Veritas™ Cluster Server Release Notes

HP-UX 11i v3

5.0.1

symantec™

Veritas Cluster Server Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: VCS 5.0.1

Document version: 5.0.1.0

Legal Notice

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/assistance_care.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level

- Network topology

- Router, gateway, and IP address information

- Problem description:

  - Error messages and log files

  - Troubleshooting that was performed before contacting Symantec

  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization

- Product registration updates, such as address or name changes

- General product information (features, language availability, local dealers)

- Latest information about product updates and upgrades

- Information about upgrade assurance and maintenance contracts

- Information about the Symantec Buying Programs

- Advice about Symantec's technical support options

- Nontechnical presales questions

- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Release Notes

This document includes the following topics:

- Introduction
- About Veritas Cluster Server
- Changes introduced in VCS 5.0.1 for HP-UX 11i v3
- Changes introduced in VCS 5.0 for HP-UX 11i v3
- Features introduced in VCS 5.0
- VCS system requirements
- No longer supported
- Fixed issues
- Known issues
- Software limitations
- VCS documentation

Introduction

This document provides important information about Veritas Cluster Server (VCS) version 5.0.1 for HP-UX 11i v3. Review this entire document before you install or upgrade VCS.

The information in the Release Notes supersedes the information provided in the product documents for VCS.

For the latest information on updates, patches, and software issues for this release, use the following TechNote on the Symantec Enterprise Support website:

http://entsupport.symantec.com/docs/331560

You can download the latest version of *Veritas Cluster Server Release Notes* from the link that is provided in the TechNote.

About Veritas Cluster Server

Veritas™ Cluster Server by Symantec (VCS) is a clustering solution that eliminates downtime, facilitates server consolidation and failover, and effectively manages a wide range of applications in heterogeneous environments.

About VCS agents

VCS bundles agents to manage a cluster's key resources. The implementation and configuration of bundled agents vary by platform.

For more information about bundled agents, refer to the *Veritas Cluster Server Bundled Agents Reference Guide*.

The Veritas High Availability Agent Pack gives you access to agents that provide high availability for third-party storage solutions. Contact your Symantec sales representative for information about agents included in the agent pack, agents under development, and agents that are available through Symantec consulting services.

VCS provides a framework that allows for the creation of custom agents. Create agents in situations where the Veritas High Availability Agent Pack, the bundled agents, or the agents for enterprise applications do not meet your needs. You can also request a custom agent through Symantec consulting services.

For more information about the creation of custom agents, refer to the *Veritas Cluster Server Agent Developer's Guide*.

VCS also provides agents to manage key enterprise applications. Before configuring an enterprise agent with VCS, verify that you have a supported version of the agent.

See "Supported VCS agents" on page 27.

About compiling custom agents

Custom agents must be developed using compilers from one of the products listed below:

■ HP C/ANSI C Developer's Bundle (S800), part number B3901BA.

■ HP aC++ Compiler (S800), part number B3913DB.

These products may be identified by various part numbers in addition to those listed.

Existing custom agents written to run on VCS versions earlier than 1.2 must be recompiled for use with VCS 5.0.

Changes introduced in VCS 5.0.1 for HP-UX 11i v3

This section lists the changes in the VCS 5.0.1 for HP-UX 11i v3 release.

Support for HP-UX Integrity Virtual Machines

Use Veritas Cluster Server (VCS) to ensure high availability for HP-UX Integrity Virtual Machines (HPVM). Use VCS to monitor HPVMs, their storage, and switches. If any component (resource) goes down, VCS can move the HPVM, and all its dependent resources to a running node.

See the *Veritas Storage Foundation™ and High Availability Solutions Application Note: Support for HP-UX Integrity Virtual Machines*, which is available at

http://entsupport.symantec.com/docs/332614.

Changes to Cluster Management Console 5.0

VCS 5.0.1 has the following changes for Cluster Management Console 5.0:

■ If you perform a fresh VCS 5.0.1 installation, the installer installs the Cluster Management Console 5.0 cluster connector and single cluster management console components as part of the optional VCS depots. However, the installer does not provide an option to configure these components.
  If you already have a management server of Cluster Management Console 5.0, you can use direct connection to manage the newly configured VCS 5.0.1 cluster. Symantec recommends that you install and configure the latest version 5.1 of VCS Management Console.
  See

■ If you upgrade VCS to 5.0.1 and if you used Cluster Management Console 5.0 to manage the cluster, you may continue to use it with VCS 5.0.1.

VCS Management Console 5.1

The installation media for this release also offers Veritas Cluster Server (VCS) Management Console 5.1. VCS Management Console was earlier known as Cluster Management Console.

VCS Management Console 5.1 can manage VCS 5.0.1 clusters using direct connection. You can also install the cluster connector for VCS Management Console 5.1 on the VCS 5.0.1 clusters.

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/business/cluster-server and click **Utilities**.

Changes to bundled agents

VCS 5.0.1 introduces the following new agents:

- DiskGroupSnap—Verifies the configuration and data integrity in a campus cluster environment.

- VCS 5.0.1 includes the following new bundled agents for Samba.

    - SambaServer agent—Monitors the smbd process.

    - SambaShare agent—Use to make a Samba Share highly available or to monitor it.

    - NetBIOS agent—Use to make the nmbd process highly available or to monitor it.

- HPVirtualMachine agent—Starts, stops and monitors virtual machines that are configured on the HPVM server.

- HPVSwitch agent—Monitors a virtual switch on an HPVM Server.

See "No longer supported" on page 27.

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

Change in behavior: DiskGroup agent

If you set the value of the PanicSystemOnDGLoss attribute to 1, VCS panics the system when the disk group becomes unavailable irrespective of whether you use I/O fencing.

See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information.

DNS agent supports A, AAAA records with corresponding PTR records

The DNS agent supports A and AAAA records. To accommodate this, and improve the agent, the HostName and Alias attributes have been replaced with the ResRecord attribute.

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

Changes to VCS agent for Oracle

The Veritas Cluster Server agent for Oracle includes the following new or enhanced features:

- Support for Oracle 11g
  See "Supported VCS agents" on page 27.

- Support for Oracle ASM

- Support to detect intentional offline

- Support to choose CUSTOM as one of the start up options when you use Hot backup feature of Oracle

- Support for csh and tcsh shell when Health check monitoring is enabled

- Support for a new action entry point pfile.vfd

See the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide* for more information.

Change in the upgrade procedure

The minimum downtime upgrade procedure has been revised and the new procedure is termed as phased upgrade. For more information, refer to the *Veritas Cluster Server Installation Guide*.

Change in attributes

This release has the following changes for VCS attributes:

- AYATimeout - VCS heartbeat attribute
  The default value of the heartbeat attribute AYATimeout is changed from 300 seconds to 30 seconds.

- Preonline - VCS service group attribute
  You can now localize the Preonline attribute for the nodes in a cluster.

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

New attributes

This release introduces the following new system attributes:

- HostMonitor—Monitors the usage of resources on the host.

- HostUtilization—Indicates the usage percentages of resources on the host.

This release introduces the following new service group attributes:

- PreSwitch—Indicates whether the VCS engine should switch a service group in response to a manual group switch.

- PreSwitching—Indicates that the VCS engine invoked the PreSwitch action function for the agent; however, the action function is not yet complete.

This release introduces the following new resource type level attribute:

- OfflineWaitLimit—Indicates the number of monitor intervals to wait for the resource to go offline after completing the offline procedure. Increase the value of this attribute if the resource is likely to take a longer time to go offline.

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

VCS agent for DB2 supports DB2 9.5

The Veritas Cluster Server Agent for DB2 supports DB2 9.5.

See "Supported VCS agents" on page 27.

See the *Veritas Cluster Server Agent for DB2 Installation and Configuration Guide* for more information.

Enhancements to VCS campus clusters

VCS 5.0.1 includes the following enhancements to campus cluster configurations:

- Support for campus clusters using VxVM remote mirror configuration
  In a campus cluster setup, you can configure VxVM diskgroups for remote mirroring.

- Support for fire drill in campus clusters using the DiskGroupSnap agent
  A fire drill tests the disaster-readiness of a configuration by mimicking a failover without stopping the application and disrupting user access.
  The DiskGroupSnap agent is used to perform the fire drill in campus clusters. You can bring online, take offline, and monitor the fire drill versions of disk groups for testing.
  You can configure this agent to either use the disks at the secondary site (Bronze configuration) or use the disks configured on a dummy site at the

secondary site (Gold configuration). Symantec recommends that you use the Gold configuration for the DiskGroupSnap resource.
See "Limitations with DiskGroupSnap agent" on page 58.

■ Support for manual failover of service groups across system zones in campus clusters
The AutoFailOver attribute controls the service group behavior in response to service group and system faults. For campus clusters, you can set the value of the AutoFailOver attribute as 2 to manually fail over the service group across the system zones that you defined in the SystemZones attribute.
The manual failover functionality requires that you enable the HA/DR license and that the service group is a non-hybrid service group.

See the *Veritas Cluster Server User's Guide* and the *Veritas Cluster Server Bundled Agents Reference Guide* for more information.

Support for VxFS file system lock

If the VxFS file system has "mntlock=key" in its mount options, then you cannot unmount the file system without specifying the key. This prevents accidental unmounts when a resource is online.

See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information.

Support for intentional offline

Certain VCS agents can identify when an application has been intentionally shut down outside of VCS control. If an administrator intentionally shuts down an application outside of VCS control, VCS does not treat it as a fault. VCS sets the service group state as offline or partial, depending on the state of other resources in the service group. This feature allows administrators to stop applications without causing a failover. The intentional offline feature is available for agents registered as V5.1 or later.

