Veritas™ Cluster Server Release Notes

HP-UX

5.0 Maintenance Pack 2

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: 5.0 MP2

Document version: 5.0MP2.0

Legal Notice

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

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:

http://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

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.

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	contractsadmin@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.

Veritas Cluster Server Release Notes

Introduction

This document provides important information about Veritas Cluster Server (VCS) version 5.0 Maintenance Pack 2 for HP-UX 11i v2. Review this entire document before you install or upgrade VCS.

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

http://entsupport.symantec.com/docs/319349

Changes introduced in this release

This section lists the changes introduced in this release of VCS.

DNS agent supports A, AAAA records with corresponding PTR records

The DNS agent now updates and monitors the host name to IP address (A, AAAA, and PTR records) in addition to the canonical name (CNAME) mapping for a DNS zone when failing over nodes across subnets.

Review details on the DNS agent.

See "DNS agent" on page 58.

VCS agent for Oracle supports Oracle 11g

The VCS Agent for Oracle now supports Oracle 11g R1.

See "About VCS agents" on page 20.

VCS Management Console 5.5

This release includes Veritas Cluster Server (VCS) Management Console 5.5. VCS Management Console was earlier known as Cluster Management Console. VCS Management Console 5.5 can manage VCS 5.0 MP2 clusters using direct connection.

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 5.5, see http://seer.entsupport.symantec.com/docs/308405.htm

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

New attribute added to DiskGroup agent

A new attribute UmountVolumes has been added to the DiskGroup agent. The details of this attribute are:

Attribute	Description
UmountVolumes	This attribute enables the DiskGroup resource to forcefully go offline even if open volumes are mounted outside of VCS control. When the value of this attribute is 1 and the disk group has open volumes, the following occurs: ■ The agent attempts to unmount the file systems on open volumes. If required, the agent attempts to kill all VCS managed and un-managed applications using the file systems on those open volumes. ■ The agent attempts to forcefully unmount the file systems to close the volumes. Type and dimension: integer-scalar Default: 0

The resource type definition for the DiskGroup agent is as follows:

```
type DiskGroup (
    static keylist SupportedActions = { "license.vfd", "disk.vfd",
    numdisks }
    static int NumThreads = 1
    static int OnlineRetryLimit = 1
    static str ArgList[] = { DiskGroup, StartVolumes, StopVolumes,
    MonitorOnly, MonitorReservation, tempUseFence,
    PanicSystemOnDGLoss, UmountVolumes }
    str DiskGroup
    str StartVolumes = 1
    str StopVolumes = 1
    boolean MonitorReservation = 0
    temp str tempUseFence = INVALID
    boolean PanicSystemOnDGLoss = 1
    boolean UmountVolumes = 0
)
```

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

Changes introduced in previous releases

The section describes changes in previous releases of VCS.

Changes introduced in VCS 5.0 MP1

This section lists the changes in the 5.0 MP1 release of VCS.

Host and node name expansion on HP-UX

The HP-UX Node and Host Name Expansion feature is supported on Symantec products. Install the NodeHostNameXpnd product bundle to enable this feature. This product bundle enables the capability to create node and host names of up to 255 bytes. Installation of this product bundle does not automatically activate 255 byte length support for node and host names. The default OS configuration will still be 8 bytes for node names and 64 bytes for host names. 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
```

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, the string size is limited to 1024 characters.

The user can enter a password of maximum 255 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. [702597]

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

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`.

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.

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

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.

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 either raw or 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 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 23.

Changes to licensing for VCS

VCS now follows the licensing scheme that is described below:

License	What’s included
VCS	■ VCS ■ Cluster Management Console ■ Database agents ■ Application agents ■ Virtual fire drill support

License	What's included
VCS HA/DR	■ 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

- 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 Sybase agent

The Veritas High Availability Agent for Sybase agent supports Sybase ASE 12.5.x and 15 on AIX, HP-UX, Linux, and Solaris.

Updates to the Oracle agent

- 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.

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 Agent Reference Guide*.

The Veritas High Availability Agent Pack gives you access to agents that provide high availability for third-party storage solutions. It is re-released regularly to add new agents. 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 also provides agents to manage key enterprise applications. This section lists the agents for enterprise applications and the software that the agents support.

Note: Before configuring an enterprise agent with VCS, verify that you have a supported version of the agent.

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

Agent	Agent version	VCS Version		Application		OS
		4.1	5.0			11iv2
Oracle	5.0	p	s	Oracle	9*i*, 10g R1, 10g R2 11g R1	s
Sybase	5.0	p	s	Sybase Adaptive Server Enterprise	12.5.x, 15	s

s – supported configuration p – supported by previous version of the agent

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

http://www.symantec.com/business/products/agents_options.jsp?pcid=1019&pvid=20_1

Custom agents

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*.

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.

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. For information on SF Oracle RAC, see the *Veritas Storage Foundation™ for Oracle® RAC Release Notes*.

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 22.

See "Supported software" on page 22.

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 software

- June 2007 release of HP-UX 11i version 2.0 or later releases of version 2.0

  For each platform, Symantec recommends applying the latest HP-UX operating system patches available from HP.

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.

- Logical Volume Manager (LVM)
- HP File System (HFS)
- Veritas Volume Manager (VxVM) 3.5, 4.1, 5.0
- Veritas File System (VxFS) 3.5, 4.1, 5.0

Requirements for accessing Cluster Manager (Java Console)

Cluster Manager (Java Console)

The VCS Java Console requires a minimum of 256MB RAM and 1280x1024 display resolution. The color depth of the monitor must be at least 8-bit (256 colors), although 24-bit is recommended.

The minimum requirements for Windows clients are Pentium II, 300MHz, 256MB RAM, and 800x600 display resolution. (Symantec recommends a minimum of Pentium III, 400MHz, and 512MB RAM.) The color depth of the monitor must be at least 8-bit (256 colors), and the graphics card must be able to render 2D images.

No longer supported

Support is no longer provided for:

- 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.

Installation and upgrade notes

This section contains instructions for installing, upgrading, and removing VCS. Before you install or upgrade, make sure that ssh or rsh is set up for passwordless communication.

Topics included in this section are:

- VCS 5.0 MP2 patches
- Installing VCS 5.0 MP2
- About upgrading to VCS 5.0 MP2
- About supported upgrade paths
- Upgrading to VCS 5.0 MP2
- Performing a minimal downtime upgrade to VCS 5.0 MP2
- Upgrading the agents
- Upgrading the VCS Java Console
- Upgrading the VCS Simulator
- Removing VCS 5.0 MP2

VCS 5.0 MP2 patches

The VCS 5.0 MP2 release includes the following patches:

PHCO_38740	1.0	VRTS 5.0 MP1 RP2 VRTSvxfen Command Patch (MP2)
PHKL_38743	1.0	VRTS 5.0 MP1 RP2 VRTSvxfen Kernel Patch (MP2)
PHNE_38738	1.0	VRTS 5.0 MP1 RP2 VRTSgab Kernel Patch (MP2)
PHNE_38739	1.0	VRTS 5.0 MP1 RP2 VRTSllt Kernel patch (MP2)
PVCO_03797	1.0	VRTS 5.0 MP1 RP2 VRTSvcs/VRTSvcsag Command Patch (MP2)
Oracle agent patch		
PVCO_03798	1.0	VRTS 5.0 MP1 RP2 VRTSvcsor/VRTScsocw Command Patch (MP2)
Sybase agent patch		
PVCO_03799	1.0	VRTS 5.0 MP1 RP2 VRTSvcssy Command Patch (MP2)

Installing VCS 5.0 MP2

You can perform a fresh install of VCS 5.0 MP2 using the installvcs program. The installvcs program installs both the base version VCS 5.0 and the 5.0 MP2 patches.

See the *Veritas Cluster Server 5.0 Installation Guide* for step-by-step instructions on using the installvcs program.

About upgrading to VCS 5.0 MP2

If you are currently running a cluster with any earlier VCS versions that is supported for upgrade, you can upgrade to VCS 5.0 MP2.

See "About supported upgrade paths" on page 25.

See "Upgrading to VCS 5.0 MP2" on page 25.

You can perform a minimal-downtime upgrade to minimize the downtime for your system.

See "Performing a minimal downtime upgrade to VCS 5.0 MP2" on page 27.

See "Upgrading the agents" on page 30.

See "Upgrading the VCS Java Console" on page 33.

See "Upgrading the VCS Simulator" on page 33.

About supported upgrade paths

Table 1-1 lists the supported upgrade paths.

Table 1-1 Supported upgrade paths

From	To	Upgrade program to use
VCS 4.1 and VCS 4.1 MP2	VCS 5.0 MP2	installvcs
VCS 5.0 and VCS 5.0 MP1	VCS 5.0 MP2	installmp

Upgrading to VCS 5.0 MP2

If you are currently running a VCS cluster, you can run the installer to upgrade to VCS 5.0 MP2. Depending on the upgrade path, you must either use the installvcs program or the installmp program.

See "About supported upgrade paths" on page 25.

Required HP-UX patches

Before upgrading to VCS 5.0 MP2, install the following HP-UX patches on each node:

PHSS_37958	LIBCL patch Required for HP-UX (PA) and HP-UX (IA) systems
PHCO_38526	Aries cumulative patch Required for HP-UX (PA) and HP-UX (IA) systems

These patches are available on HP IT resource center (www.itrc.hp.com).

Before upgrading to VCS 5.0 MP2, Symantec recommends that you take a backup of the types.cf and main.cf configuration files.

Stop the application agents that are installed on the VxVM disk (example, NBU agent). Perform the following steps to stop the application agents.

To stop the application agents

1 Take the resources offline on all systems that you want to upgrade.

