge base article for more information:

http://kb.vmware.com/kb/1002415

Find the patch number from the knowledge base article, and download it from:

http://www.vmware.com/download/vi/vi3_patches.html

Patch for VMware Perl and COM scripting API

On ESX 3.0.x systems that run VCS 5.1 or a subsequent VCS MP release on top of 5.1, ensure that the VMware Perl and COM Scripting API version 2.3.1 (or later) are installed. The ESXVirtualMachine agent requires this patch so that it can correctly determine virtual machine availability.

To download and install the Scripting API patch, refer to VMware documentation for details.

Patch for ESX Server 3.0.1 freezes during rescan operations

Patches the ESX Server hosts to fix a problem where they stop responding during a rescan.

Review the VMware knowledge base articles for more information:

- http://kb.vmware.com/kb/1000039
- http://kb.vmware.com/kb/10229

Update for bind utilities

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 operating systems

Refer to the following information for supported operating systems for VCS for ESX.

- "Supported operating systems in virtual machines for high availability" on page 14
- "Supported operating systems in virtual machines for application monitoring or disaster recovery" on page 14
- "Supported operating systems for increasing allocated storage" on page 16

Supported operating systems in virtual machines for high availability

VCS for ESX provides high availability for all the operating systems that VMware ESX supports as virtual machine guests.

If you need application monitoring or disaster recovery refer to the following section.

Supported operating systems in virtual machines for application monitoring or disaster recovery

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

Table 1-1 Supported operating systems and architectures

Guest operating systems	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 with .NET Framework 2.0 required)	x86 (32-bit) x86 (64-bit)	NTFS
Windows Server 2008: Standard Edition or Enterprise Edition	x86 (32-bit) x86 (64-bit)	NTFS NTFS
*Red Hat Enterprise Linux 4 (RHEL 4) Update 5	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
*SUSE Linux Enterprise Server 9 (SLES 9) with SP4	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM

Table 1-1 Supported operating systems and architectures

Guest operating systems	Architectures	File systems/ Volume managers
SUSE Linux Enterprise Server 10 (SLES 10) with SP1	x86 (32-bit) x86 (64-bit)	ext2, ext3, reiserfs/ LVM
†Solaris 10	x86	

† Does not support application monitoring.

* This version is supported due to a known Linux file system issue. For more information, see "Certain Linux virtual machine file systems can get mounted as "read-only" at virtual machine boot" on page 36.

On Linux-based operating systems: Veritas products will operate on subsequent kernel and patch releases provided the operating systems maintain kernel ABI (application binary interface) compatibility.

On Windows-based operating systems: Veritas products will operate on subsequent service pack (SP) releases provided that the vendor maintains forward compatibility.

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

Supported operating systems for increasing allocated storage

Table 1-2 lists the guest operating systems that VCS supports for increasing allocated storage.

Table 1-2 Supported operating systems for increasing allocated storage

Guest operating systems	32-bit	64-bit	Supported file systems
Windows 2000	Yes	No	NTFS
Windows Server 2003	Yes	No	NTFS
Windows Server 2008	Yes	Yes	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

* Supports increasing allocated storage once.

Note that file systems on raw device maps do not support increasing allocated storage.

Supported applications

VCS provides agents to monitor the following applications that run in virtual machines.

Table 1-3 Supported 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
“ “	WebLogic Server	9.0, 9.1, 9.2, and 10.0

Table 1-3 Supported applications

Platform	Applications	Versions
Windows	Exchange	Exchange Server 2003 Exchange Server 2007 (SP1)
Windows	SharePoint Portal Server	SharePoint Portal Server 2007 High availability is provided to backend SQL database.
" "	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)
" "	WebSphere Application Server	6.0 WebSphere Application Server is configured as a GenericService agent on virtual machines running Windows.

VCS additionally provides the following agents to monitor other applications:

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

Support for detecting intentional offline for specific applications

Certain agents can identify when an application has been intentionally shut down as opposed to when an application has crashed. When VCS detects an intentional offline, VCS does not trigger a failover. This feature allows administrators to manage the applications (start/stop) that run inside the virtual machines without causing additional failovers.

Table 1-4 Agents that support detection of intentional offline of the configured application

Guest operating systems	Applications
Linux	■ Apache ■ Oracle ■ NetIsnr ■ SAP NetWeaver ■ WebLogic Server
Windows	■ Exchange Server ■ Internet Information Services (IIS) ■ SQL Server ■ GenericService ■ WebSphere Application Server

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

Veritas Cluster Server hardware requirements

Make sure that your hardware meets the following requirements.