See the *Veritas Cluster Server Agent Developer's Guide* for information on agents that support this feature.

VCS process to monitor utilization of CPU and Swap

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.

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

Multi-tiered application support using the RemoteGroup agent for global groups

VCS supports the RemoteGroup agent when it points to a global group. The RemoteGroup agent must map the state of the global group in the local cluster.

See the *Veritas Cluster Server User's Guide* for more information on the functionality of this agent.

LLT supports point-to-point unicast heartbeating mechanism

The default heartbeating mechanism in LLT is now point-to-point unicast and not broadcast heartbeating.

Enhanced encryption mechanism for agent passwords

The vcsencrypt utility now supports stronger encryption mechanism for agent passwords. Use the vcsencrypt utility to generate a security key that you can use to create a more secure password for the agent.

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

VCS documentation is available on the software disc

The VCS documentation package (VRTSvcsdc) is deprecated. The software disc contains the documentation for VCS in Portable Document Format (PDF) in the cluster_server/docs directory.

Symantec recommends copying pertinent documents from the disc to your system directory /opt/VRTS/docs for reference.

Changes introduced in VCS 5.0 for HP-UX 11i v3

This section lists the changes in the VCS 5.0 for HP-UX 11i v3 release.

Host and node name expansion on HP-UX

The HP-UX Node and Host Name Expansion feature is supported on Symantec products.

You must enable a dynamic kernel tunable parameter, expanded_node_host_names, using the following kctune command to allow the use of larger names on the system:

```
# /usr/sbin/kctune expanded_node_host_names=1
```

Reboot the node after executing this command.

Change in stack size for VCS agents

On HP-UX PA-RISC systems, the default stack size for threads is 64K. This stack size is not sufficient for VCS agents. To increase the stack size, an environment variable, PTHREAD_DEFAULT_STACK_SIZE, is set to 512K in the file /opt/VRTSvcs/bin/vcsenv.

This environment variable must not be modified. Reducing the value of this variable can cause SIGBUS error in VCS agents.

VCS FEN messages are now VxFEN messages

Error messages that are related to the fencing module, VCS FEN, are now read as VxFEN.

Change in string size for some attribute values

For group name, resource name, attribute name, type name, and VCS username and password, the string size is limited to 1024 characters.

Campus cluster support

You can configure a campus cluster using functionality provided by Veritas Volume Manager.

To set up a campus cluster, make sure the disk group contains mirrored volumes. The mirrors must be on separate storage at different sites. Use site tags to distinguish between mirrors located at different sites. You could also use enclosure-based naming.

See the *Veritas Volume Manager Administrator's Guide* for detailed instructions.

Symantec recommends using I/O fencing in campus clusters.

Change in behavior: hastop command

VCS ignores the value of the cluster-level attribute EngineShutdown while the system is shutting down.

Change in behavior: BrokerIP attribute of the RemoteGroup agent

The BrokerIP attribute now requires only the IP address. Do not include the port number when you configure the attribute. [789878]

For a secure remote cluster only, if you need the RemoteGroup agent to communicate to a specific authentication broker, then set this attribute.

Type: string-scalar

Example: "128.11.245.51"

Fire drill support in Veritas Cluster Management Console

Veritas Cluster Management Console adds support for fire drills. The console lets you run fire drills and displays the status of the last fire drill.

- Viewing the status of the last fire drill—The service group listing tables display a column for the Physical Fire Drill Status, which indicates the results of the last fire drill.

- Running a fire drill.

    - Verify that replication for an application is working correctly.

    - Verify that a secondary disaster recovery (DR) application service group can be brought online successfully.

- Viewing fire drill logs—If a service group is configured with a physical fire drill group, a tab labelled Fire Drill Logs appears on the secondary tab bar in the Group:Summary view. Click this tab to view the VCS log messages about the fire drill group on the remote cluster and the resources that belong to it.

See the *Veritas Cluster Server User's Guide* for information about fire drills.

Viewing the status of the last fire drill

The column Fire Drill Status has been added to service group listing tables. A service group listing table is on the Cluster:Groups view.

For VCS global service groups that are configured with a fire drill group, this column indicates the results of the most recently run fire drill. The following are the possible states:

unknown	No fire drill has been run or the Cluster Management Console has come online after the most recent fire drill
running	Fire drill in progress
passed	Fire drill group came online on the secondary cluster
failed	Fire drill group did not come online on the secondary cluster

If multiple management servers are connected to the global cluster that contains the primary global group, the table does not show fire drill status for that group.

Running a fire drill

The Cluster Management Console supports fire drills in multi-cluster mode only. Before you run a fire drill, you must do the following:

■ Configure the local (primary) and remote (secondary) global groups

■ Set up the replication for the storage at the primary and secondary sites

■ Configure the fire drill group using the FDSETUP command line wizard.

To run a fire drill from the Cluster Management Console

1   On the navigation bar, click **Home**.

2   On the secondary tab bar, click **Clusters**.

3   In the Home:Clusters view, in the Clusters Listing table, click the name of the primary global cluster.

4   On the secondary tab bar, click **Groups**.

5   In the Cluster:Groups view, in the Groups Listing table, click the name of the primary global group.

6   In the Group:Summary view, in the Remote Operations task panel, click **Run fire drill**.

    You can view results of the fire drill in the Cluster:Groups view, the Group:Summary view, and in the Group:Fire Drill Logs view.

Viewing fire drill logs

Running a fire drill creates fire drill logs. If a service group is configured with a fire drill group, a tab labeled Fire Drill Logs appears on the secondary tab bar in the Group:Summary view.

To view fire drill logs

1   On the navigation bar, click **Home**.

2   On the secondary tab bar, click **Clusters**.

3   In the Home:Clusters view, in the Clusters Listing table, click the name of a VCS global cluster.

    The global cluster must contain a global service group (primary group) that is configured with a fire drill group at a secondary location.

4   On the secondary tab bar, click **Groups**.

5   In the Cluster:Groups view, in the Groups Listing table, click the name of the primary global group.

6   In the Group:Summary view, on the secondary tab bar, click **Fire Drill Logs**.

This tab contains VCS log messages about the fire drill group on the remote (secondary) cluster and the resources that belong to it.

Features introduced in VCS 5.0

This section lists the features introduced in the VCS 5.0 release.

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

Cluster Management Console

The new Cluster Management Console replaces Cluster Manager (Web Console) and CommandCentral Availability.

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 stand-alone system to manage multiple clusters or you can install the console on cluster nodes to manage a local cluster. When installed to manage a local cluster, the console is configured as part of the ClusterService group and the AppName attribute is set to cmc.

See

Cluster Monitor is now called Cluster Connector

CommandCentral Availability installed a component called Cluster Monitor on cluster nodes. The updated component is called Cluster Connector.

VCS privileges for operating system user groups

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

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

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

Five levels of service group dependencies

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

New RemoteGroup agent to monitor service groups in remote clusters

The new RemoteGroup agent monitors and manages service groups in a remote cluster. See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information about the agent.

Enhancements to the hastop command

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

Table 1-1 lists the EngineShutdown attribute's values and description.

Table 1-1   EngineShutdown attribute values

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

Simulator supports deleting simulated clusters

VCS Simulator now supports deleting simulated clusters.

Symantec recommends using the same tool (command line or Java Console) to create and delete a cluster. For example, if you created the cluster from the Java Console, delete the cluster from the Java Console.

I/O fencing updates: DMP support

Dynamic multi-pathing (DMP) allows coordinator disks to take advantage of the path failover and the dynamic adding and removal capabilities of DMP. You can configure coordinator disks to use Veritas Volume Manager DMP feature.

You can set the coordinator disks to use DMP as the hardware path to a drive.

See the *Veritas Cluster Server Installation Guide* for more information.

Minimal downtime upgrade to VCS 5.0

See the *Veritas Cluster Server Installation Guide* for a strategy on upgrading to VCS 5.0 while ensuring a minimal downtime for your applications.

Backup of VCS configuration files

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

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

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

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

CPU binding

In certain situations, the HP-UX operating system may assign the CPU to high priority interrupts or processes like HAD. To overcome this issue, VCS provide the option of running HAD on a specific processor. This way you can shield HAD from other high priority processes.

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

HAD diagnostics

When the VCS engine HAD dumps core, the core is written to the directory /var/VRTSvcs/diag/had, where the diagnostic information is stored. When HAD and GAB encounter heartbeat problems, VCS runs the script /opt/VRTSvcs/bin/vcs_diag to collect the diagnostic information.

The current working directory of VCS engine is VCS_DIAG whose default value is $VCS_HOME/diag. In earlier versions of VCS, the default directory of HAD was VCS_HOME whose default value was /opt/VRTSvcs.

Separate logger thread for HAD

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

Enhanced NFS lock failover

The new NFSRestart agent provides high availability to NFS locks. Use the agent in conjunction with the NFS agent.

See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information.

Support for VLAN interfaces

The NIC and MultiNICA agents now support VLAN interfaces. The agents do not configure the NICs, but can monitor them.

See the OS vendor's documentation on how to configure VLAN on your host, and ensure that the switch or router connected to such an interface is compatible with your configuration. Both server-side and switch-side VLAN configurations are supported.

Virtual fire drill

VCS supports a virtual fire drill capability that lets you test whether a resource can fail over to another node in the cluster. Virtual fire drills detect discrepancies between the VCS configuration and the underlying infrastructure on a node; discrepancies that might prevent a service group from going online on a specific node.