```
# hares -offline resname -sys sysname
```

2 Stop the application agents that are installed on VxVM disk on all the systems.

```
# haagent -stop AgentName -sys sysname
```

3 Ensure that the agent processes are not running.

```
# ps -ef | grep Agent
```

This command does not list any processes in the VxVM mount directory.

To upgrade to VCS 5.0 MP2

1 Log in as superuser on one of the systems for installation.

2 Insert the disc containing the 5.0 MP2 software into the disc drive of one of the cluster nodes.

3 Mount the disc on a suitable mount point.

4 Navigate to the folder containing the upgrade program and start the upgrade program:

- If you are upgrading from VCS 4.1 or VCS 4.0 MP2, run the following program:

```
# ./installmp [-rsh]
```

- If you are upgrading from VCS 5.0 or VCS 5.0 MP1, run the following program:

```
# ./installvcs [-rsh]
```

5. Make sure that you have saved any changes to your configuration.

   ```
   # haconf -dump -makero
   ```

6. After the initial system checks and the requirements checks are complete, press **Return** to start upgrading the depots.

7. When the installation is complete, note the locations of the summary, log, and response files indicated by the installer.

8. Perform the following steps only if you are upgrading using installmp program:

   - Update the types.cf file to the new version.

     ```
     # cp -p /etc/VRTSvcs/conf/config/types.cf \
     /etc/VRTSvcs/conf/config/types.cf.orig
     # cp -p /etc/VRTSvcs/conf/types.cf \
     /etc/VRTSvcs/conf/config/types.cf
     ```

   - If you had added custom type definitions in the original types.cf file, you must add them to the new types.cf file.

9. Update the main.cf file to configure resources affected by the upgrade. See "Changes introduced in this release" on page 8.

10. Execute the following command to restart your systems:

    ```
    # /usr/sbin/shutdown -r now
    ```

Performing a minimal downtime upgrade to VCS 5.0 MP2

You can perform a minimal downtime upgrade in the following phases:

- Select a group of one or more cluster nodes as a standby node to upgrade and leave a group of one or more nodes running.
- Upgrade the standby node as follows:
  - Switch over the service group to the nodes that are running.
  - Freeze service group operations and stop VCS on the standby nodes.
  - Install the maintenance patch.
  - Restart the cluster services.
  - Switch back the service group to the upgraded nodes.
- Upgrade the remaining nodes in the second group.

To perform a minimal downtime upgrade

If you do not have the fencing module configured on your cluster, ignore all commands related to fencing in this procedure.

1. Select a node (or a group of nodes) in the cluster as the standby node.

2. Backup llttab, llthosts, gabtab, types.cf, and main.cf files.

```
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.bkp
```

3 Run the following command to stop VCS.

```
# /sbin/init.d/vcs stop
```

4 If fencing is configured, stop fencing using following command:

```
# /sbin/init.d/vxfen stop
```

5 Stop gab.

```
# /sbin/gabconfig -U
```

6 Stop llt.

```
# /sbin/lltconfig -Uo
```

7 Install VCS 5.0 MP2 using the installmp script:

```
# ./installmp [-rsh]
```

8 Update the types.cf file to the new version.

```
# cp -p /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.orig
# cp -p /etc/VRTSvcs/conf/types.cf \
/etc/VRTSvcs/conf/config/types.cf
```

9 If you had added custom type definitions in the original types.cf file, you must add them to the new types.cf file.

10 After the initial system checks and the requirements checks are complete, press **Return** to start upgrading the depots.

11 When the installation is complete, note the locations of the summary, log, and response files indicated by the installer.

Do not start the GAB and LLT processes. Do not start any VCS processes at this time.

12 Restore the copied llttab, llthosts and gabtab files.