Table 1-5 Hardware requirements for a cluster

Item	Description
Cluster Server systems	From one to sixteen VMware ESX Servers that run the supported VMware ESX Server operating system version.
DVD drive	One drive in a system that can communicate to all the nodes in the cluster.
Disks	Typical Cluster Server configurations require that shared disks support applications that migrate between systems in the cluster.
Disk space	See Table 1-6, "Disk space requirements and totals."
Network Interface Cards	In addition to the built-in public Network Interface Card (NIC), VCS requires at least one more NIC per system. Symantec recommends two additional NICs.
Fibre Channel or SCSI host bus adapters	Typical VCS configuration requires at least one SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.
RAM	Each VCS system requires at least 256 megabytes in addition to other system and application requirements.

Veritas Cluster Server required disk space

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

Table 1-6 Disk space requirements and totals

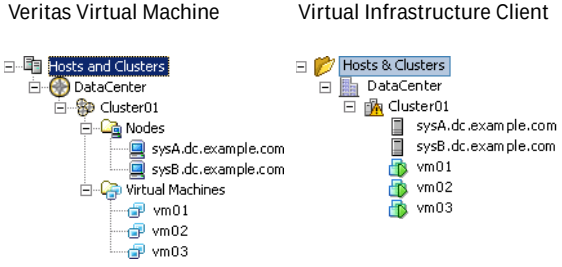
Package	/	/opt	/usr	/var	Totals
Required	5 MB	300 MB	10 MB	5 MB	320 MB
Optional	5 MB	45 MB	0 MB	0 MB	50 MB
Required and optional total	10 MB	345 MB	10 MB	5 MB	370 MB

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

VMware ESX components and configuration requirements

- 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.
- 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.

Figure 1-1 Maintaining an exact correlation between products



Installation notes for VCS 5.1

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 5.1 version of the product.

Merge updated type definitions after upgrade from 5.0 to 5.1

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 Server 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 the 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 while installing VCS, if you enter an invalid license key, and terminate the installation program. If you run the installation 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 Server 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.

Cannot attach the 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.

Software limitations

The following limitations apply to this release.

VCS 5.1 MP1 is incompatible with ESX Server 3.5

Do not install VCS 5.1 MP1 onto ESX Server 3.5. You can install VCS 5.1 MP2 onto ESX Server 3.5.

Do not suspend virtual machines when the virtual machine is a resource in VCS service group

Suspending virtual machines on ESX Nodes that are under active VCS control is not supported. If you want to suspend virtual machines, freeze the VCS service group and suspend. You can unfreeze the service group after you resume the virtual machine.

Windows 64-bit guest operating systems on ESX 3.0 randomly crashes

Windows 64-bit applications that run in ESX 3.0 suffer random crashes. This known VMware issue is addressed in their forums here:

http://communities.vmware.com/thread/75536

Note that if this thread URL changes or is moved, search their community forums for: 32-bit application on 64-bit windows. [1295866]

The rui.crt file has a new location in VirtualCenter 2.0.x and 2.5.x

When you use VirtualCenter 2.0.x and 2.5.x, and if you cannot find the rui.crt file, you may have to look in this directory for it:

```
C:\Documents and Settings\All Users\Application Data\VMware\
VMwareVirtualCenter\SSL\
```

Note that this file is in a hidden folder, and cannot be found using the Windows search. [1157286]

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 systems without the evacuate option

Symantec recommends that you always run the `hasys -freeze` or `hasys -freeze -persistent` commands with the `-evacuate` option. Use the `-evacuate` option to maintain compatibility between VCS and the VMware cluster.

VCS does not support raw devices in disaster recovery environments

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

Application Configuration Wizards on windows virtual machines do not support modifying configurations

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

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

The IIS agent detects an intentional offline of IIS services. The agent, however, 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.

The Exchange agent does not detect intentional offline of protocol virtual servers

The Exchange agent detects an intentional offline of protocol services. The agent does not, however, 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 to stop the corresponding service.

Limitations related to LVM settings

VCS agents for Hitachi TrueCopy, EMC MirrorView, and IBM MetroMirror 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 a virtual IP address 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 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.

Issues related to installing and configuring VCS

ESX local host credentials file may need to be regenerated

The ESXHost agent, the replication agents, and the fire drill agents use the ESX local host credentials file. The ESX local host credentials file is generated by the VCS installer for authentication and is required to use the VMware SDK interface.