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

New term: Daemon Down Node Alive (DDNA)

Daemon Down Node Alive (DDNA) is a condition in which the VCS high availability daemon (HAD) on a node fails, but the node is running. When HAD fails, the hashadow process tries to bring HAD up again. If the hashadow process succeeds

in bringing HAD up, the system leaves the DDNA membership and joins the regular membership.

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

Change in behavior: Use comma or semicolon as delimiter

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

Change in behavior: New format for engine version

The new EngineVersion attribute replaces the MajorVersion and MinorVersion attributes. VCS stores version information in the following format:

major.minor.maintenance_patch_num.point_patch_num

For example:

5.0.30.0

Change in behavior for the resfault trigger

VCS now provides finer control over the resfault trigger. The resfault trigger is now invoked if the TriggerResFault attribute is set to 1.

Change in behavior: New location for enterprise agents

VCS enterprise agents are now installed in the /opt/VRTSagents/ha/bin directory.

The *agent*Types.cf files are now located at /etc/VRTSagents/ha/conf/*agent*.

Change in behavior: New location of message catalogs and attribute pools

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

/opt/VRTS/messages/*language*/module_name

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

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

Change in behavior: New option for the hastart and had commands

Use the -v option to retrieve concise information about the VCS version. Use the -version option to get verbose information.

Changes to bundled agents

VCS introduces the following new agents:

■ NFSRestart—Provides high availability for NFS record locks.

■ RemoteGroup—Monitors and manages a service group on another system.

■ Apache (now bundled on all platforms)—Provides high availability to an Apache Web server.

See "No longer supported" on page 27.

Changes to licensing for VCS

Table 1-2 describes the licensing scheme that VCS now follows.

Table 1-2   VCS licensing scheme

License	What's included
VCS	This license includes the following: ■ VCS ■ Cluster Management Console ■ Database agents ■ Application agents ■ Virtual fire drill support
VCS HA/DR	This license includes the following: ■ VCS ■ Cluster Management Console ■ Database agents ■ Application agents ■ Replication agents ■ Global clustering ■ Fire drill support

Note:

Database agents are included on the VCS 5.0 disc. The replication and application agents are available via the Veritas High Availability Agent Pack.

New attributes

VCS 5.0 introduces the following new attributes. See the *Veritas Cluster Server User's Guide* for more information.

Resource type attributes:

- AgentFile—Complete name and path of the binary for an agent. Use when the agent binaries are not installed at their default locations.

- AgentDirectory—Complete path of the directory in which the agent binary and scripts are located. Use when the agent binaries are not installed at their default locations.

Cluster attributes:

- EngineShutdown—Provides finer control over the hastop command.

- BackupInterval—Time period in minutes after which VCS backs up configuration files.

- OperatorGroups—List of operating system user account groups that have Operator privileges on the cluster.

- AdministratorGroups—List of operating system user account groups that have administrative privileges on the cluster.

- Guests—List of users that have Guest privileges on the cluster.

System attributes:

- EngineVersion—Specifies the major, minor, maintenance-patch, and point-patch version of VCS.

Service group attributes:

- TriggerResFault—Defines whether VCS invokes the resfault trigger when a resource faults.

- AdministratorGroups—List of operating system user account groups that have administrative privileges on the service group.

- OperatorGroups—List of operating system user account groups that have Operator privileges on the service group.

- Guests—List of users that have Guest privileges on the service group.

Removed attributes

VCS 5.0 does not use the following attributes:

- DiskHbStatus—Deprecated. This release does not support disk heartbeats. Symantec recommends using I/O fencing.

- MajorVersion—The EngineVersion attribute provides information about the VCS version.

- MinorVersion—The EngineVersion attribute provides information about the VCS version.

Updates to the Oracle agent

The Veritas High Availability Agent for Oracle introduces the following changes:

- New monitoring option—The basic monitoring option of the Oracle agent now allows health check monitoring in addition to the process check monitoring. You can choose the health check monitoring option for Oracle 10g and later.

- Support for virtual fire drills—VCS requires you to keep the configurations in sync with the underlying infrastructure on a cluster node. Virtual fire drills detect such discrepancies that prevent a service group from going online on a specific system.
  Refer to the *Veritas Cluster Server User's Guide* for more information.
  The agent uses the Action entry point to support the virtual fire drill functionality.

Updates to the Sybase agent

The Veritas High Availability Agent for Sybase introduces the following changes:

- The agent supports Sybase ASE 12.5.x and 15.

- The agent supports encrypted passwords.

VCS system requirements

This section describes system requirements for VCS.

The following information applies to VCS clusters. The information does not apply to SF Oracle RAC installations.

VCS requires that all nodes in the cluster use the same processor architecture and run the same operating system version. All cluster nodes must be at the same patch level.

See "Supported hardware" on page 26.

See "Supported operating systems" on page 26.

Veritas Installation Assessment Service

The Veritas Installation Assessment Service (VIAS) utility assists you in getting ready for a Veritas Storage Foundation and High Availability Solutions installation or upgrade. The VIAS utility allows the preinstallation evaluation of a configuration, to validate it prior to starting an installation or upgrade.

https://vias.symantec.com/

Supported hardware

VCS supports vpar/npar with the 11iv2 May 2005 release.

The compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit the following URL:

http://entsupport.symantec.com/docs/283161

Before installing or upgrading Veritas Cluster Server, review the current compatibility list to confirm the compatibility of your hardware and software.

Supported operating systems

VCS supports the following operating system versions:

- HP-UX 11i v3 March 2009 OEUR release or later

Note: Within a cluster, all systems must run on the same processor type and use the same operating system version and patch level. Mixed PA-RISC and Itanium clusters are not supported.

Supported software

VCS supports the following volume managers and files systems:

- Logical Volume Manager (LVM)

- HP File System (HFS)

- Veritas Volume Manager (VxVM) with Veritas File System (VxFS)

  - VxVM 4.1 with VxFS 4.1

  - VxVM 5.0.1 with VxFS 5.0.1

Other required HP-UX software

If you plan to install VCS from an NFS mounted directory, you must install the software `ONCplus - HP-UX 11i v3 version B.11.31.07.01`. The `ONCplus B.11.31.06` software bundled with HP-UX 11i v3 March 2009 OEUR release reports issues with long path names. This causes the installation to fail as the installer cannot copy files from the mounted directory to the systems on which you want to install VCS.

To download the software:

■ Go to http://software.hp.com.

■ Search for the software depot `ONCplus`.

■ Download ONCplus for HP-UX 11i v3 version B.11.31.07.01.

Supported VCS agents

Veritas agents support a specified application version on HP-UX 11i v3 if the application vendor supports that version on HP-UX 11i v3.

Table 1-3 lists the agents for enterprise applications and the software that the agents support.

Table 1-3   Supported software for the VCS agents for enterprise applications

Agent	Agent version	VCS version	Application	Application version	OS version
DB2	VCS 5.0.1	5.0 and later	DB2 Enterprise Server Edition	9.5	HP-UX 11i v3
Oracle	VCS 5.0.1	5.0 and later	Oracle Database Enterprise Edition	9i 10g R1 10g R2	HP-UX 11i v3
Sybase	VCS 5.0.1	5.0 and later	Sybase Adaptive Server Enterprise	12.5.x, 15.0.x	HP-UX 11i v3

See the Installation and Configuration Guide for the agents for more details.

For a list of the VCS application agents and the software that the agents support, see the Veritas Cluster Server Agents Support Matrix at Symantec website.

No longer supported

VCS no longer supports the following:

- CampusCluster agent

- ServiceGroupHB agent.
  This release does not support disk heartbeats. Symantec recommends using I/O fencing.

- Disk heartbeats (GABDisk).
  This release does not support disk heartbeats. Symantec recommends using I/O fencing.

- The updated Oracle agent does not support Oracle 8.0.x and Oracle 8.1.x.

- VCS documentation package (VRTSvcsdc)
  The VCS documentation package (VRTSvcsdc) is deprecated. The software disc contains the documentation for VCS in Portable Document Format (PDF) in the *cluster_server/docs* directory.
  Symantec recommends copying pertinent documents from the disc to your system directory /opt/VRTS/docs for reference.

Fixed issues

Refer to the following sections depending on the VCS version:

- See "Issues fixed in VCS 5.0.1 for HP-UX 11i v3" on page 28.

- See "Issues fixed in VCS 5.0 for HP-UX 11i v3" on page 36.

- See "Issues fixed in VCS 5.0" on page 39.

Issues fixed in VCS 5.0.1 for HP-UX 11i v3

Table 1-4 lists the issues fixed in VCS 5.0.1 on HP-UX 11i v3.