```
# cp /etc/llttab.bkp   /etc/llttab
# cp /etc/llthosts.bkp /etc/llthosts
# cp /etc/gabtab.bkp   /etc/gabtab
# cp /etc/VRTSvcs/conf/config/main.cf.bkp \
/etc/VRTSvcs/conf/config/main.cf
```

13 Edit the main.cf file to configure new attributes.

14 Change the cluster ID in /etc/llttab file.

Find the line containing "set-cluster" and change the cluster ID following this keyword. Make sure that the new cluster ID is unique within the LAN.

15 Edit the main.cf file to freeze all the groups.

Add the "Frozen = 1" line to all group definitions.

Example:

If original group definition is

```
Group oracle_sg (
    SystemList = { North = 0, South = 1 }
    AutoStartList = { North, South }
```

The new group definition, after adding "Frozen = 1", should be:

```
Group oracle_sg (
    SystemList = { North = 0, South = 1 }
    AutoStartList = { North, South }
    Frozen = 1
```

16 Start all VCS components:

```
# /sbin/init.d/llt start
# /sbin/init.d/gab start
# /sbin/gabconfig -cx
# /sbin/init.d/vxfen start
# /sbin/init.d/vcs start
```

17 Perform the above procedure on each node (or set of nodes), until you reach the last node (or set of nodes) in the cluster.

18 If you are left with the last node or nodes in the cluster, stop VCS components on that node:

```
# /opt/VRTSvcs/bin/hastop -local
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# /sbin/lltconfig -Uo
```

19 Unfreeze and bring all services groups online in the new upgraded cluster. On the upgraded node, run the following commands:

- Open the configuration so that changes can be made to it:

  ```
  # /opt/VRTSvcs/bin/haconf -makerw
  ```

- For each group in main.cf, run the following commands:

  ```
  # /opt/VRTSvcs/bin/hagrp -unfreeze groupname -persistent
  # /opt/VRTSvcs/bin/hagrp -online groupname -sys sysname
  ```

- Finally, save the configuration using the following command:

  ```
  # /opt/VRTSvcs/bin/haconf -dump -makero
  ```

20 Upgrade the last node or group of nodes in the cluster.

21 Modify the `/etc/llttab` file and provide the cluster ID for the new cluster.

22 Start all VCS components on the last nodes that were upgraded.

```
# /sbin/init.d/llt start
# /sbin/init.d/gab start
# /sbin/init.d/vcs start
# /sbin/init.d/vxfen start
```

Upgrading the agents

The installvcs program does not upgrade the VCS agents for Oracle and Sybase. If previous versions of these agents are installed on your cluster, you must upgrade these agents manually.

For information on supported agent versions, see "About VCS agents" on page 20.

The following table lists the high-level procedure to upgrade the agents to version 5.0 MP2.

Table 1-2 Upgrade procedure for agents

Upgrade agent from version	To version	Procedure
-	5.0 MP2 (Fresh install)	Install the agents using the 5.0 MP2 disc. Follow the procedure for installing the agent mentioned in the agent installation guide. ■ See the *Veritas™Cluster Server Agent 5.0 for Oracle Installation and Configuration Guide* ■ See the *Veritas™Cluster Server Agent 5.0 for Sybase Installation and Configuration Guide*
4.1	5.0 MP2	■ Remove the previous version of the agent. Follow the procedure for removing the agent mentioned in the agent installation guide. - See the *Veritas Cluster Server Enterprise Agent 4.1 for Oracle Installation and Configuration Guide* - See the *Veritas Cluster Server Enterprise Agent 4.1 for Sybase Installation and Configuration Guide* ■ Install the 5.0 MP2 version of the agent. - See the *Veritas™Cluster Server Agent 5.0 for Oracle Installation and Configuration Guide* - See the *Veritas™Cluster Server Agent 5.0 for Sybase Installation and Configuration Guide*
5.0 and 5.0 MP1	5.0 MP2	See "Upgrading the Oracle agent from 5.0 or 5.0 MP1 to 5.0 MP2" on page 31. See "Upgrading the Sybase agent from 5.0 or 5.0 MP1 to 5.0 MP2" on page 32.

Upgrading the Oracle agent from 5.0 or 5.0 MP1 to 5.0 MP2

Perform the following steps on all the nodes in the cluster.

To upgrade the Oracle agent

1 Ensure that "/opt/VRTS/bin" directory is included in your PATH environment variable so you can execute all the VCS commands. Refer to *Veritas Cluster Server Installation Guide* for more information.

2 Verify that the version of VRTSvcs is 5.0 MP1 for HP-UX 11i v2.

3 Freeze all the service groups persistently.

```
# haconf -makerw
# hagrp -freeze group -persistent
# haconf -dump -makero
```

4 Stop the cluster on all nodes. If the cluster is writable, you can close the configuration before stopping the cluster.

```
# haconf -dump -makero
```

5 From any node, execute the following command.

```
# hastop -all
```

or

```
# hastop -all -force
```

6 Verify that the cluster is stopped on all nodes by running the `ha` command.

```
# hasys -state
```

7 On all nodes, make sure that both had and hashadow processes are stopped. In addition, stop the VCS CmdServer on all nodes.

```
# CmdServer -stop
```

8 Use the swinstall command to install the patch on each node in the cluster:

```
# cd patch_location
# swinstall -s `pwd` PVCO_03798
```

9 Verify that the 5.0 MP2 patch has been installed.

```
# swlist | grep PVCO_03798
```

The following information is displayed after successful patch installation:

```
PVCO_03798   1.0    VRTS 5.0 MP1 RP2 VRTSvcsor/VRTScsocw Command
Patch(MP2)
```

10 Start the cluster services on all cluster nodes. First, start VCS on one node:

```
# hastart
```

11 Start VCS on all the other nodes by running the `hastart` command after the first node goes to LOCAL_BUILD or RUNNING state.

12 Unfreeze all the groups.