If the ESX local host credentials file is accidentally deleted or corrupted, you may need to regenerate this file. [1141366]

Workaround: Before running this command, ensure that you back up the following files:

- `/etc/VRTSvcs/conf/config/main.cf`
- `/etc/VRTSvcs/conf/config/types.cf`

Regenerate the ESX local host credentials file by running the following command at /opt/VRTS/install:

```
# installvcs -configure
```

After running this command, restore the backup files.

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.

Unexpected results with long switch names

The monitor agent function 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.

Version field for VCS VMware ESX license key may be set incorrectly

When the `vxlicrep` command is run, the version field for the Veritas Cluster Server (VCS) for VMware ESX license key may be set to an incorrect value of 7. This issue occurs only with license keys released with the 5.1 version of the VCS for VMware ESX product. [1115392]

Workaround: To determine the actual version of VCS installed on the cluster nodes, type the `had -version` command.

To confirm that the actual version of VCS 5.1 for VMware ESX is installed, verify that the following fields are set to these values.

```
Engine Version    5.1
Join Version      5.1.30.0
Build Date        Thu 03 Jan 2008 07:01:00 PM PST
PSTAMP            Veritas-5.1.30.0-01/03/08-19:01:00
```

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:
...
...
```

Issues related to VCS on the ESX Server

Unable to take virtual machines offline on inaccessible NFS datastores

VCS is unable to bring virtual machines offline on NFS datastores when the NFS server or NFS shares are inaccessible. In this situation VCS can detect the NFS datastore failure, however, the ESXVirtualMachine resource gets stuck in the WAITING TO GO OFFLINE state. [1318097]

Refer to the following TechNote for updates on this issue:

http://entsupport.symantec.com/docs/306520

In a DRS-enabled cluster, VCS migrate moves the virtual machine out of the resource pool

In a DRS-enabled VMware cluster, when VCS migrates the virtual machine from one node to another it moves out of the resource pool that it was associated with. [1361542]

Workaround: Use the Virtual Infrastructure Client to move the virtual machine back to the DRS resource pool that it was associated with.

Agent passwords for attributes cannot contain spaces

VCS does not allow agent passwords that are set up as attributes for the agents in the esxlocalhost credential file to contain spaces. [1369820]

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 Server nodes are configured using IP addresses

VCS does not support running the `hagrp -migrate` command to trigger VMotion if you have configured ESX Server nodes 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.

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 fail over within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required.
50916	Unable to automatically fail over 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 fail over within cluster %s. However, group is still online/partial on one or more systems in the cluster
51033	Global group %s is unable to fail over within cluster %s and AutoFailOver is %s. Administrative action is required.

VCS 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`.

VCS engine 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 disaster recovery

SRDF agent's CompositeGroup attribute value of 1 is not supported

VCS does not support setting the value of the CompositeGroup attribute to 1 for the SRDF agent. [1361469]

DNS entries not getting updated

The VMIP agent updates or replaces the virtual machines existing DNS entries with a new set of values. It cannot be used to add more DNS entries to the virtual machine. [1186611, 1191220]

For example, if a virtual machine has two DNS entries listed in the resolv.conf, but the VMIP agent attribute (*DNS of the exact name) has three listed, the VMIP agent only updates the first two entries listed in the attribute for the virtual machine.

Workaround: If you need VCS to update more DNS entries on the virtual machine, add them in /etc/resolv.conf manually, then they are updated during a failover by the VMIP agent.

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 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.

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.

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 the highest priority cluster as a failover target

When a global cluster fault occurs, the Declare Cluster dialog enables you to fail over groups 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 fire drill