Table 1-4 VCS 5.0.1 on HP-UX 11i v3 fixed issues

Incident	Fix description
612587	The haclus -wait command does not hang now when cluster name is not specified.
643021	VCSAgExecInContainer() does not create the requested child process if the container is down.
797703	The output for the command vxfenadm -d displays an unknown character "M".
861792	Service groups are now listed in the groups table in the Recover Site wizard.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
862507	GAB_F_SEQBUSY flag is set even when the sequence request is not sent.
914752	Optimized LLT to print "node inactive" messages less frequently so as to not flood the dmesg buffer.
990610	The man page for the vxfentsthdw command does not have information about -d option.
1031514	Added cross-links for LLT to deal with one-way link situations.
1050999	Resolved a HAD issue that caused the ShutdownTimeout value to not work correctly.
1051193	The vxfen unconfigure command now uses the correct key to preempt/abort from faulted paths.
1053377	/usr/bin:/bin:/usr/sbin:/sbin is added first in the PATH env variable so that 'df', 'uname', and so on are picked up from these paths.
1054674	The wac process must produce an appropriate log message when it receives an affirmative response.
1056559	Fixed an issue where the NFSRestart monitor threw a, "too many open files" error.
1057418	The I/O fencing component can now retrieve the serial number of LUNs from a Pillar Data array. I/O fencing can now start without any issues and port b comes up for PillarData Arrays.
1057465	The vxfentsthdw command with the -f option attempts to copy a file even if source and destination location of the file is the same.
1016548	The issue that caused node panic with message "GAB: Port f halting system due to network failure" is fixed.
1061056	Child process of the agents now do not make calls to the logging functions of the VCSAgLog object.
1067667	When the VCS engine is stopping with evacuation, even if resource faults for a group with OnlineRetryLimit greater than zero, the evacuation completes.
1073342	Memory leak in LLT message recovery llt_msg_recv().
1074605	System panics with vxfen critical as the panic string.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1078230	The command vxfentsthdw produces error with the -f <mapfile> option, if the mapfile is created with absolute disk paths.
1084656	Executing WMT on cluster nodes causes GAB to panic.
1091284	Bug in printing port latency statistics.
1096394	Fixed an issue where notifier blocked the IPM socket.
1099651	Fixed the issue where the Process agent flooded the log and message files with the V-16-1001-9004 error message.
1102457	The vxfen initialization code has been modified to properly initialize parameters and avoid dereferencing of null pointer.
1137118	vxfen startup may indicate split brain due to pre-existing transient keys on coordinator disks.
1184144	LLT retransmits packets more efficiently now, by tranmitting up to N packets at at time, where N is less then the number of packets transmitted and outstanding for acknowledgement.
1190339	Fixed the error where vxfenadm could not unregister keys and as a result gave continuous error messages.
1113667	Replaced a fork call with a safer one.
1113791	The vxfen utility produces errors due to the presence of stale vxfen device files on the system.
1120189	Shutting down vxfen fails to create the vxfen log file and returns error and exits when there is no /var/VRTSvcs/log directory.
1133171	When new resources are added, the service threads in the corresponding agent will get created upto a maximum of NumThreads threads.
1156843	Sybase agent configuration with the -s option in the Sybase home path fails to bring the dervice group online.
1179686	Cookie APIs do not provide atomic clearing of the cookie.
1186414	The hastart command and triggers must run on the locale specified by the LANG variable.
1187580	Issues with the ActionTimeout attribute are fixed.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1193697	The default heartbeating mechanism in LLT is now point-to-point and not broadcast heartbeating.
1193980	A non-root user fails to authenticate on a secure cluster if a stale ~/.vcspwdis file is present.
1195685	Split brain occurs beacuse LLT is unable to communicate and subsequently the cluster nodes form separate GAB membership.
1201174	The `hastart` command produces core dumps when GAB is not configured.
1201615	LLT can read the correct physical address in a cross link scenario.
1203403	lltcanput is changed for same nid of destination as source.
1203620	Setting the AutoEndBkup to 1 (i.e. stop backup) does not end the backup process.
1204594	GAB takes longer time than expected to form membership in a cross-link scenario.
1208944	`vxfentsthdw` command was not using correct disk format for the disks. This issue is now fixed.
1209193	Repeated requests for password when ha commands are executed using a system based user.
1210437	Running the command hares -flushinfo on CVMVolDg or CFSMount resources produces core dumps.
1214464	The VCS agent for Sybase now uses the `getent passwd` command to check the user details defined in the Owner attribute.
1219148	When monitoring a global group, the RemoteGroup agent produces core dumps.
1226137	Steward produces core dumps when a cluster attempts to perform an enquiry in secure mode.
1237028	Adding encrypted passwords and maintaining clear text passwords are supported for backward compatibility for enterprise agents.
1237415	The reqhb mechanism is started 2 seconds before peer inact time to distinguish between peer node hang and peer node death case.
1238938	The n_heartbeat2 is reinitialized so that link trouble messages are not reported frequently in crosslinks.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1248000	For LLT, fixed the broadcast calculation logic while calculating the broadcast address for Class B network address.
1249376	Restricted LLT/GAB device permissions to 600 so that it cannot be accessed by non-root users.
1249385	Restricted VxFEN device permissions to 600 so that they cannot be accessed by non-root user.
1250544	MultiNICB agent reports false interface failures with multiple Auto Port Aggregation (APA) interfaces.
1253854	Fixed an incident where vxfenadm returns 255 instead of 0 even if it does not have any error.
1251518	During installation of Veritas Cluster Server 5.0 on HP-UX 11i v3, sometimes LLT or GAB filesets may be in the installed state as seen by 'swlist -l fileset -a state' .
1254474	GAB supports 128 nodes.
1256313	While unfreezing a group, check if there exists concurrency violation. Fire a concurrency violation trigger to remove the concurrency.
1259488	To prevent panics due to chained mblks, msgdsize is changed.
1259756	When NFSv4Support is set to 0, the nfsd and mountd daemons start with "--no-nfs-version 4" option.
1268550	The DiskGroup agent is enhanced to support large storage configurations.
1280144	Subroutines are added to set and reset locale in the ag_i18n_inc module.
1282209	Output from action entry point is now visible to the caller.
1285439	The clean script of the VCS agent for Sybase now supports removal of the IPC resources that the Sybase processes allocate.
1292809	The `vxfenconfig -l` command lists the coordinator disks that the vxfen driver uses .
1296465	If the ClusterService group is online on the same node on which a global service group is also online and if the node goes down, then the service group is failed over to a remote site.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1301698	If I/O fencing is started in the disabled mode, and if the vxfen_mode in /etc/vxfenmode file is changed later to SCSI-3, vxfen can be stopped without any error.
1319732	The VRTSvxfen package contained sample files for "sanvm" mechanism which is not supported. The spurious file has been removed from packages. References to "sanvm" mechanism have been removed from the vxfenmode man page.
1379299	For LLT, fixed the format string used to print messages so that the correct message is displayed.
1379532	The online script of the VCS agent for Oracle is fixed to use the startup force command when the value of the StartUpOpt attribute is set to STARTUP_FORCE.
1393158	The MultiNICA agent incorrectly reports that it is online even though the connection with NIC is lost.
1394624	For LLT, declare the global variable as volatile. This prevents the compiler from reordering any code statements around this variable.
1395905	The dmpconfig file descriptor is appropriately closed in vxfenadm.
1396404	While installing VCS, VRTSgab failed to install on both the cluster Nodes. This issue is now fixed.
1400037	The get node status messages were turned on in vxfen, which filled up the kernel log buffer. The get node status messages are turned off by default.
1421929	Modified the vxfen packaging files to use stricter permissions for vxfen commands. This has been done to improve security of the commands on all the platforms.
1410287	Issues with MultiNICA agent.
1452086	If I/O fencing is started in disabled mode, and if you change the /etc/vxfenmode file later to SCSI-3, the vxfen driver throws a spurious error when you stop vxfen. This issue has been fixed.
1464882	Introduced a ref count method in VxFEN to keep track of reconfigurations pending to clients. With this method, VxFEN un-configuration is allowed only when there are no pending reconfigurations. There is no client in the running state.

Table 1-4 VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1470032	'/etc/vxfentab' file created by '/sbin/ init.d/vxfen start' command now contains comments about the file.
1470065	The vxfenswap command allows you to change coordinator disks having keys registered on these already.
1474309	Fixed an issue where the error message for 'vxfenconfig -o rollback' did not provide the correct reason for failure to run the command.
1484568	Added a shared disks counter in vxfenclearpre which is displayed to the user after clearing keys from each of the shared disks. Example: Cleaning up the data disks for all shared disk groups.
1504693	[GAB/LLT] Fixed an issue in which LLT cannot provide back enable to GAB. This resulted in an error being produced from the GAB module gabwrite() function.
1512076	Created a soft link /var/adm/utils pointing to /opt/VRTS/bin/SG-CFS-lltgabutil.sh to fix the LLT warning during VCS installation.
1514889	If I/O fencing is unconfigured when it is waiting for seed port membership, now a proper message is displayed.
1522749	VxFEN is not able to shut down which causes the node to crash while halting the SG cluster.
1523423	[GAB] The issue that caused port w to halt the system due to depleted memory reserves is now fixed.
1525392	GAB waits after un-configuration till LLT closes the GAB ports.
1540807	errno is made thread specific so that errno returned by gab_receive is consistent. The gab library (libgab.so) is compiled with flags "-mt" and "-DREENTERENT" to make errno per thread.
1556310	Fixed an issue in which I/O fencing does not appear to be configured on node' when vxfen is configured in i18n envirenment.
1590749	vxfentsthdw test failed in both raw and DMP mode with IBM_XIV array.
1597627	The order of the lock "vxfen debug spinlock" is increased to higher than the order of RFSM locks.
1600786	If the vxfenswap utility is run on existing coordinator disks, then the registrations are done in the commit phase instead of the modify phase.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1631012	In the configuration of LLT over UDP4, when an IP address is not plumbed on a link and some IP address is specified in llttab file, lltconfig prints an error and the link is not configured.
1631270	Fencing when started with a blank vxfendg file displays the correct message.
1635044	The vxfentsthdw utility is enhanced to search path for scp/ssh in the following order: ■ use the path for ssh/scp set through SSH_ENV/SCP_ENV environment variables ■ use the standard path ■ use the paths defined in the PATH environment variable
1665036	vxfen-startup script and relevant vxfen startup code has been enhanced to retry if GAB/LLT returns EBUSY to VxFEN.
1670337	A new option (-t) is added to the `lltshow` command to track the OS time outs registered by LLT with the OS.
1672296	Messages related to VRTSvxfen are observed during installation of SFHA stack in DRD Clone disk.
1676233	The erroneous error messages that were recorded while uninstalling VRTS packages are now resolved.
1720205	Changed the VxFEN init script to bail out the startup process when /etc/vxfendg file does not have exactly one disk group.
1721992	lltping checks the status of links reports an error for invalid links.
1733231	vxfenswap (vxfenclearpre) utility uses the `vxgettext` command to print messages on the console . This command appends "\n" after each message. But, the new line should not be added to the messages which require input from the user. To fix this issue, "\c" is added to the messages (which requite user input) to suppress the trailing new line.
1733238	"shutdown -r now" message to be removed or modified in `vxfenclearpre` command.
1749396	[GAB] When LLT and GAB are started on both the nodes of a two node cluster simultaneously , GAB shows jeopardy even if two links are configured under LLT. This issue is now fixed.