```
# haconf -makerw
# hagrp -unfreeze group -persistent
# haconf -dump -makero
```

Upgrading the Sybase agent from 5.0 or 5.0 MP1 to 5.0 MP2

Perform the following steps on all the nodes in the cluster.

To upgrade the Sybase agent

1. Ensure that "/opt/VRTS/bin" directory is included in your PATH environment variable so you can execute all the VCS commands. Refer to *Veritas Cluster Server Installation Guide* for more information.
2. Verify that the version of VRTSvcs is 5.0 MP1 for HP-UX 11i v2.
3. Freeze all the service groups persistently.

   ```
   # haconf -makerw
   # hagrp -freeze group -persistent
   # haconf -dump -makero
   ```
4. Stop the cluster on all nodes. If the cluster is writable, you can close the configuration before stopping the cluster.

   ```
   # haconf -dump -makero
   ```
5. From any node, execute the following command.

   ```
   # hastop -all
   ```
   or

   ```
   # hastop -all -force
   ```
6. Verify that the cluster is stopped on all nodes by running the `ha` command.

   ```
   # hasys -state
   ```
7. On all nodes, make sure that both had and hashadow processes are stopped. In addition, stop the VCS CmdServer on all nodes.

   ```
   # CmdServer -stop
   ```
8. Use the swinstall command to install the patch on each node in the cluster:

   ```
   # cd patch_location
   # swinstall -s `pwd` PVCO_03799
   ```
9. Verify that the 5.0 MP2 patch has been installed.

   ```
   # swlist | grep PVCO_03799
   ```
   The following information is displayed after successful patch installation:

   ```
   PVCO_03799 1.0     VRTS 5.0 MP1 RP2 VRTSvcssy Command Patch(MP2)
   ```
10. Start the cluster services on all cluster nodes. First, start VCS on one node:

    ```
    # hastart
    ```
11. Start VCS on all the other nodes by running the `hastart` command after the first node goes to LOCAL_BUILD or RUNNING state.
12. Unfreeze all the groups.

    ```
    # haconf -makerw
    # hagrp -unfreeze group -persistent
    # haconf -dump -makero
    ```

Upgrading the VCS Java Console

This release includes updates for Cluster Manager (Java Console).

To upgrade the Java Console on a Windows client

1. Stop Cluster Manager if it is running.
2. Remove Cluster Manager from the system.
3. Insert the software disc into a drive on your Windows system.
4. Start the installer from the following path:
   \windows\VCSWindowsInstallers\ClusterManager\EN\setup.exe
5. Follow the wizard instructions to complete the installation.

Upgrading the VCS Simulator

This release includes updates for VCS Simulator.

To upgrade VCS Simulator on a Windows client

1. Stop all instances of VCS Simulator.
2. Stop VCS Simulator, if it is running.
3. Remove VCS Simulator from the system.
4. Insert the software disc into a drive on your Windows system.
5. Start the installer from the following path:
   \windows\VCSWindowsInstallers\Simulator \EN\vrtsvcssim.msi
6. Follow the wizard instructions to complete the installation.

Removing VCS 5.0 MP2

This section describes the procedure to manually remove VCS 5.0 MP2 packages from your cluster.

The following table lists the VCS version that is restored on the cluster after removing the VCS 5.0 MP2 packages.

Upgraded from	VCS version restored after uninstallation
VCS 4.1 and VCS 4.1 MP2 to VCS 5.0 MP2	VCS 5.0
VCS 5.0 to VCS 5.0 MP2	VCS 5.0
VCS 5.0 MP1 to VCS 5.0 MP2	VCS 5.0 MP1

To remove VCS 5.0 MP2

1. List the service groups in your cluster along with their status. On any node, type:

   ```
   # hagrp -state
   ```

2. Take the ClusterService group offline if it is configured.

   ```
   # hagrp -offline -force ClusterService -sys system
   ```

3. Make the VCS configuration writable. On any node, type:

   ```
   # haconf -makerw
   ```

4. Freeze all service groups. On any node, type:

   ```
   # hagrp -freeze service_group -persistent
   ```

   where service_group is the name of the service group.

   Note that the ClusterService group cannot be frozen.

5. Save the configuration (main.cf) file with the groups frozen. On any node, type:

   ```
   # haconf -dump -makero
   ```

6. Take a backup of the current main.cf and all types.cf configuration files.

   For example, on one of the nodes in the cluster, type:

   ```
   # cp /etc/VRTSvcs/conf/config/main.cf
   /etc/VRTSvcs/conf/main.cf.save
   # cp /etc/VRTSvcs/conf/config/types.cf
   /etc/VRTSvcs/conf/types.cf.save
   ```

7. Shut down VCS and the VCS CmdServer. On any node, type:

   ```
   # hastop -all -force
   # CmdServer -stop
   ```

8. Verify that VCS has shut down. On each node, type:

   ```
   # gabconfig -a
   ```

   The output resembles

   ```
   GAB Port Memberships
   Port a gen 23dc0001 membership 01
   ```

   Note that the output shows no membership for port h.

9. Stop vxfen on each cluster node, if the VCS cluster uses the fencing option.

   ```
   # vxfenconfig -U
   ```

10. Unconfigure GAB. On each node, type:

    ```
    # gabconfig -U
    ```

11. Unconfigure LLT. On each node, type:

    ```
    # lltconfig -Uo
    ```

12. Remove the VCS 5.0 MP2 patches from each node in the cluster.

    Type the following command:

    ```
    # swremove -x autoreboot=true  PHCO_38740  PHKL_38743
    PHNE_38738  PHNE_38739  PVCO_03797
    ```

13 Restore the types.cf configuration files from the location where you saved them, or manually edit the /etc/VRTSvcs/conf/config/types.cf to remove the newly added attributes.

14 Restart all the nodes in the cluster.

```
# shutdown -ry now
```

15 After VCS has started, perform the following steps:

a Verify all resources have been probed. On each node, type:

```
# hastatus -summary
```

b Unfreeze all service groups. On any node, type:

```
# haconf -makerw
# hagrp -unfreeze service_group -persistent
# haconf -dump -makero
```

where service_group is the name of the service group.

c Bring the ClusterService group online, if necessary. On any node type:

```
# hagrp -online ClusterService -sys system
```

where system is the system name.

Removing the 5.0 MP2 Oracle agent patch

Perform the following steps to remove the Oracle agent patch.

To remove the Oracle agent patch

1 Make sure that VCS is not running in the cluster.

```
# hastop -all
```

or

```
# hastop -all -force
```

2 Remove the patch from each node using the swremove command:

```
# swremove PVCO_03798
```

3 Verify that the patch has been removed from each node.

```
# swlist | grep PVCO_03798
```

The patch number PVCO_03798 should not be displayed, which confirms that the Oracle agent patch is removed.

Removing the 5.0 MP2 Sybase agent patch

Perform the following steps to remove the Sybase agent patch.

To remove the Sybase agent patch

1 Make sure that VCS is not running in the cluster.

```
# hastop -all
```

or

```
# hastop -all -force
```

2 Remove the patch from each node using the swremove command:

```
# swremove PVCO_03799
```

3 Verify that the patch has been removed from each node.

