Veritas™ Cluster Server One Release Notes

AIX, HP-UX, Linux, Solaris

5.0

Veritas Cluster Server One 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

Document version: 5.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
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	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

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

Enterprise services that are available include the following:

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

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

www.symantec.com

Select your country or language from the site index.

Veritas Cluster Server One Release Notes

What's included

These release notes include the following topics:

Introduction

This document provides important information about Veritas™ Cluster Server One (VCS One) by Symantec for supported versions of AIX, HP-UX, Linux, and Solaris. Review this entire document before installing VCS One.

For the latest information about updates, patches, and software issues for this release, read the Late-Breaking News TechNote:

http://entsupport.symantec.com/docs/330554

Also, be sure to read the *Veritas Cluster Server One Getting Started Guide* and the *Veritas Cluster Server One Installation Guide* before you install.

Changes in this release

The sections that follow describe the changes in this release.

Terminology

The terminology for VCS One has changed. The term *server farm* is being deprecated, and replaced with the term *VCS One cluster*. Because the term *server farm* still appears in some places in the user interface, the documentation uses the terms *VCS One cluster* and *server farm* interchangeably. Both terms refer to the Policy Master and the collection of objects that the Policy Master manages.

Disaster recovery

Disaster recovery uses global clustering to provide protection against large-scale disasters such as major floods, hurricanes, and earthquakes that cause outages for an entire city or region. In such situations, you can use VCS One global clusters to facilitate data availability.

Replication agents

This release of VCS One supports the following replication agents: SRDF, HTC, and SVC. Future versions of VCS One and the Agent Pack will support additional replication agents.

Support for additional client operating systems

VCS One now supports installation of the client on SUSE Linux Enterprise Server (SLES) 11 and Red Hat Enterprise Linux 5 (RHEL 5).

See “Supported platforms and software for the Policy Master” on page 14 for details.

Usability enhancements

This release includes the following usability enhancements:

- Context sensitive menus. You can now right-click objects in tables to invoke operations in the context of the object.
- Batch operations. You can select multiple objects and perform operations—such as modifying the system list, or setting the resource fault policy—on all the objects at once.
- Partial page refresh. You can more quickly and easily perform tasks such as bringing a group online or taking a group offline because VCS One no longer refreshes an entire page each time the data on that page changes. In the current release, when data on a page changes, only the modified data refreshes.
- Enhanced resource dependency view. You can more quickly render graphs with a larger number of nodes and edges.

Simulator enhancements

The VCS One Simulator is now a self-extracting .exe file that you can install to a single directory. To remove the Simulator you need only delete the directory in which you installed it. You can run multiple instances of the Simulator simultaneously on the same system, from the same extracted directory. With multiple Simulator instances, you can now simulate a disaster recovery scenario.

Deprecated command

The `hadb -backupxml` command has been deprecated. This command has been replaced with `haconf -dbtoxml`. The `haconf -dbtoxml` command backs up the current active configuration database to the main.xml and types.xml files in the specified directory. Caution: The command overwrites existing files using the same names.

For details on these commands, see *Veritas Cluster Server One Command Reference Guide*.

Support for VMware ESX server virtualization technology

ESX is not supported in the current release, but will be available in the future.

Support for Windows clients

Windows clients are not supported in the current release, but will be available in the future.

Solaris projects

This release no longer supports Solaris projects.

New agent attributes

Symantec has introduced four new attributes—EPClass, EPPriority, OnlineClass, and OnlinePriority—to enable you to control the scheduling class and scheduling priority of the agent operations. Agent operations include online, offline and monitor.

For more information about these attributes, see *Veritas Cluster Server One User's Guide*.

SUSE Linux Enterprise Server 9 (SLES 9) support

This release no longer provides client support for SUSE Linux Enterprise Server 9 (SLES 9), SP3 x86 (32-bit) and x64 (64-bit).

Red Hat Enterprise Linux 4 (RHEL 4) support

This release no longer provides Policy Master support for Red Hat Enterprise Linux 4 (RHEL 4) x64. This version of VCS One supports RHEL 4 for the client.