Table 1-4   VCS 5.0.1 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
1702445	When a node joins the cluster at the time when another node with a LLT node-id lower than that of the new joiner is leaving the cluster, the new node may get panic from GAB running on a node (with the lowest LLT node id) with the following string: "Port b halting system due to network failure" This issue is now fixed.
1749323	LLT gives an error if an attempt is made to configured more than 8 links.
1748713	[VxFEN] When vxfenswap is invoked without -n option and ssh is not configured for password free logins, it prompts the user for password multiple times. Modified the code to check whether ssh/rsh is configured for password free logins. Otherwise, it prints appropriate message and bails out.

Issues fixed in VCS 5.0 for HP-UX 11i v3

lists the issues fixed in VCS 5.0 on HP-UX 11i v3.

Table 1-5   VCS 5.0 on HP-UX 11i v3 fixed issues

Incident	Fix description
243186	Assertion in VCS engine.
244988	Very large login name and password takes all the service groups offline. Fix: For group name, resource name, attribute name, type name, and VCS username and password, the string size is limited to 1024 characters.
545469	The Monitor entry point does not detect an online when the Oracle instance is not started by the user defined in the Owner attribute.
570992	Cluster Management Console does not display some icons properly.
598476	If you have a service group with the name ClusterService online on the last running node on the cluster, the hasim -stop command appears to hang.
602636	Service group fails over to the second node on killing both HAD and hashadow. As part of the fix for this issue, a regression was introduced in LLT, which is fixed in incident 620535.

Table 1-5   VCS 5.0 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
609555	The Remote Group Agent wizard in the Java GUI rejects the connection information for the remote cluster with the domain type other than the local cluster.
	Fix: The RGA Wizard can now connect to all supported domain types irrespective of the domain type of local cluster.
614654	Change the unregister code path to do a combination of PREEMPT and then unregister.
616580	Importing resource types fails on Simulator on Windows systems.
616652	The template for the NFS service has an incorrect definition for the NIC resource.
616964	In a secure environment, the RemoteGroup agent does not authenticate on a remote host for the first time.
617616	The installvcs -security command fails while enabling security in "auto" mode for DNS qualified Root Broker.
	Fix: Support for fully qualified host name or partially qualified host name of Root Broker added to installer.
619219	Running the hastart command twice causes an assertion to be displayed.
620529	Cluster Management Console does not display localized logs.
	If you installed language packs on the management server and on VCS 5.0 cluster nodes, Cluster Management Console did not initially show localized logs.
625490	For the agent framework module, ag_i18n_inc.sh does not invoke halog when script entry points use the VCSAG_LOGDBG_MSG API, even if the debug tag is enabled.
627564	VCS configuration wizards on HP-UX PA secure clusters fail to start.
627568	The STARTUP_FORCE value needs to be added in the drop-down list of StartUpOpt values in the Oracle and RAC wizards as the default value for StartUpOpt.
627647	The Action entry point for Oracle fails because set_environment() function prototype differs.
646372	The hatype -modify … -delete …command works incorrectly. The command deletes the first element of the keylist attribute.

Table 1-5   VCS 5.0 on HP-UX 11i v3 fixed issues *(continued)*

Incident	Fix description
702594	The Oracle agent does export SHLIB_PATH and other environment in CSH.
702597	VCS ignores the value of the cluster-level attribute EngineShutdown while the system is shutting down.
784335	The Oracle agent cannot identify the shell when the /etc/passwd file has multiple occurrence of the $Owner string.
1020838	Clean entry point for MonitorProcesses attribute does not work correctly.
1060963	NFSRestart monitor leaks file descriptors.
1096394	HAD dumps core when Notifier resource is configured.
1113667	Use of vfork causes a deadlock between parent and child processes.
1133223	Replace thread-unsafe calls with thread-safe calls.
1161339	Application agent does not inherit user defined LANG parameter.
1170248	Mount Agent and filesystems greater than 2TB size.
1174520	HAD asserts if service group with single system in SystemList is unfreezed.

Additionally, the following incidents were also fixed.

Concurrency violation with online firm dependencies

The concurrency violation trigger could not offline a service group if the group had a parent online on the system with local firm dependency. The concurrency violation continued until the parent was manually taken offline.

Web server configuration page offers two locale options

The configuration page for the Symantec Web server (VRTSWeb) offered two Japanese locale options. Both options had UTF-8 encoding, and there were no functional difference between the two.

Oracle agent uses pfile for initialization

The agent for Oracle obtained its initialization parameters from the pfile. VCS could not monitor Oracle instances created from the spfile.

Cluster Manager installation on Windows XP

When installing Cluster Manager on a Windows XP system, the following error appeared: "The installer has insufficient privileges to access this directory: C:\Config.Msi."

Issues fixed in VCS 5.0

Table 1-6 lists the fixed issues for VCS 5.0.

Table 1-6   VCS 5.0 fixed issues

Incident	Issue description
n/a	The concurrency violation trigger could not offline a service group if the group had a parent online on the system with local firm dependency. The concurrency violation continued until the parent was manually taken offline.
n/a	The configuration page for the Symantec Web server (VRTSWeb) offered two Japanese locale options. Both options had UTF-8 encoding, and there were no functional difference between the two.
n/a	The agent for Oracle obtained its initialization parameters from the pfile. VCS could not monitor Oracle instances created from the spfile.
n/a	When installing Cluster Manager on a Windows XP system, the following error appeared: "The installer has insufficient privileges to access this directory: C:\Config.Msi."
584243	hares options do not filter correctly.
515644	hacf does not handle MAXARG values of vector/associative attributes in the main.cf.
426932	Indeterministic service thread cancellation.
271167	Provide finer control over the hastop -all command.
254947	GAB and LLT device files have open permissions.
252347	Behavior of parent group is incorrect when groups are linked with online global firm and child group faults.
248069	Commands do not close socket after successful termination.
247698	Need to move logging activities out of single-threaded HAD.
246238	Information required when had is restarted either by hashadow or gab.

Known issues

The following issues are open for this release of VCS.

Issues related to installing and upgrading VCS

This section covers the issues related to installing and upgrading VCS.

Errors recorded in the swremove logs of VRTSgab during VCS upgrade from 4.1 to 5.0.1

When VCS is upgraded from 4.1 to 5.0.1 on HP-UX 11i v3 using the Veritas product installer, the installer reports errors for GAB and errors are recorded in the swremove logs related to VRTSgab. [1719136]

You can safely ignore these error messages.

VCS agents dump core after the operating system is upgraded from HP-UX 11i v2 to HP-UX 11i v3 using the update-ux command

On PA-RISC architecture, the VCS agents (Oracle, Netlsnr, Sybase, SybaseBk, MultiNICB, and so on) may dump core after the operating system is upgraded from HP-UX 11i v2 to HP-UX 11i v3 using the update-ux command.[1630968]

This is because on HP-UX PA-RISC systems, the default thread stack size is limited to 64k. When the agent requires more than 64k stack memory, it may dump core due to SIGBUS error.

Workaround: Before running the update-ux command, edit the /opt/VRTSvcs/bin/vcsenv file to append following lines to it:

```
PLATFORM=`uname -s`
ARCHITECTURE=`uname -m`
if [ "${PLATFORM}" = "HP-UX" ] && [ "${ARCHITECTURE}" = "9000/800" ]; then
        PTHREAD_DEFAULT_STACK_SIZE=524288
        export PTHREAD_DEFAULT_STACK_SIZE
fi
```

Operational issues for VCS

This section covers the operational issues for VCS.

Volumes outside of VCS control that are mount locked cannot be unmounted without specifying the key

If a VxFS file system has "mntlock=key" in its mount options, then you cannot unmount the file system without specifying the key. Groups having DiskGroup resources configured with UmountVolumes set, may fail to switch or failover if the volumes are mount locked. [1276594]

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 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: [251660]

- 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 the `hastop -force` command 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.

Node cannot join cluster because port v is not ready for configuration

This behavior is observed when a node leaves a cluster and another node tries to join the cluster at the same time. If the GAB thread is stuck in another process, the new node cannot join the cluster and GAB logs the following warning:

```
GAB WARNING V-15-1-20126 Port v not ready
for reconfiguration, will retry.
```

Using the coordinator attribute

This release contains an attribute for disk groups called coordinator, which configures disks as coordinator disks by the I/O fencing driver. Setting the attribute prevents the coordinator disks from being reassigned to other disk groups. See the Veritas Volume Manager documentation for additional information about the coordinator attribute.

The attribute requires that the disk group contain an odd number of disks. Symantec recommends that you use only three coordinator disks. Using more (five or seven) disks may result in different subclusters.