```
# swlist | grep PVCO_03799
```

The patch number PVCO_03799 should not be displayed, which confirms that the Sybase agent patch is removed.

Fixed issues

Refer to the following sections for information about:

- Issues fixed in VCS 5.0 MP2
- Issues fixed in VCS 5.0 MP1
- Issues fixed in VCS 5.0

Issues fixed in VCS 5.0 MP2

The following incidents have been fixed in this release.

Table 1-3 Fixed issues

Issue	Description
248532	Issue with offline local group dependencies.
612587	The `haclus -wait` command hangs when the cluster name is not specified.
797703	The output of the `vxfenadm` command with -d option had unwanted "^ M" character attached to the RFSM state information of all nodes.
805121	Partial groups go online erroneously if you kill and restart the VCS engine.
834240	Lock order violation in the agent framework causes deadlock in agent.
834496	The hacf -verify command fails if the IP address is specified.
837563	Oracle agent dumps core on HP-UX PA-RISC architecture.
857159	The gcoconfig command assigns priority 0 to all nodes.
862507	GAB_F_SEQBUSY is being set even when the sequence request is not sent.
866690	RemoteGroup agent dumps core on a secure cluster.

Table 1-3 Fixed issues

Issue	Description
914752	LLT messages fill dmesg buffer.
929570	Sybase and SybaseBk agents dump core.
970396	For LLT, reduce peer inactivity time using the request heartbeat mechanism.
990610	`vxfentsthdw` script issues with -f option and documentation for -d option.
1011472	Memory leaks in Oracle and Netlsnr agents.
1020838	Clean entry point of the Application agent does not work for "wac" type of configuration.
1031514	For LLT, add heuristic to deal with one-way link situations.
1036780	'haclus' dumps core.
1038373	LLT caused panic while communicating.
1057465	vxfentsthdw -f option rcp output.
1060657	GAB panics the system.
1060963	NFSRestart monitor gives the following error, "Too many open files".
1073342	Memory leak in llt_recv_msg().
1074605	System panics with "vxfen critical" as the panic string.
1078230	Error in the script \"/opt/VRTSvcs/vxfen/bin/vxfentsthdw\" is resolved.
1084656	GAB panics with string "Fault when executing in kernel mode".
1091284	Bug in printing port latency statistics.
1096394	VCS engine dumps core when Notifier resource is configured.
1101634	Issues with MultiNICA agent on HP-UX.
1102457	Unresolved kernel interruption during vxfen startup.
1104213	Reject 'hagrp -freeze' if service group is in a transition state (Online to offline or vice versa).
1113667	Use of vfork causes a deadlock between parent and child processes.
1113791	vxfenconfig ERROR V-11-2-1002 Open failed for device: /dev/vxfen.
1117839	DNS group goes to a partial state after killing the DNS agent.

Table 1-3 Fixed issues

Issue	Description
1120189	Stopping VXFEN .... FAIL * during shutdown.
1120697	GCO ICMP heartbeat AYATimeout value does not default to 300.
1137118	The fencing driver retries startup for some time before deciding on a pre-existing split brain.
1161339	Application agent does not inherit user defined LANG parameter.
1170248	Mount agent uses statvfs instead of using statvfs64.
1174911	Group switch/failover logic does not complete if parent group gets autodisabled in between.
1186414	The `hastart` command and the triggers run on the locale specified by the LANG variable.
1187580	ActionTimeout attribute does not function as expected.
1195685	After a split brain, the node of the surviving cluster panics.
1201174	VCS engine dumps core in VCSMutexDestroy.
1203620	For the Oracle agent, after setting "AutoEndBkup" to 1, the backup process actually did not end.
1204594	GAB takes longer time than expected time for membership in cross link.
1206153	DNS agent multiple problems on VCS 5.0 MP1.
1210437	VCS engine dumps core after running the `hares -flushinfo` command on CVMVolDg or CFSMount resources.
1250544	MultiNICB agent on HP-UX reports false failures on multiple APA interfaces.
1271764	Health check monitoring does not work when the oracle owner's shell is set to csh.
1282209	Output from action entry point is not always visible to the caller.
1285122	Race condition for MSG_RES_DELETE followed by MSG_RES_ADD.
1296465	Unable to failover Service Group to secondary site.
1296972	CFSMount agent failure during failover tests.
1397692	VCS engine clients hang in connect() if the target node is down.

Issues fixed in VCS 5.0 MP1

The following issues were fixed in this release.

Table 1-4 Fixed issues

Issue	Description
784335	The Oracle agent cannot identify the shell when the /etc/passwd file has multiple occurrence of the $Owner string.
702597	VCS ignores the value of the cluster-level attribute EngineShutdown while the system is shutting down.
702594	The Oracle agent does export SHLIB_PATH and other environment in CSH.
646372	The `hatype -modify` ... `-delete` ...command works incorrectly. The command deletes the first element of the keylist attribute.
627647	The Action entry point for Oracle fails because set_environment() function prototype differs.
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.
627564	VCS configuration wizards on HP-UX PA secure clusters fail to start.
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.
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.
619219	Running the hastart command twice causes an assertion to be displayed.
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.
616964	In a secure environment, the RemoteGroup agent does not authenticate on a remote host for the first time.
616652	The template for the NFS service has an incorrect definition for the NIC resource.

Table 1-4 Fixed issues

Issue	Description
616580	Importing resource types fails on Simulator on Windows systems.
614654	Change the unregister code path to do a combination of PREEMPT and then unregister.
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.
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.
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.
570992	Cluster Management Console does not display some icons properly.
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.
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.
243186	Assertion in VCS engine.

Issues fixed in VCS 5.0

The following issues were fixed in VCS 5.0.

Table 1-5 Fixed issues

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.

Table 1-5 Fixed issues

Issue	Description
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.”
926544	Mount Agent has a problem monitoring two Mount resources with the same mount point.
908910	NFSRestart agent entry points should not create lock files in /tmp directory. Create entry points in the $VCSLOG/lock directory.
861785	Issues with the creation of the fire drill service group.
848078	The nfs_postoffline trigger should not start the nfsd or mountd daemons if there is no NFS or NFSRestart agent in the service group.
805061	The VCS install program does not support e1000g NIC interface.
787222	Erroneous information in entry point output when zone name is larger than 11 characters.
620378	Complex group dependencies and timing issues leads to different failovers.
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.
418971	Cannot configure multiple Sybase servers with VCS.
393849	Performance issues with the Mount agent.
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.

Table 1-5 Fixed issues

Issue	Description
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 version of VCS.

- "Operational issues for VCS" on page 42
- "Issues related to the VCS engine" on page 44
- "Issues related to I/O fencing" on page 45
- "Issues related to global service groups" on page 46
- "Issues related to VCS bundled agents" on page 47
- "Issues related to the Oracle agent" on page 48
- "Issues related to Cluster Manager (Java Console)" on page 48
- "Issues related to Cluster Management Console" on page 49
- Issues related to VCS Simulator

Operational issues for VCS

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:

- More than one autostart group uses the same Prerequisites.

- One group, G2, is already online on a node outside of VCS control, and the other group, G1, is offline when VCS is started on the node.
- The offline group is probed before the online group is probed.

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

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

Trigger not invoked in REMOTE_BUILD state

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

The hagetcf script reports an error

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

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

Workaround: This message may be safely ignored.

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.

Installer terminates when “b” option is chosen while configuring VCS

Choose the ‘c’ option to configure VCS on 16-node cluster. While configuring VCS, if the ‘b’ option is chosen to go back, the installer is terminated. [615926]

Workaround: Do not choose the ‘b’ option.

Issues related to the VCS engine

Engine may hang in LEAVING state

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

state and hangs.
Workaround: Issue the command `hastop -local -force`.

Timing issues with AutoStart policy

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

Issues related to I/O fencing

The vxfen driver reports an error when stopping I/O fencing

If I/O fencing is started in disabled mode, and if you change the /etc/vxfenmode file later to scsi3, the vxfen driver throws the following spurious error when you stop vxfen:

```
ERROR: failed to stop vxfen
```

However, the actual I/O fencing stop operation is successful. [1301698, 1504943]

Workaround: This error message may be safely ignored.

Preexisting split brain after rebooting nodes

The fencing driver in 5.0 uses Veritas DMP to handle SCSI commands to the disk driver if fencing is configured in dmp mode. 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.

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

Workaround: This message may be safely ignored.

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
```

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 global service groups

Switch across clusters may cause concurrency violation

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

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

Global service group does not go online on AutoStart node

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

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

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

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

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

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

Issues related to VCS bundled agents

Extra definitions seen in types.cf

Extra definitions are seen in the types.cf for types HPVirtualMachine and HPVSwitch. These definitions can be ignored. [1460688]

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 Oracle agent

Intentional offline attribute has incorrect value in OracleTypes.cf

Workaround: Set the IntentionalOffline attribute to zero in the OracleTypes.cf [1465604]

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. Refer to the *Veritas High Availability 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.