About VCS One agents

This section describes the three types of VCS One agents:

- VCS One comes packaged (bundled) with platform-specific sets of agents that enable VCS One to provide high availability. These include agents for mount points, IP addresses, and file systems. After you install VCS One on a client system, these agents are available immediately.
  For more information about VCS One bundled agents, see the *Veritas Cluster Server One Bundled Agents Reference Guide*.
- Both VCS One and VCS also provide a set of agents that enable high availability for key enterprise applications for third-party products. These agents include the following:
  - Databases
  - Replication solutions

- Middleware solutions
- Enterprise applications

These agents are available in the Agent Pack, which is updated quarterly. The same Agent Pack applies to both VCS One and VCS. The Agent Pack is included with VCS One and available by downloading it.

For information on how to download the Agent Pack, see the following URL:

https://fileconnect.symantec.com

To download, you need to enter the serial number that is associated with your product.

Before you install and configure a VCS One agent for an enterprise application, check that you have the latest agent version. You may view the latest agent versions by clicking on the "Veritas Cluster Server Agents Support Matrix" link on this Web page:

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

For more information about VCS One agents for enterprise applications, see the individual agent's guide, the Agent Pack, or contact Symantec Consulting Services.

- To create custom agents for applications, contact Symantec consulting services or develop custom agents yourself. Creating custom agents requires knowledge of VCS One, scripting skills, and basic programming logic.
  For more information about creating VCS One agents, see the *Veritas Cluster Server One Agent Developer's Guide* or contact Symantec Consulting Services.
- This release notes document covers known issues and software limitations for the VCS One agents that ship with the 3Q2009 Agent Pack.

Licensing

VCS One is a licensed product. During installation, you will be required to select the appropriate license type for your installation.

Table 1-1 lists the VCS One license types.

Table 1-1 VCS One license types

VCS One license type	Description
Demo	A demo license, which entitles you to use the product for 30 days for evaluation purposes only. After one year, the product auto-disables high availability (HA) for the Policy Master and significantly reduces functionality.
NFR	A not-for-resale license, which is limited to one year. For use by Symantec partners and customers for stack certification and testing purposes. After one year, the product auto-disables high availability (HA) for the Policy Master and significantly reduces functionality.
Permanent	A permanent license.

VCS One provides three levels of functionality as described in Table 1-2. You can purchase and use the functionality level that meets your business needs.

Table 1-2 VCS One functionality levels

Functionality level	Provides	Features
VCS One Start	■ The ability to monitor, start, stop, and move applications	VCS One with all features enabled except: ■ Auto-failover ■ Priority-based application availability
VCS One HA	■ The ability to monitor, start, stop, and move applications ■ Failover capability within a local site	VCS One with all features enabled except failover across sites
VCS One HA/DR	■ The ability to monitor, start, stop, and move applications ■ Failover capability across sites	VCS One with all features enabled

Note: If you purchased VCS One Start, make sure that you set the GrpFaultPolicy and NodeFaultPolicy attributes to NoFailover for each service group you create when you create the group. For information about how to set these attributes when you create a service group, see the *Veritas Cluster Server One User's Guide*.

System requirements

This release of Veritas Cluster Server One supports the following hardware and operating systems.

Supported hardware

For information on supported hardware, see the hardware compatibility list (HCL) in the following TechNote. The hardware compatibility information for Veritas Storage Foundation and High Availability Solutions 5.0 MP1, MP2, and MP3 applies for VCS One:

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

System requirements

Table 1-3 Veritas Cluster Server One system requirements

System	Platform
Policy Master Cluster	■ Two to four Linux systems Systems running Opteron® or Extended Xeon® 64-bit processors (not Itanium®) OR ■ Two to four Solaris systems Sparc-based
Cluster systems	AIX, HP-UX, Linux, and Solaris-based systems

Policy Master configuration database storage requirements

The Policy Master cluster nodes require access to shared storage that will contain the Policy Master configuration database and associated files. This storage can be either SAN- or NFS-based.

The following requirements for each type of storage are mandatory. These requirements allow the VCS One I/O fencing feature to function correctly and ensure the integrity of the database through failure conditions.

SAN-based storage requirements

SAN-based storage must support SCSI-3 persistent reservations (PR).

NFS-based storage requirements

NFS-based storage must be served from a NetApp Filer. No other NFS server is approved or supported with this release of VCS One.

Supported platforms and software for the Policy Master

This section lists the supported platforms, Storage Foundation versions, and required patches for the Policy Master.