Some alert messages do not display correctly

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

51033	Global group %s is unable to failover within cluster %s and AutoFailOver is %s. 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
51031	Unable to automatically fail over global group %s remotely because local cluster does not have Authority for the group.
51030	Unable to find a suitable remote failover target for global group %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.
50914	Global group %s is unable to failover within cluster %s and ClusterFailOverPolicy is set to %s. Administrative action is required.
50913	Unable to automatically fail over global group %s remotely because clusters are disconnected and ClusterFailOverPolicy is set to %s. Administrative action is required.
50836	Remote cluster %s has faulted. Administrative action is required.
50761	Unable to automatically fail over global group %s remotely because ClusterList values for the group differ between the clusters. Administrative action is required.

Issues related to the VCS engine

This section covers the issues related to the VCS engine.

LinkHbStatus does not reflect the link status correctly

After disabling the LLT links of a node, the LinkHbStatus does not reflect the 'DOWN' flag for that node in 'hasys -disp'.[1831129]

Engine may hang in LEAVING state

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

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

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 the VCS bundled agents

This section covers issues related to the VCS bundled agents.

RemoteGroup agent's monitor function may time out when remote system is down

If a RemoteGroup agent tries to connect to a system (specified as IpAddress) that is down, the monitor function of the RemoteGroup agent times out for the resource. [1397692]

LVMVolumeGroup resources do not depend on DiskReservation resources

An LVMVolumeGroup resource does not depend on a DiskReservation resource. [1179518]

Problem in failing over the IP resource

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

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

LVMLogicalVolume agent may hang

The LVMLogicalVolume agent may hang in some situations, depending on the value of the IOTimeout attribute. Symantec recommends using the LVMCombo agent instead of the LVMLogicalVolume and LVMVolumeGroup agents.

LVM agents do not detect disconnected cable

LVM commands continue to function correctly when the cable to disks is pulled. The LVM agent does not detect a fault in this situation.

Issues related to the I/O fencing for VCS

This section covers the issues related to I/O fencing feature for VCS.

Preexisting split brain after rebooting nodes

If I/O fencing is configured in dmp mode, the fencing driver in VCS 5.0 uses Veritas DMP to handle SCSI commands to the disk driver. This allows fencing to use Veritas DMP for access to the coordinator disks. With certain disk arrays, when paths are failed over due to a path failure, the SCSI-3 persistent reservation keys for the previously active paths are not removed. If the nodes in a cluster are all

rebooted at the same time, then the cluster will not start due to a `Preexisting split brain` message. [609407]

Workaround: Use the vxfenclearpre script to remove the keys from the coordinator disks as well as from the data disks.

Stopping vxfen when the fencing module is being configured

Trying to stop the vxfen driver when the fencing module is being configured results in the following error.

```
VXFEN vxfenconfig ERROR V-11-2-1013 Unable to unconfigure vxfen
VXFEN vxfenconfig ERROR V-11-2-1022 Active cluster is currently fencing.
```

Workaround: This message may be safely ignored.

I/O fencing configuration fails if fencing module is running on another node

The `vxfenconfig -c` command fails if any of the following commands are running on other nodes in the cluster:

```
/sbin/vxfenconfig -U
/sbin/vxfenconfig -c

vxfenconfig -U
vxfenconfig -c
```

Some vxfenadm options do not work with DMP paths

Some options of the vxfenadm utility do not work well with DMP paths such as /dev/vx/rdmp/sdt3.

Workaround: Use the -a option to register keys instead of -m option for DMP paths.

Issues related to Symantec Product Authetication Service with VCS

This section covers the issues related to Symantec Product Authentication Service with VCS.

The atldapconf command fails if the user in the Active Directory does not belong to any group

While using the atldapconf command, the user group must be specified. [1596332]

Output of addldapdomain returns error

The output of addldapdomain returns an error and the help contains incorrect information [1589886]

Issues related to global service groups

This section covers the 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 VCS Agent for DB2

This section covers issues related to the VCS agent for DB2.

awk error message

On IA-64, the default awk command may produce this error: Input line /usr/bin:/bin:/usr/s cannot be longer than 3,000 bytes. The source line number is 1.

Workaround: Install GNU awk.

Issues related to the VCS Agent for Oracle

This section covers the issues related to the VCS agent for Oracle.

NOFAILOVER action specified for certain Oracle errors

The Veritas High Availability agent for Oracle provides enhanced handling of Oracle errors encountered during detailed monitoring. The agent uses the reference file oraerror.dat, which consists of a list of Oracle errors and the actions to be taken.

See the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide* for a description of the actions.

Currently, the reference file specifies the NOFAILOVER action when the following Oracle errors are encountered:

```
ORA-00061, ORA-02726, ORA-6108, ORA-06114
```

The NOFAILOVER action means that the agent sets the resource's state to OFFLINE and freezes the service group. You may stop the agent, edit the oraerror.dat file, and change the NOFAILOVER action to another action that is appropriate for your environment. The changes go into effect when you restart the 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.

ASM instance does not unmount VxVM volumes after ASMDG resource is offline

In configurations where ASMInstance resource is part of a separate parallel service group, the ASM instance does not unmount the volumes even after the ASMDG resource is taken offline. Therefore, the Volume resource cannot be taken offline. This issue occurs when you use VxVM volumes as ASM disk groups. [918022]

Workaround: Configure the ASMInstance resource as part of the failover service group where ASMDG resource is configured.

Issues related to the Cluster Manager (Java Console)

This section covers the issues related to the Cluster Manager (Java Console).

Cluster Manager (Java Console) may display an error while loading templates

You can access the Template View in the Cluster Manager from the Tools > Templates menu. If you have Storage Foundation configured in a VCS cluster setup, the following error may occur while the Cluster Manager loads the templates. (1433844)

```
VCS ERROR V-16-10-65 Could not load :- /etc/VRTSvcs/Templates/DB2udbGroup.tf
```

Workaround: Ignore the error.

Exception when selecting preferences

On Windows systems, selecting the Java (Metal) look and feel of the Java Console may cause a Java exception. [585532]

Workaround: After customizing the look and feel, close restart the Java Console.

Java Console errors in a localized environment

When connected to cluster systems using locales other than English, the Java Console does not allow importing resource types or loading templates from localized directories. [585532]

Workaround: The workaround is to copy the types files or templates to directories with english names and then perform the operation.

Printing to file from the VCS Java Console throws exception

VCS Java Console and Help throw an exception while printing to a file from a system that does not have a printer configured. Also, the content is not written to the file.

Workaround: Before printing, make sure at least one printer is configured on the system where the VCS Java Console is launched.

Common system names in a global cluster setup

If both local and remote systems have a common system name in a global cluster setup, group operations cannot be performed on those systems using the Java console.

Workaround: Use command-line interface to perform group operations.

Some Cluster Manager features fail to work in a firewall setup

In certain environments with firewall configurations between the Cluster Manager and the VCS cluster, the Cluster Manager fails with the following error message [1392406]:

```
V-16-10-13 Could not create CmdClient. Command Server
may not be running on this system.
```

Workaround: You must open port 14150 on all the cluster nodes.

Issues related to the VCS Management Console

This section covers the issues that are related to the VCS Management Console.

Cluster Connector installation and configuration for fresh install of VCS 5.0 MP3 is not available

If you want to manage clusters that have VCS 5.0MP3, you must use the direct connection mode.

Warning messages in the log file when running the installmp command

The installmp command logs the following messages. [782798]

```
warning: user vcsbuild does not exist - using root
warning: group fcf does not exist - using root
warning: user vcsbuild does not exist - using root
warning: group fcf does not exist - using root
```

Workaround: None. You may ignore these messages.

Platform attribute in the ClusterConnector.config file is not updated

The Platform attribute in the ClusterConnector.config file remains set to Solaris irrespective of the installation platform. The ClusterConnector.config file is created by the ClusterConnectorConfig agent and is used to set values in resource type definitions and main.cf configurations for the agent. [837685]

The ClusterConnectorVersion attribute might have no value because this value is not used in the current release.

Known issue for the Migrate Site task

The Migrate Site task starts the Migrate Site wizard that enables you to migrate one or more global service groups to one or more remote target clusters. The Cluster Management Console does not migrate a faulted service group. If you attempt to migrate a faulted service group, you may see an entry similar to the following in the management server log:

```
2006-11-20 10:38:33 INFO    Unable to use the -force option when
the cluster that has Authority for the group is not completely
down {vrts.vxcs.mcm.gui.web.actions.wizard.MigrateSiteLastPage
lookupFinish()
```

Workaround: In the Global Application Group Selection panel, select only service groups that are in the online or partial state. Do not select service groups that are in the faulted state.

swverify errors for Veritas Cluster Management Console Cluster Connector (VRTScmccc)

Running the `swverify` command on a node after installing VCS 5.0 on HP-UX 11i v3 might report an error for the /etc/VRTSvcs/conf/config/ClusterConnectorConfigType.cf file of VRTScmccc package. [1235978]

Workaround: This error is harmless and can be fixed by modifying the IPD for VRTScmccc with the following commands:

On PA-RISC systems

"swmodify -a is_volatile=true -x files=/etc/VRTSvcs/conf/config/ClusterConnectorConfigType.cf VRTScmccc.VRTSCMCPA"

On IA64 systems

"swmodify -a is_volatile=true -x
files=/etc/VRTSvcs/conf/config/ClusterConnectorConfigType.cf
VRTScmccc.VRTSCMCIA"

Erroneous output from `gares` command

The `gares` command returns a value for the Start attribute that is different from
what the hares command returns. The local values are inverted (exchanged). For
example, if gares returns 1, hares returns 0. [853969]

Workaround: This situation can result if the attribute values with local scope are
missing for a newly-added system in the system list of a service group. Use the
switch command for the CMC_CC service group (for configurations that use the
cluster connector) or reconnect to the cluster (for configurations that use direct
connection).