Issues related to Cluster Manager (Java Console)

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.

Issues related to Cluster Management Console

The following issues apply to the version of Cluster Management Console that is bundled with VCS 5.0 MP2. Symantec recommends upgrading to the latest version of VCS Management Console. For information about VCS Management Console 5.5, see "VCS Management Console 5.5" on page 8.

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.

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.

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.

Uninstall of Cluster Connector in a secure cluster leaves the VxSS service group frozen

On UNIX, when you remove the cluster connector from a secure cluster, the VxSS service group is frozen. [619106]

Workaround: Manually unfreeze the VxSS group. Run the following commands.

```
/opt/VRTSvcs/bin/haconf -makerw
/opt/VRTSvcs/bin/hagrp -unfreeze VxSS -persistent
/opt/VRTSvcs/bin/haconf -dump -makero
```

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

Simulator clusters WIN_SQL_VVR_C1 and WIN_SQL_VVR_C2 fail to start

Simulator clusters WIN_SQL_VVR_C1 and WIN_SQL_VVR_C2 fail to start from the default configuration with the following error : [1529713]

```
V-16-1-49017 Simulator is already running on port '15550' for
cluster ' WIN_SQL_VVR_C1'
```

Workaround: Remove the following lines from the files /opt/VRTScssim/WIN_SQL_VVR_C1/conf/config/main.cf and /opt/VRTScssim/WIN_SQL_VVR_C2/conf/config/main.cf

```
include MSSearchTypes.cf
include RVGPrimaryTypes.cf
include SQLServer2000Types.cf
include VvrRvgTypes.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 env variable.

Documentation errata

This section adds or replaces content in the VCS 5.0 documents:

- Veritas Cluster Server User's Guide
- Veritas Cluster Server Bundled Agents Reference Guide
- Veritas Cluster Server Installation Guide
- Veritas High Availability Agent for Oracle Installation and Configuration Guide
- Veritas Cluster Server Agent Developer's Guide

Veritas Cluster Server User's Guide

Review the following additions or corrections to the *Veritas Cluster Server User's Guide* for 5.0:

User's Guide does not mention backward-compatibility of the Java Console

The VCS User's Guide does not mention the backward-compatibility of Cluster Manager (Java Console.) The console enables or disables features depending on whether the features are supported in the cluster that the console is connected to. For example, the Cluster Shell icon is grayed out when you connect to recent versions of VCS. But the icon is enabled when you connect to a pre-4.1 version of a VCS cluster. [641680]

Updated definition of the IntentOnline attribute

The definition of IntentOnline needs to be updated to include following information:

VCS sets IntentOnline attribute value to 2 for failover groups while VCS attempts to autostart a service group. Once the service group is online, VCS sets IntentOnline value to 1. [831858]

Veritas Cluster Server Centralized Management Guide

This information replaces the information in the *Veritas Cluster Server Centralized Management Guide* for 5.0. Numbers in parentheses indicate the page number of the Centralized Management Guide where this information appears.

Backing up the database

Backing up the database (page 158) is necessary so that crucial configuration and historical information can be recovered in the event of a failure. You can back up the database using the Cluster Management Console or the CLI. During the backup task, an archived copy of the database file and the associated transaction log file are backed up to a physically separate location. This location can be a tape drive or a disk drive. [703139]

To backup the database to a file

1. In the **Administration: Management Server Database** view, in the **Operations** task panel, click **Backup database to a file**.
2. In the **Enter a valid directory or tape drive on the server** dialog box, enter an existing directory path on the management server.

   If the directory path you specify does not exist, the database backup command does not create it.
3. Click **OK**.

To backup the database to a file using the command line

◆ `gadb -backup -to` *`archive`*

This command creates an archive backup file that contains both the database and transaction log. The database archive file is created in the directory path specified by *`archive`*. The database archive file name is of the form:

```
CCAvailDbBackUp@yyyy-mm-dd_hh_mi_ss.1
```

The timestamp portion is in GMT.

Creating custom reports

The section on accessing the database information contains references to $ms_host, which is a variable. Read $ms_host as *ms_host.*

When configuring ODBC, replace *ms_host.* with the name of the management server host. Do not include the $ sign in the host name.

Veritas Cluster Server Bundled Agents Reference Guide

Review the following additions or corrections to the *Veritas Cluster Server Bundled Agents Reference Guide* for 5.0:

LVMVolumeGroup agent

The guide incorrectly states that an LVMVolumeGroup resource depends on a DiskReservation resource. Ignore the dependency mentioned for LVMVolumeGroup agent on page 28. [1179518]

NFSRestart agent

Replace the sample configuration for the NFSRestart agent with the following one:

Basic NFSRestart configuration

```
include "types.cf"

cluster vcs_test (
        )

system sysA (
        )

system sysB (
        )

group NFSgrp1 (
        SystemList = { sysA = 0, sysB = 1 }
        AutoStartList = { sysA, sysB }
        )

        DiskGroup dg01 (
                DiskGroup = dg01
                StartVolumes = 0
                StopVolumes = 0
                )

        IP ip1 (
                Device = lan0
                Address = "11.123.175.11"
                NetMask = "255.255.248.0"
                )

        Mount Mount_dir1 (
                MountPoint = "/dir1"
                BlockDevice = "/dev/vx/dsk/dg01/vol01"
                FSType = vxfs
                MountOpt =
                "ioerror=mwdisable,largefiles,qio,delaylog"
                FsckOpt = "-n"
                )

        NFS nfs1 (
                Nservers = 8
                LockFileTimeout= 360
                )

        NFSRestart nfsres1 (
                LocksPathName = "/dir1"
                NFSLockFailOver = 1
                NFSRes = nfs1
                )

        NIC nic1 (
                Device = lan0
                NetworkHosts = {"11.123.170.107"}
                )

        Share Share_dir1 (
                PathName = "/dir1"
                )

        Volume dg01_vol01 (
                Volume = vol01
                DiskGroup = dg01
                )