For more information, see:

- "Supported platforms"
- "Supported versions of Storage Foundation"
- "Required patches"

Supported platforms

Table 1-4 shows the operating systems and architectures supported by the VCS One Policy Master.

VCS One operates on subsequent kernel and patch releases provided the operating systems maintain kernel application binary interface (ABI) compatibility.

Table 1-4 Supported operating systems and architectures

Operating system	Architecture
Red Hat Enterprise Linux 5 (RHEL 5)	x64 (Intel Xeon, AMD Opteron)
Solaris 10 Update 3 and later	64-bit SPARC

Supported versions of Storage Foundation

Veritas Storage Foundation HA is installed with the VCS One Policy Master. Table 1-5 lists the Storage Foundation HA versions that are installed with the VCS One Policy Master.

Table 1-5 Storage Foundation HA versions installed with the Policy Master

Policy Master platform	Architecture	Storage Foundation version installed
Red Hat Enterprise Linux 5 (RHEL 5)	x64 (Intel Xeon, AMD Opteron)	Veritas Storage Foundation High Availability 5.0 MP3
Solaris 10 Update 3 and later	64-bit SPARC	Veritas Storage Foundation High Availability 5.0 MP3 RP1. The VCS One Policy Master also supports Veritas Storage Foundation High Availability 4.x, although it is not installed with the Policy Master.

Required patches

This section provides information about required patches for the Policy Master.

Linux

Ensure that the following required Linux patches are installed before installing the VCS One Policy Master on Linux operating systems.

Table 1-6 Required patches

Operating system	Required Linux patches	Where to download
Red Hat Enterprise Linux 5 (RHEL 5)	Authentication in VCS One requires the standard C++ version 5.0. You must install the following C++ compat library rpm before installing the VCS One Policy Master: compat-libstdc++-33-3.2.3-61.i386.rpm	You can obtain the compat libraries from the following URL: http://rpmfind.net/linux/RPM/System_Environment_Libraries.html

Solaris

Ensure that the following required Solaris patches are installed before installing the VCS One Policy Master on Solaris operating systems.

Table 1-7 Required patches

Operating system	Required Solaris patches	Where to download
Solaris 9 SPARC	111711-11 111712-11	Solaris patches may be downloaded from: http://www.sunsolve.sun.com
Solaris 10 SPARC	119254-53 (or later) 127111-11 (or later)	These patches are required by the VRTSvxvm package. Solaris patches may be downloaded from: http://www.sunsolve.sun.com
Solaris 10 x64	119964-05	Solaris patches may be downloaded from: http://www.sunsolve.sun.com

Supported platforms and software for the client

The VCS One client runs on Linux, Solaris, AIX, and HP-UX. This section lists the supported platforms, Storage Foundation versions, and HA Agent Pack version for the VCS One client.

For more information, see:

- "Supported platforms"
- "Supported versions of Storage Foundation"
- "Required patches"
- "Supported High Availability Agent Pack"

Supported platforms

The VCS One client runs on Linux, Solaris, AIX, and HP-UX.

VCS One operates on subsequent kernel and patch releases provided the operating systems maintain kernel application binary interface (ABI) compatibility.

Supported Linux platforms

Table 1-8 shows the Linux operating systems and architectures supported by the VCS One client.

Table 1-8 Supported Linux operating systems and architectures

Operating system	Architecture
Red Hat Enterprise Linux 4 (RHEL 4)	x86 (32-bit)
Red Hat Enterprise Linux 4 (RHEL 4)	x64 (Intel Xeon, AMD Opteron)
Red Hat Enterprise Linux 5 (RHEL 5)	x64 (Intel Xeon, AMD Opteron)
SUSE Linux Enterprise Server Linux 10, SP2	x64 (Intel Xeon, AMD Opteron)
SUSE Linux Enterprise Server Linux 11	x64 (Intel Xeon, AMD Opteron)

Supported Solaris platforms

Table 1-9 shows the Solaris operating systems and architectures supported by the VCS One client.

Table 1-9 Supported Solaris operating systems and architectures

Operating system	Architecture
Solaris 9	64-bit SPARC
Solaris 10 Update 3 and later	64-bit SPARC
Solaris 10 Update 3 and later	x64

Supported AIX platforms

Table 1-10 shows the AIX operating systems and architectures supported by the VCS One client.