Cluster Management Console displays fatal errors

CMC displays fatal errors when it encounters an invalid XML file for an agent.
[595973]

Workaround: None. Make sure the XML files for custom agents are valid.

The database fails to back up or restore to a path with Japanese characters

The database fails to back up or restore to the specified path with Japanese
characters in it, when the command gadb -backup is run. [767796]

Workaround: Use English folder names when backing up, then copy the database
file to the Japanese folder manually, if required.

Cannot uninstall updates on Windows management server

On Windows, uninstalling the VCS 5.0 MP1 management server using Add or
Remove Programs removes only the entry from the Add or Remove Programs list.
No files are removed. You must perform a management server uninstallation
using the original VCS 5.0 uninstallation program. You cannot revert a VCS 5.0
MP1 management server back to a VCS 5.0 management server. [841149]

View displays incorrect version

After upgrading to the Cluster Management Console for VCS 5.0 MP1, the
Admin:Management Server view (Admin –> Management Server) shows an

incorrect version of 5.0.1136.0 and an incorrect installation history. The correct information is in the About box. [856103]

Default SMTP and SNMP addresses in notification policies for Cluster Management Console

When you configure notification settings, the Edit SMTP Settings task asks you to provide default email or default SNMP console addresses. The policy configuration wizard uses these addresses only to populate the recipient lists during policy configuration. The wizard does not automatically configure policies with these addresses.

When you launch the Notification Policy Configuration wizard, the default email address you specified appears in the Notification Recipients dialog box.

If you add email addresses to this list, the wizard adds them to the policy along with the default address. However, if you delete all the addresses from the Email Recipients list, including the default email address, the wizard configures no email addresses in the policy.

Leave default email addresses in the recipients list to configure them into the policy.

The same behavior applies to specifying default SNMP addresses.

Console displays logs in English and Japanese

If your management server is configured to run in the Japanese locale, but the managed cluster does not have the Japanese language pack installed, the management server displays a mix of logs in English and Japanese. [778176]

Workaround: Make sure the managed cluster has the Japanese language pack installed.

Some Cluster Management Console controls not immediately active

In some versions of Internet Explorer, you may need to click Flash-based screens, popups, and wizards once before the controls become active. Controls that require this activating click show the following message when you roll over them with your mouse pointer [603415]:

```
Press SpaceBar or Click to activate this Control
```

Login screen may not display after inactivity timeout

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

Workaround: Use the browser refresh feature and the login screen will display.

Very large clusters may not load into Cluster Management Console

Very large clusters may not load into Cluster Management Console. [493844]

Workaround: To accommodate very large clusters, increase the value of the loadClusterQueryTimeout property in the management server configuration file, /opt/VRTScmc/conf/ManagementServer.conf. The management server generates this file upon startup.

To load large clusters into Cluster Management Console

1 Stop the Cluster Management Server web console:

    /opt/VRTSweb/bin/stopApp cmc

2 Add the following line to the file /opt/VRTScmc/conf/ManagementServer.conf:

    loadClusterQueryTimeout=60000

   Adjust the value as needed to allow complete initial load of your cluster information.

3 Start the Cluster Management Server web console:

    /opt/VRTSweb/bin/startApp cmc ../VERITAS

Log entries in the Management Server:Logs view

The Management Server:Logs view might contain log entries for the management server and for the cluster. [610333]

Management server log entries have the value site in the Object Type column. Cluster log entries have the value cluster in the Object Type column.

Cannot install if VxAT 4.3 is installed

If you have installed Symantec Product Authentication Services on a system using the 4.3 client/server installer, install of Cluster Management Console will not

succeed because the path to the AT binaries is not in the path. Since this path is not present, the custom action DLL in our MSI will not be able to run certain AT-related commands. [617861]

Workaround: Add the path for the AT binaries before attempting a Cluster Management Console install.

Windows management server uninstall using Add or Remove Programs does not remove folder

After using Add or Remove Programs to remove (uninstall) the Windows management server, an empty Cluster Management Console folder remains:

The default path is C:\Program Files\VERITAS.

Workaround: Delete the empty folder after the uninstall.

Windows cluster monitor uninstall does not remove folder

After a Windows cluster monitor uninstall, an empty folder remains:

The default path is C:\Program Files\VERITAS.

Workaround: Delete the empty folder after the uninstall.

Uninstalling Cluster Connector does not remove entry from Add\Remove Programs on Windows

After you uninstall cluster connector on Windows cluster nodes, the Add or Remove Programs control panel continues to show an entry for cluster connector. This persistent entry prevents any reinstallation of cluster connector. [599424]

Workaround: Remove the Veritas Cluster Management Console entry from the list using Windows Installer Cleanup Utility. Run the utility to remove the entry on each node. If you do not have the utility, you may download it from the Microsoft support site.

Windows install over Terminal Services needs Service Pack 4

Per Microsoft, Windows 2000 without at least Service Pack 4 has problems installing multiple MSI files that alter the same registry key over Terminal Services.

Workaround: If you want to install to a Windows 2000 host using Terminal Services, first ensure that the system has Windows 2000 Service Pack 4 installed.

Removing the CMC_SERVICES domain

Uninstalling the management server in multi-cluster environments does not remove the *CMC_SERVICES* domain. [612176]

You can verify the existence of this domain using the following command:

```
vssat showpd --pdrtype ab --domain CMC_SERVICES
```

You must manually remove the CMC_SERVICES domain using the command line. To manually remove all the peripherals in the CMC_SERVICES domain, enter the following command:

```
vssat deleteprpl --pdrtype ab --domain
CMC_SERVICES --prplname principalname
```

Enter the following command to remove the domain:

```
vssat deletepd --pdrtype ab --domain CMC_SERVICES@hostname
```

You can determine the host name using the following command:

```
vssat showpd
```

Issues related to VCS Simulator

This section covers the issues related to VCS Simulator.

Simulator clusters with Windows configurations fail to start on UNIX host platforms

The following clusters are affected: Win_Exch_2K3_primary, Win_Exch_2K3_secondary, Win_Exch_2K7_primary, Win_Exch_2K7_secondary, WIN_NTAP_EXCH_CL1, WIN_NTAP_EXCH_CL2, Win_SQL_Exch_SiteA, Win_SQL_Exch_SiteB, WIN_SQL_VVR_C1, WIN_SQL_VVR_C2. [1363167]

Workaround: For each of these clusters, there is a separate directory named after the cluster under the VCS Simulator installation directory

C:\Program Files\VERITAS\VCS Simulator on Windows

/opt/VRTScssim on Unix

Perform the following steps:

- Navigate to the conf/config directory under this cluster specific directory.

- Open the types.cf file in an editor and change all instances of the string "i18nstr" to "str".

- Open the SFWTypes.cf file in an editor if it exists in this directory and change all instances of the string "i18nstr" to "str".

- Repeat these steps for the following files if they exist: MSSearchTypes.cf, SQLServer2000Types.cf, ExchTypes.cf, SRDFTypes.cf.

VCS Simulator does not start on Windows systems

On Windows systems, starting VCS Simulator displays an error that the required MSVCR70.DLL is not found on the system. [859388]

Workaround: Run the following command:

```
set PATH=%PATH%;%VCS_SIMULATOR_HOME%\bin;
```

Or append %VCS_SIMULATOR_HOME%\bin; to PATH environment variable.

Error in LVMVolumeNFSGroup template for AIX

In the VCS Simulator, the AIX_NFS cluster gives error while loading the LVMVolumeGroupNFS template. [1363967]

This problem can also affect real AIX clusters if they try to load this template.

Workaround: For the Simulator, navigate to the Templates/aix directory under the VCS Simulator installation directory (C:\Program Files\VERITAS\VCS Simulator on Windows, /opt/VRTScssim on Unix). Open the LVMVolumeNFSGroup.tf file and look for all instances of the MajorNumber = "". Remove the empty double-quotes and set the correct integer value for MajorNumber.

For real clusters, make identical changes to /etc/VRTSvcs/Templates/LVMVolumeNFSGroup.tf.

Other known issues

This section covers other known issues.

Startup or shutdown failure messages reported for LLT, GAB, and VXFEN

If you need to reboot the system when you install VCS, the init scripts for LLT, GAB, and VXFEN report start or stop failure messages. This is because VCS is not yet configured and the required configuration files are not yet generated for these components. These messages may be ignored. [1666327]

Software limitations

The following limitations apply to this release.

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.

VCS deletes user-defined VCS objects that use the HostMonitor object names

If you had defined the following objects in the main.cf file using the reserved words for the HostMonitor daemon, then VCS deletes these objects when the VCS engine starts [1293092]:

- Any group that you defined as VCShmg along with all its resources.

- Any resource type that you defined as HostMonitor along with all the resources of such resource type.

- Any resource that you defined as VCShm.

GAB panics the systems while VCS gets diagnostic data

On receiving a SIGABRT signal from GAB, VCS engine forks off vcs_diag script. When VCS engine fails to heartbeat with GAB, often due to heavy load on the system, the vcs_diag script does a sys req to dump the stack trace of all processes in the system to collect diagnostic information. The dump of stack trace is intended to give useful information for finding out which processes puts heavy load. However, the dumping puts extra load on the system that causes GAB to panic the system in such heavy loads. See *Veritas Cluster Server User's Guide* for more information. [383970]

Workaround: Disable the vcs_diag script. To disable, rename the file /opt/VRTSvcs/bin/vcs_diag to /opt/VRTSvcs/bin/vcs_diag.backup.