ip1 requires nic1
        ip1 requires Share_dir1
        Mount_dir1 requires dg01_vol01
        nfsres1 requires ip1
        Share_dir1 requires Mount_dir1
        Share_dir1 requires nfs1
        dg01_vol01 requires dg01
```

DNS agent

This information replaces the information in the guide for the DNS agent.

The DNS agent updates and monitors the mapping for the following:

- the host name to IP address (A, AAAA, or PTR record)
- the canonical name (CNAME)

The agent performs these tasks for a DNS zone when failing over nodes across subnets (a wide-area failover). Resource records (RR) can include different types: A, AAAA, CNAME, name server, SOA, and PTR records.

Use the DNS agent when the failover source and target nodes are on different subnets. The agent updates the name server and allows clients to connect to the failed over instance of the application service.

Agent functions

Online — Sends a DNS query to retrieve the Start of Authority (SOA) record of the zone that the Domain agent attribute defines. The master server's name is in the SOA field. Unless you define the StealthMasters attribute, it is the only server for the update. When you define the StealthMasters attribute, only the servers that the attribute defines are updated.

The agent creates PTR records for each RR of type A or AAAA if the value of the CreatePTR attribute is true. A prerequisite for this feature is that the same master or stealth servers serve the forward (A or AAAA) and reverse zones.

Offline — If attribute OffDelRR is true, offline removes all records that the ResRecord keys define.

Monitor — Returns the ONLINE state if at least one name server reports all mappings that ResRecord defines. The name servers are the master or StealthMaster, and all the servers for which an NS record for the zone exists.

Clean — Removes the Online lock file, if it exists.

Open — Removes the Online lock file if the resource is reported online on another node inside the cluster to prevent concurrency violation. If the lock file exists, at least one name server has to report all the RRs that the ResRecord attribute defines. If one name server cannot report all the RRs, the agent function removes the Online lock file.

State definitions

ONLINE — All the RRs that one name server reports.

OFFLINE — Indicates an offline state when either of the following is true:

- The online lock does not exist.
- At least one server cannot report all of the RRs' mappings.

UNKNOWN — A problem exists with the configuration.

Attributes

Table 1-6 Required attributes

Required attribute	Description
Domain	A string representing the DNS zone that the agent administers. The domain name can only contain alphanumeric symbols and the dash. Type and dimension: string-scalar Examples: ■ “demo.symantec.com” (forward mapping) ■ “2.168.192.in-addr.arpa” (IPv4 reverse mapping)
ResRecord	An association of DNS resource record values. Each ResRecord attribute consists of two values: *DNS record key* = *DNS record data*. Note that the record key must be a unique value. Type and dimension: association-scalar Examples: ■ For forward mapping, where the zone is demo.symantec.com: - sles901 = “192.168.2.191” - ww2 = sles901 - sles9ip6 = “2007::1:2:3:abc” ■ For forward mapping, where the zone is demo.symantec.com. A multi-home DNS record, typically for one host with two network interfaces, different address, but the same DNS name. This results in two-A records, or a single A record with continuation lines. sle902 = “192.168.2.102 10.87.13.22" ■ For reverse IPv4 address mapping, where the zone is 2.168.192.in-addr.arpa: 191 = “sles901.demo.symantec.com” ■ For reverse IPv6 address mapping, where the zone is 3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.2.ip6.arpa: cba = “sles9ip6.demo.symantec.com”

Table 1-6 Required attributes

Required attribute	Description
ResRecord (continued)	The agent uses case-insensitive pattern matching—and a combination of the Domain and ResRecord attribute values—to determine the resource record type. The RR type is as follows: ■ PTR: if the Domain attribute ends with .arpa ■ A: if the record data field is four sets of numbers, where a space separates each set. The following details the pattern it tries to match: [*1-223*].[*0-255*].[*0-255*].[*0-255*] Hexadecimal is not supported. ■ AAAA: if the record data fields are in multiple sets of hexadecimal format, then this record is an IPv6 associated type AAAA record. ■ CNAME: for any other results. **Note:** If a name in the ResRecord attribute does not comply with RFC 1035, then a warning is issued to the log file. The ResRecord association is not used.

Table 1-7 Optional attributes

Optional attribute	Description
TTL	A non-zero integer represents the “Time To Live” value, in seconds, for the DNS entries in the zone that you want to update. A lower value means more hits on your DNS server, while a higher value means more time for your clients to learn about changes. The time-in-seconds value may take the value 0, which indicates never caching the record, to a maximum of 2,147,483,647, which is over 68 years! The current best practice recommendation (RFC 1912) proposes a value greater than one day, and on RRs that do not change often, consider multi-week values. Type and dimension: integer-scalar Default: 86400 Example: “3600”

Table 1-7 Optional attributes

Optional attribute	Description
StealthMasters	The list of primary master name servers in the domain. This attribute is optional since the first name server is retrieved from the zones SOA (Start of Authority) record. If the primary master name server is a stealth server, define this attribute. A stealth server is a name server that is authoritative for a zone, but does not appear in zone's SOA record. It is hidden to prevent direct attacks from the Internet. Type and dimension: string-keylist Example: { "10.190.112.23" }
TSIGKeyFile	Required when you configure DNS for secure updates. Specifies the absolute path to the file containing the private TSIG (Transaction Signature) key. Type and dimension: string-scalar Example: /var/tsig/Kexample.com.+157+00000.private
CreatePTR	Use the CreatePTR attribute to direct the online agent function to create PTR records for each RR of type A or AAAA. You must set the value of this attribute to true (1) to create the record. Before you can use this attribute, the same master or stealth servers must serve the forward (A or AAAA) and reverse zones. Type and dimension: boolean-scalar Default: 0 Example: 1
OffDelRR	Use the OffDelRR attribute to direct the offline agent function to remove all the records that the ResRecord key defines. You must set the value of this attribute to true (1) to have the agent remove all the records. The online agent function always adds records if they do not exist. Type and dimension: boolean-scalar Default: 0 Example: 1

Resource type definition

```
type DNS (
    static str ArgList[] = { Domain, TTL, TSIGKeyFile,
    StealthMasters, ResRecord, CreatePTR, OffDelRR }
    str Domain
    int TTL = 86400
    str StealthMasters[]
    str TSIGKeyFile
    str ResRecord{}
    boolean CreatePTR = 0
    boolean OffDelRR = 0
)
```

Monitor scenarios

Depending on the existence of the Online lock file and the defined Resource Records (RR), you get different status messages from the Monitor function.

Table 1-8 Monitor scenarios for the Online lock file

Online lock file exists	Expected RR mapping	Monitor returns
NO	N/A	OFFLINE
YES	NO	OFFLINE
YES	YES	ONLINE

Sample Web server configuration

Take the former Veritas corporate web server as an example. A person using a web browser specifies the URL www.veritas.com to view the Veritas Web page. Where www.veritas.com maps to the canonical name mtv.veritas.com, which is a host in Mountain View running the web server. The browser, in turn, retrieves the IP address for the web server by querying the domain name servers. If VCS fails the web server for www.veritas.com from Mountain View to Heathrow, the domain name servers must be updated with the new canonical name mapping. This update occurs so that the web browsers are directed to Heathrow instead of Mountain View. The DNS agent should update the name server to change the mapping of www.veritas.com. From mtv.veritas.com to the canonical name of the standby system in Heathrow, hro.veritas.com, in case of a failover.

Secure DNS update for BIND 9

The DNS agent expects that the zone's allow-update field contains the IP address for the hosts that can dynamically update the DNS records. This functionality is default for the DNS agent. Since a competent black hat can, however, spoof IP addresses, consider TSIG as an alternative.

TSIG (Transaction Signature) as specified in RFC 2845, is a shared key message authentication mechanism, which is available in DNS. A TSIG key provides the means to authenticate and verify the validity of exchanged DNS data. It uses a shared secret key between a resolver and either one or two servers to provide security.

Setting up secure updates using TSIG keys for BIND 9

In the following example, the domain is example.com.

To use secure updates using TSIG keys

1. Run the `dnssec-keygen` command with the HMAC-MD5 option to generate a pair of files that contain the TSIG key:

   ```
   # dnssec-keygen -a HMAC-MD5 -n HOST example.com.
       Kexample.com.+157+00000
   ```

2. Open the Kexample.com.+157+00000.key file. After you run the `cat` command, the contents of the file resembles:

   ```
   # cat Kexample.com.+157+00000.key
       example.com. IN KEY 512 3 157 +Cdjlkef9ZTSeixERZ433Q==
   ```

3. Copy the shared secret (the TSIG key), which looks like:

   ```
   +Cdjlkef9ZTSeixERZ433Q==
   ```

4. Configure the DNS server to only allow TSIG updates using the generated key. Open the named.conf file and add these lines.

   ```
   key example.com. {
       algorithm hmac-md5;
       secret "+Cdjlkef9ZTSeixERZ433Q==";
   };
   ```

   Where **+Cdjlkef9ZTSeixERZ433Q==** is the key.

5. In the named.conf file, edit the appropriate zone section and add the allow-updates sub-statement to reference the key:

   ```
   allow-update { key example.com. ; } ;
   ```

6. Save and restart the named process.

7. Place the files containing the keys on each of the nodes that is listed in your group's SystemList. The DNS agent uses this key to update the name server.

   Copy both the private and public key files on to the node. A good location is in the /var/tsig/ directory.

8 Set the TSIGKeyFile attribute for the DNS resource to specify the file containing the private key.