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

This issue occurs if the configuration has a 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.

Firedrill automation works incorrectly when a datastore contains multiple virtual machines

This issue occurs when the firedrill automation incorrectly detects only the first vmx file from the datastore generated as a result of the snapshot. This affects both EMC Mirrorview and Hitachi TrueCopy agents. [1114535]

Workaround: You must manually correct the attribute of the ESXVirtualMachine resource in the configuration file and bring the firedrill service group online.

Issues related to virtual machines running Linux

Application agent cannot monitor kernel processes

The Application agent cannot monitor processes that have wildcard characters that give a special meaning to the grep command. This issue applies to the Application agent installed inside of all Linux virtual machines as well as the ESX Servers. [1364107]

Certain Linux virtual machine file systems can get mounted as “read-only” at virtual machine boot

Certain Linux operating systems can become read-only due to a kernel flaw. Refer to the VMware knowledge base article for more information. VCS system requirements now support Linux operating systems that do not have this issue.

http://kb.vmware.com/kb/51306

Gateway attribute does not get updated on certain rhel4 virtual machines

The VMIP agent is not able to update the default gateway of certain virtual machines running RedHat Linux on a VCS disaster recovery failover. [1191220]

Workaround: To ensure that the VMIP agent is able to correctly update the gateway, make sure that the gateway setting is updated inside the /etc/sysconfig/network file, instead of the individual /etc/sysconfig/network-scripts/ifcfg-eth* files.

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.

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.

Oracle agent health check may not work

If you set the MonitorOption attribute 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 the value of the MonitorOption attribute to 0 to continue monitoring the resource.

Oracle agent health check does not work in a csh environment

Health check monitoring is not supported for the csh shell.

Issues related to virtual machines running Windows

The IIS agent does not work in Windows 2000 virtual machines

This 5.1 MP2 issue is due to a new set of WMI APIs that are unsupported on Windows 2000, the IIS agent does not work in Windows 2000. [1369144]

Refer to this Late Breaking News URL for updates on this issue:

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

The IIS configuration wizard does not throw an error when the DefaultAppPool service is stopped

If IIS is configured and the “root” Application Pool service is stopped, the Web resource does not come online. The IIS configuration wizard does not notify you that the service is stopped during configuration of the IIS resource. [1270357]

Workaround: If the resource that is being configured is for a Web site and the value of the AppPoolMon setting is DEFAULT/ALL, then make sure the "root" application pool is running.

The IIS agent configured with IIS bound to an IP address requires manual intervention on disaster recovery failover

The Windows IIS agent takes in an IP address as an attribute if the iis-webserver is bound to only a single IP on the node. When a disaster recovery failover event occurs, however, the IP address of the VM changes. [1071149]

Workaround: After a disaster recovery failover of a Windows virtual machine with IIS setup for VCS monitoring, reconfigure the IIS resource. Log into the virtual machine and run the IIS configuration wizard. When the wizard prompts you to select the Web sites, chose the Web sites that you want to monitor, and enter the newer IP addresses that correspond to each Web site for this particular disaster recovery site.

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]

The SQL Wizard sets the default instance name to the computer name when configuring SQL 2000 on Win 2000

When running the SQL Configuration wizard on Windows 2000 SP4 to configure the default instance of SQL 2000, the instance name gets set to the computer name.

This causes the agent to not be able to find the service and the resource remains in an UNKNOWN state. The instance name attribute for the default instance should be NULL. Manually making the change and restarting the vcsagmd service fixes the issue. [1190750]

Workaround: Locate the main.cmd file and the .SQLServer2000.main.cmd file at: %VCS_HOME%\conf\config. Type `set vcs_home` at the command prompt to find the value of %VCS_HOME%. For example:

```
C:\Documents and Settings\Administrator>set vcs_home
    VCS_HOME=C:\Program Files\Veritas\cluster server
```

The main.cmd file contains configuration information for agents. If SQL Server 2000 default instance on Windows 2000 is configured, find an entry similar to:

```
"modifyres SQLServer2000 MSSQLSERVER_SQLServer2000_SQL Instance str
hostName".
```

Remove hostname from last statement, the new statement is:

```
"modifyres SQLServer2000 MSSQLSERVER_SQLServer2000_SQL Instance
str"
```

Make sure there is no other change to this file. Save and close this file.

Re-start the vcsagmd service in the service control manager.

Windows 64-bit guest operating systems path redirection for VMIP and GrowFS agents

On Windows 2003 server 64-bit guest operating systems access to system commands is redirected from system32 to sysWOW64 for the VMIP and GrowFS agent for all 32-bit applications. [1186533]

Workaround 1: A Microsoft workaround is KB942589. Find it and an associated hotfix here: http://support.microsoft.com/kb/942589. The hotfix creates a NTFS junction from %SYSTEMROOT%\Sysnative to %SYSTEMROOT%\system32.

Workaround 2: In case the hotfix is not available, use the junction utility (available at http://www.microsoft.com/technet/sysinternals/FileAndDisk/Junction.mspx). Execute the following command after installing junction.exe inside of the guest operating system's file system:

install_path\junction.exe %SYSTEMROOT%\Sysnative %SYSTEMROOT%\system32

The monitor.pl entry points of the VMIP and the GrowFS agent for Windows guest OS will check the alternative Sysnative path for missing commands.

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.

The diskpart.exe and shutdown.exe files are not available on the base installation of Windows 2000

The absence of these binaries may cause problems for GrowFS and VMIP. [1188035]

Workaround: For diskpart.exe, you can use a Microsoft provided Resource Kit extension that the agent uses if installed in the default location:

"C:\PROGRA~[0-9]\RESOUR~[0-9]\diskpart.exe".

No workaround exists for shutdown.exe currently.

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]

Issues related to Veritas Virtualization Manager (VVM)

Veritas Virtualization Manager (VVM) can hang if left idle for long amounts of time

If you leave VVM idle and open for long amounts of time, it can hang. If it hangs, close the application and re-open it. [1367745]

VVM does not configure disaster recovery for virtual machines already configured for high availability

If a virtual machine is configured for HA, VVM does not configure disaster recovery. It displays a message that the virtual machine is already configured for high availability.

Workaround: Delete the existing service group and then configure for disaster recovery. [1190226]

VVM 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.

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/

Cannot add ISO image for virtual machines on some platforms

The Veritas Virtualization Manager does not support adding an ISO image on Windows 2000 32-bit virtual machines. [1283240]

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

Issues related to VCS Management Console

Replication information on the IBM MetroMirror agent does not appear in the VCS Management Console UI

Information on the IBM MetroMirror agent replication does not appear in the VCS Management Console 5.1 user interface. Use the VCS management console to manage an IBM MetroMirror resource. You may not get additional information regarding the state and details of replication in the user interface. [1171325] [1187155]

Fixed issues

The following section discusses fixed known issues in VCS 5.1 MP2 and in previous releases.

Issues fixed in VCS 5.1 MP2

The following issues are fixed in this release of VCS.

1265876	ESX concurrency violation trigger fails to take the virtual machine service group offline on the correct VCS node.
1193310	RemoteGroup Resource is unable to go offline.
1185584	The Veritas Virtualization Manager now supports adding an ISO image for virtual machines on SLES 9 and SLES 10 platforms.
1130788	Fixed an issue where installing VCS (installvcs) with the response file failed.
1110943	Fixed an ExternalStateChange attribute issue where a service group did not come ONLINE.

Issues fixed in VCS 5.1 MP1

The following issues are fixed in this release of VCS.

1123062	Online timeout of one VMIP resource when multiple VMIPs are configured on a single VM. See “Changes in the 5.1 MP1 release” on page 7.
1119239	VMIP guest operating system agent fails to configure VMIP correctly on SLES VM
1114612	Intermittent error messages thrown by the ESXHost agent
1104350	Fire drill resource fails due to incorrect pairdisplay output
612587	The haclus -wait command hangs when cluster name is not specified.

Issues fixed in VCS 5.1

The following issues were fixed in VCS 5.1.

898182	Newly-added disk not detected by virtual machine running Windows.
855817	Issue with the Browse button in the SQL Agent Configuration wizard.
838275	ESXVirtualMachine agent may not detect virtual machine fault
793819	GuestOSApp agent may fault during VMotion
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.

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
Veritas Cluster Server Implementation Guide	`vcs_implementation.pdf`
Veritas Cluster Server Release Notes	`vcs_notes.pdf`
Veritas Cluster Server User's Guide	`vcs_users.pdf`
Veritas Cluster Server Bundled Agents Reference Guide	`vcs_bundled_agents.pdf`
Veritas Cluster Server Agent Developer's Guide	`vcs_agent_dev.pdf`
Veritas Cluster Server Agent for EMC MirrorView Configuration Guide	`vcs_mirrorview_config.pdf`
Veritas Cluster Server Agent for Hitachi TrueCopy Configuration Guide	`vcs_truecopy_config.pdf`
Veritas Cluster Server Agent for IBM MetroMirror Configuration Guide	`vcs_metromirror_config.pdf`
Veritas Cluster Server Agent for EMC SRDF Configuration Guide	`vcs_srdf_config.pdf`