Using agents in NIS

Programs using networked services (for example, NIS, NFS, RPC, or a TCP socket connection to a remote host) can hang if the host is disconnected from the network. If such a program is used as an agent entry point, a network disconnect can cause the entry point to hang and possibly time out. For example, if the host is configured to use NIS maps as a client, basic commands such as ps -ef can hang if there is network disconnect. Symantec recommends creating users locally. To reflect local users, configure:

/etc/nsswitch.conf

Fire drill does not support volume sets

The fire drill feature for testing fault readiness of a VCS configuration supports only regular Volume Manager volumes. Volume sets are not supported in this release.

Limitations with DiskGroupSnap agent

The DiskGroupSnap agent has the following limitations:

■ The DiskGroupSnap agent does not support layered volumes. [1368385]

■ If you use the Bronze configuration for the DiskGroupSnap resource, you could end up with inconsistent data at the secondary site in the following cases [1391445]:

  ■ After the fire drill service group is brought online, a disaster occurs at the primary site during the fire drill.

  ■ After the fire drill service group is taken offline, a disaster occurs at the primary while the disks at the secondary are resynchronizing.

Symantec recommends that you use the Gold configuration for the DiskGroupSnap resource.

VxVM site for the diskgroup remains detached after node reboot in campus clusters with fire drill

When you bring the DiskGroupSnap resource online, the DiskGroupSnap agent detaches the site from the target diskgroup defined. The DiskGroupSnap agent invokes VCS action entry points to run VxVM commands to detach the site. These commands must be run on the node where the diskgroup is imported, which is at the primary site.

If you attempt to shut down the node where the fire drill service group or the diskgroup is online, the node goes to a LEAVING state. The VCS engine attempts to take all the service groups offline on that node and rejects all action entry point requests. Therefore, the DiskGroupSnap agent cannot invoke the action to reattach the fire drill site to the target diskgroup. The agent logs a message that the node is in a leaving state and then removes the lock file. The agent's monitor function declares that the resource is offline. After the node restarts, the diskgroup site still remains detached. [1272012]

Workaround:

You must take the fire drill service group offline using the `hagrp -offline` command before you shut down the node or before you stop VCS locally.

If the node has restarted, you must manually reattach the fire drill site to the diskgroup that is imported at the primary site.

Manually removing VRTSat package erases user credentials

Symantec recommends saving user credentials before manually removing the VRTSat package. If you need the credentials again, you can restore them to their original locations.

To save user credentials

1   Run the vssat showbackuplist command. The command displays the data files and backs them up into the SnapShot directory /var/VRTSatSnapShot. Output resembles the following:

```
vssat showbackuplist
B| /var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B| /var/VRTSat/.VRTSat/profile/certstore
B| /var/VRTSat/RBAuthSource
B| /var/VRTSat/ABAuthSource
B| /etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
```

2   Move the credentials to a safe location. Preserving the directory structure makes restoring the files easier.

To restore user credentials

1   Navigate to the SnapShot directory or the safe location where you previously saved credentials:

```
cd /var/VRTSatSnapShot/
```

2   Restore the files:

```
cp ABAuthSource /var/VRTSat/
cp RBAuthSource /var/VRTSat/
cp VRTSat.conf /etc/vx/vss/
cd /var/VRTSatSnapShot/
cp -rp profile /var/VRTSat/.VRTSat/
```

Bundled agent limitations

This section covers the software limitations for VCS 5.0 bundled agents.

NFS wizard limitation

The NFS wizard allows only one NFS service group to be created. You need to create additional groups manually.

Volume agent clean may forcibly stop volume resources

When the attribute FaultOnMonitorTimeouts calls the Volume agent clean entry point after a monitor time-out, the vxvol -f stop command is also issued. This command forcibly stops all volumes, even if they are still mounted.

NFS failover

If the NFS share is exported to the world (*) and the NFS server fails over, NFS client displays the following error, "Permission denied".

To avoid this error, export NFS shares explicitly using FQDN hostnames.

False concurrency violation when using PidFiles to monitor application resources

The PID files created by an application contain the PIDs for the processes that are monitored by Application agent. These files continue to exist even after a node running the application crashes. On restarting the node, the operating system may assign the PIDs listed in the PID files to other processes running on the node.

Thus, if the Application agent monitors the resource using the PidFiles attribute only, the agent may discover the processes running and report a false concurrency violation. This could result in some processes being killed that are not under VCS control.

Networking agents do not support IPv6 protocol

The bundled IP, NIC, IPMultiNIC, MultiNICA, IPMultiNICB, and MultiNICB agents for VCS 5.0.1 do not support the IPv6 enhanced IP protocol.

VCS does not provide a bundled agent for volume sets

VCS 5.0.1 does not provide a bundled agent to detect Volume Manager volume sets, Problems with volumes and volume sets can only be detected at the DiskGroup and Mount resource levels.

Workaround: Set StartVolumes and StopVolumes attributes of the DiskGroup resource that contains volume set to 1. If a file system is created on the volume set, use a Mount resource to mount the volume set.

Cluster Management Console limitations

This section covers the software limitations for Cluster Management Console.

Cluster connector not supported on some OS versions

Cluster Management Console does not support cluster connector on AIX 5.1, Solaris 7, and RHEL 3.0. If your cluster runs on any of these platforms, you must use direct connection to manage the cluster from a management server.

Limited peer management server support

Peer management server support is limited to a configuration of two management servers in an enterprise. An enterprise of three or more management servers is not supported in this release.

Management server cannot coexist with GCM 3.5 Master

The Cluster Management Console management server should not be installed on the same system with a GCM 3.5 Master. These two products will conflict with each other and are not supported running on the same system.

Agent info files needed for Agent Inventory report

By design, the Agent Inventory report requires agent info files that supply the information reported on individual agents. These files are shipped with agents in VCS.

Global clusters must be CMC-managed clusters

All clusters forming a global cluster (using the VCS 4.0 Global Cluster Option) must be managed clusters in order for Veritas Cluster Management Console views to display correct and consistent information. Managed clusters are running the cluster connector or have a direct connection with the management server.

HP-UX cluster connector install fails if filesystem mount fails

If an HP-UX system has a mount that is not in /etc/fstab or /etc/checklist, the HP-UX installer swinstall will not work. Be sure the mount has an entry in these files.

Be sure the HP-UX system is configured to not attempt mounting of all the filesystems when performing an install or uninstall. This can be accomplished by adding the following lines to the /var/adm/sw/defaults file:

```
swinstall.mount_all_filesystems=false
swremove.mount_all_filesystems=false
```

Windows Active Directory installation requires NetBIOS

If you install Cluster Management Console management server in a Windows Active Directory domain, NetBIOS must be turned on. A native (non-NetBIOS) Active Directory environment is not supported in this release.

Remote root broker not supported on Windows

If you set up a management server on a Windows system, you must configure a root broker on the management server system. This release does not support specifying a remote root broker during management server install [841739].

The root broker can be changed after install using the configureRemoteRoot.exe installed in C:\Program Files\VERITAS\Cluster Management Console\bin (default install directory).

Cluster Manager (Java console) limitations

This section covers the software limitations for Cluster Manager (Java Console).

Use the VCS 5.0 Java Console to manage clusters

Cluster Manager (Java Console) from previous VCS versions cannot be used to manage VCS 5.0 clusters. Symantec recommends using the latest version of Cluster Manager.

See the *Veritas Cluster Server Installation Guide* for instructions on upgrading Cluster Manager.

Run Java Console on a non-cluster system

Symantec recommends not running Cluster Manager (Java Console) for an extended period on a system in the cluster. The Solaris version of the Java Virtual Machine has a memory leak that can gradually consume the host system's swap space. This leak does not occur on Windows systems.

Cluster Manager and wizards do not work if the hosts file contains IPv6 entries

VCS Cluster Manager and Wizards fail to connect to the VCS engine if the /etc/hosts file contains IPv6 entries.

Workaround: Remove IPv6 entries from the /etc/hosts file.

VCS Simulator does not support I/O fencing

When running the Simulator, be sure the UseFence attribute is set to the default, "None."

Undocumented commands, command options, and libraries

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

VCS documentation

The software disc contains the documentation for VCS in Portable Document Format (PDF) in the *cluster_server*/docs directory.

You can access the VCS 5.0 MP3 documentation online at the following URL:

http://www.symantec.com/business/support/overview.jsp?pid=15107

VCS documentation set

Table 1-7 lists the documents that VCS includes.

Table 1-7   VCS documentation

Title	File name
Veritas Cluster Server Installation Guide	vcs_install.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 DB2 Installation and Configuration Guide	vcs_db2_install.pdf
Veritas Cluster Server Agent for Oracle Installation and Configuration Guide	vcs_oracle_install.pdf
Veritas Cluster Server Agent for Sybase Installation and Configuration Guide	vcs_sybase_install.pdf

lists the documentation for the VCS component - Symantec Product Authentication Service.

Table 1-8   Documentation for VCS components

Title	File name
Symantec Product Authentication Service Installation Guide	at_install.pdf
Symantec Product Authentication Service Administrator's Guide	at_admin.pdf

VCS manual pages

The manual pages for the VRTSllt, VRTSgab, and VRTSvcs are installed in /opt/VRTS/man. Set the MANPATH environment variable so the man(1) command can point to the VCS manual pages.

For Bourne or Korn shell (sh or ksh), type:

```
MANPATH=$MANPATH:/opt/VRTS/man
  export MANPATH
```

For C shell (csh or tcsh), type:

```
setenv MANPATH ${MANPATH}:/opt/VRTS/man
```

For more information, refer to the man(1) manual page.

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 document version (located on the second page), and chapter and section titles of the text on which you are reporting.