```
DNS www (
Domain = "example.com"
ResRecord = {www = north}
TSIGKeyFile a= "/var/tsig/Kexample.com.+157+00000.private"
)
```

Veritas Cluster Server Installation Guide

Review the following additions or corrections to the *Veritas Cluster Server Installation Guide* for 5.0:

Symantec Product Authentication Service 4.3.x required for cluster connector installation

You must install cluster connector from a system that has Symantec Product Authentication Service 4.3.x, or at least the authentication broker installed.

You can also install cluster connector from a cluster node, provided that you are installing cluster connector on nodes that are part of the same cluster. [611353]

Cluster connector must be taken offline before it is uninstalled

Ensure that you take the CMC service group offline before you uninstall cluster connector. Otherwise, cluster connector remains running even after you uninstall the cluster connector software. [796739]

To take the CMC service group offline on UNIX platforms

1 Obtain a command prompt on the management server host system.

2 Enter the following command:

```
/opt/VRTSvcs/bin/hagrp -offline CMC -sys
```

Replace sys with the name of the system that is running the CMC service group.

Replacing commands to start LLT and configure GAB

In the Installation Guide, in the Adding and removing cluster nodes chapter, on page 189, replace the command in step 3 with [629062]:

On the new system, run the command:

```
/sbin/init.d/llt start
```

On page 190, replace step 2 from the “To configure GAB” procedure with:

On the new node, run the command, to configure GAB:

```
/sbin/init.d/gab start
```

Corrections to csgnic definition in main.cf file

The sections Example main.cf, for clusters without the GCO option, on page 136 and Example main.cf for a centrally managed cluster using Cluster Management Console, on page 139 contain the following csgnic definition. [See Etrack incident 838660]

```
NIC csgnic (
    Device = lan0
        )
```

With this definition, the csgnic resource may fault intermittently. To overcome this issue, the NetworkHosts parameter must be provided.

Modify the csgnic definition to add NetworkHosts attribute. The sample configuration is as follows:

```
NIC csgnic (
    Device = lan0
    NetworkHosts = { "10.10.12.2", "10.10.12.3" }
    )
```

Veritas High Availability Agent for Oracle Installation and Configuration Guide

Review the following additions or corrections to the *Veritas High Availability Agent for Oracle Installation and Configuration Guide* for 5.0:

- On page 14, the command documented to invoke the Info entry point is not correct. Use the following command:

  ```
  hares -value resource ResourceInfo [system]\
  [-clus cluster | -localclus]
  ```

- On page 18, the description of IGNORE action is missing the following information:

  When the Veritas Agent for Oracle encounters an error that does not have a matching error code in the oraerror.dat file, then the agent ignores the error.

- The details in the Encrypting passwords section of the document is inadequate in the document. Refer to the following information:

  VCS provides a utility to encrypt database user passwords and listener passwords. You must encrypt the Pword attribute in the Oracle agent and the LsnrPwd attribute in the Netlsnr agent before configuring these attributes.

  Oracle provides the option of storing the listener password in the listener.ora file, in both clear text and encrypted formats. Irrespective of the format in which the password is stored in Oracle, you must encrypt the password using the vcsencrypt utility before configuring the LsnrPwd attribute.

If you encrypted the listener password using the Oracle lsnrctl utility, make sure that you pass the encrypted password to the vcsencrypt utility. You can find the Oracle lsnrctl encrypted password from the following line in the listener.ora file:

```
PASSWORDS_ENCRYPTED = XXXXXXXX
```

When the agent decrypts this password, the decrypted password for the listener must be of the same format as stored in the listener.ora file.

Veritas Cluster Server Agent Developer’s Guide

On page 91, the syntax for clean entry point is incomplete. The correct syntax is as follows:

```
clean resource_name ArgList_attribute_values clean_reason
```

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.

System names in VCS

Systems specified in the VCS configuration file, main.cf, and in the files /etc/nodename and /etc/llthosts, must be consistent. The names cannot include periods and thus must not be in the fully qualified form. If you create the file /etc/VRTSvcs/conf/sysname to contain system names used by main.cf, VCS uses the file to verify the names.

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.

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.

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.

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/profile
```

2 Restore the files:

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

Bundled agent limitations

RemoteGroup resource faults when the remote group is still online

The RemoteGroup agent does not work with parallel service groups.

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 do not support the IPv6 enhanced IP protocol.

VCS does not provide a bundled agent for volume sets

VCS 5.0 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

The following limitations apply to the version of Cluster Management Console that is bundled with VCS 5.0 MP2. Symantec recommends upgrading to the latest version of VCS Management Console. For information about VCS Management Console 5.5, see "VCS Management Console 5.5" on page 8.

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

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 5.0 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.

Documentation

Product guides are available on the documentation disc in PDF and HTML formats. We recommend copying pertinent information, such as installation guides and release notes, from the disc to your system directory /opt/VRTS/docs for reference.

VCS documentation set

VCS includes the following documents.

Title	File Name
Veritas Cluster Server 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

Title	File Name
Veritas Cluster Server Agent Developer's Guide	vcs_agent_dev.pdf
Veritas Cluster Server Centralized Management Guide	vcs_central_mg.pdf
Veritas High Availability Agent for Oracle Installation and Configuration Guide	vcs_oracle_install.pdf
Veritas High Availability Agent for Sybase Installation and Configuration Guide	vcs_sybase_install.pdf

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

Getting help

For technical assistance, visit
http://www.symantec.com/business/support/assistance_care.jsp

and select phone or email support. Select a product to use the Knowledge Base Search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and the customer email notification service. If you encounter an error when using a product, include the error number preceding the message when contacting Technical Services. You can also use the error number to search for information in TechNotes or documents on the website.