Veritas Cluster Server Application Note: SRDF replication in a VCS for VMware environment	http://entsupport.symantec.com/docs/295185

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
- Manual failover in a campus cluster
- The disaster recovery Preswitch check

Documentation addendum

Veritas Cluster Server User's Guide, host monitoring daemon

This section of the addendum covers host monitoring additions in several different chapters in the *Veritas Cluster Server User's Guide*.

About cluster control, communications, and membership in chapter, "Introducing Veritas Cluster Server"

This section follows the "About the high-availability daemon (HAD)" section on page 27.

VCS also starts HostMonitor daemon when the VCS engine comes up. The VCS engine creates a VCS resource VCShm of type HostMonitor and a VCShmg service group. The VCS engine does not add these objects to the main.cf file. Do not modify or delete these components of VCS. VCS uses the HostMonitor daemon to monitor the resource utilization of CPU and Swap. VCS reports to the engine log if the resources cross the threshold limits that are defined for the resources.

About VCS keywords and reserved words in chapter, "VCS configuration concepts"

Add HostMonitor to the list on page 55.

System attributes in appendix, “VCS attributes”

Add the HostMonitor attribute to the table that starts on page 625.

System attribute name: HostMonitor (system use only)

Definition: List of host resources that the HostMonitor daemon monitors.

- Type and dimension: string-keylist
- Default: { CPU, Swap }

Veritas Cluster Server User’s Guide: encrypting agent passwords and the use of security keys

This section of the addendum replaces one section that deals specifically with encrypting agent passwords. It adds information about encrypting agent passwords with security keys.

Encrypting agent passwords in chapter, “Administering the cluster from the command line”

This addendum section replaces the encrypting passwords section, and adds to the section that starts on page 234 of the User’s Guide.

Use the `vcsencrypt` utility to encrypt passwords when editing the VCS configuration file main.cf when configuring agents that require user passwords.

Note: Do not use the `vcsencrypt` utility when entering passwords from a configuration wizard or from the Java and Web consoles.

To encrypt an agent password

1. Run the utility from the command line.

   ```
   vcsencrypt -agent
   ```

2. The utility prompts you to enter the password twice. Enter the password and press Return.

   ```
   Enter New Password:
   Enter Again:
   ```

3. The utility encrypts the password and displays the encrypted password. Use the displayed password to edit the VCS configuration file main.cf.

Encrypting agent passwords using security keys in chapter, “Administering the cluster from the command line”

The following sections are in addition to the previous section. All of these sections appear in the, “Administering the cluster from the command line” chapter of the *Veritas Cluster Server User’s Guide*.

Use the vcsencrypt utility to generate a security key to create a more secure passwords for agents.

Privilege requirements generating security keys

By default, only superusers can generate security keys.

You can grant password encryption privileges to group administrators.

Creating secure agent passwords

Follow these instructions to create secure passwords for agents.

To encrypt agent passwords using security keys

1. Make sure you have the privileges required to encrypt passwords.
2. Generate a security key from a node where VCS is running. You need to do this once.
   - Make the VCS configuration writable.
     ```
     haconf -makerw
     ```
   - Run the vcsencrypt utility:
     ```
     vcsencrypt -gensecinfo
     ```
   - When prompted, enter a password and press Return.
     ```
     Please enter a passphrase of minimum 8 characters.
     Passphrase:
     Generating SecInfo...please wait...
     SecInfo generated successfully.
     SecInfo updated successfully.
     ```
   - Save the VCS configuration file.
     ```
     haconf -dump
     ```
3. Encrypt the agent password with the security key that you generated.
   - On a node where VCS is running, enter the following command:
     ```
     vcsencrypt -agent -secinfo
     ```
   - When prompted, enter a password and press Return. The utility prompts you to enter the password twice.
     ```
     Enter New Password:
     Enter Again:
     ```
     The utility encrypts the password and displays the encrypted password.

4 Verify that VCS uses the new encryption mechanism.

- Verify that the SecInfo cluster attribute is added to the main.cf file with the security key as the value of the attribute.
- Verify that the password that you encrypted resembles the following:

```
SApswd=7c:a7:4d:75:78:86:07:5a:de:9d:7a:9a:8c:6e:53:c6
```

Granting password encryption privileges to group administrators

Follow these instructions to grant password encryption privileges to group administrators.

To grant password encryption privileges to group administrators

- Set the value of the cluster attribute SecInfoLevel to R+A:

```
haclus -modify SecInfoLevel R+A
```

To restrict password encryption privileges to superusers

- Set the value of the cluster attribute SecInfoLevel to R:

```
haclus -modify SecInfoLevel R
```

Changing the security key

Follow these instructions to change the security key.

If you change the security key, make sure you reencrypt all the passwords that you created with the new security key. Otherwise, agents will fail to decrypt the encrypted password correctly and hence manage to monitor resources correctly.

To change security key

1 Save the VCS configuration and make it writeable.

```
haconf -makerw
```

2 Run the following command:

```
vcsencrypt -gensecinfo -force
```

3 Save the VCS configuration and make it read only.

```
haconf -dump -makero
```

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/business/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.