Table 1-10 Supported AIX operating systems and architectures

Operating system	Architecture
AIX 5.3	Power5
AIX 6.1	Power5 and Power6

Supported HP-UX platforms

Table 1-11 shows the HP-UX operating systems and architectures supported by the VCS One client.

Table 1-11 HP-UX operating systems and architectures

Operating system	Architecture
HP-UX 11i v2 with the September 2007 Quality Pack	IA and PA
HP-UX 11i v3 with the September 2007 Quality Pack	IA and PA

Supported versions of Storage Foundation

Veritas Storage Foundation for client nodes is not included with VCS One, but is recommended. Although it is not installed with the VCS One client, Storage Foundation is supported on VCS One client nodes. This section includes information about the versions of Storage Foundation supported by the VCS One client.

Table 1-12 lists the Storage Foundation versions supported on VCS One client nodes.

Table 1-12 Storage Foundation versions supported on VCS One client nodes

Client platform	Architecture	Storage Foundation version supported
Red Hat Enterprise Linux 4 (RHEL 4)	x86 (32-bit)	Veritas Storage Foundation 4.x
Red Hat Enterprise Linux 4 (RHEL 4)	x64 (Intel Xeon, AMD, Opteron)	Veritas Storage Foundation 4.x and 5.0 MP3
Red Hat Enterprise Linux 5 (RHEL 5)	x64 (Intel Xeon, AMD, Opteron)	Veritas Storage Foundation 5.0 MP3
SUSE Linux Enterprise Server Linux 10, SP2	x64 (Intel Xeon, AMD, Opteron)	Veritas Storage Foundation 5.0 MP3
SUSE Linux Enterprise Server Linux 11	x64 (Intel Xeon, AMD, Opteron)	Veritas Storage Foundation 5.0 Release Update 1 (RU1)
Solaris 9	64-bit SPARC	Veritas Storage Foundation 4.x and 5.0 MP3
Solaris 10 Update 3 and later	64-bit SPARC	Veritas Storage Foundation 4.x and 5.0 MP3
Solaris 10 Update 3 and later	x64	Veritas Storage Foundation 5.0
AIX 5.3	Power5	Veritas Storage Foundation 4.x and 5.0 MP3
AIX 6.1	Power5 and Power6	Veritas Storage Foundation 5.0MP3 for AIX 6.1
HP-UX 11i v2 with the September 2007 Quality Pack	IA and PA	Veritas Storage Foundation 5.0MP1
HP-UX 11i v3 with the September 2007 Quality Pack	IA and PA	Veritas Storage Foundation High Availability 5.0 for HP-UX 11i v3

Required patches

AIX

Ensure that the following required AIX patch is installed before installing the VCS One client on AIX 5.*x* operating systems.

Table 1-13 Required patches

Operating system	Required AIX patch	Where to download
AIX 5.*x*	xlC.aix50.rte-8.0.0.8 (or later)	The patch may be downloaded from: http://www-1.ibm.com/support/docview.wss?uid=swg24015076

Note: This patch upgrades xlC.rte to version 8.0.0.8. To check the existing xlC.rte version on an AIX system, enter:
`lslpp -L | grep xlC.rte`
`xlC.rte 8.0.0.8 C F C Set ++ Runtime`		

AIX 5.*x*	The required C++ runtime is 8.0 and above.	To download this patch, use the following URL: http://www-1.ibm.com/support/docview.wss?uid=swg24015076

HP-UX

Ensure that the following required HP-UX patch is installed before installing the VCS One client on HP-UX 11i operating systems.

Table 1-14 Required patches

Operating system	Required HP-UX patch	Where to download
HP-UX 11i v2 PA-RISC	PHCO_34718 (or later)	The patch may be downloaded from: http://www.hp.com
HP-UX 11i (all versions)	PHSS_26560 PHSS_26946 PHSS_27740	The patches may be downloaded from: http://www.hp.com
HP-UX 11i (all versions	TOUR package is needed to support iPv6 functionality.	The patch may be downloaded from: https://h20293.www2.hp.com/portal/swdepot/try.do?productNumber=TOUR

Supported High Availability Agent Pack

This release supports the Veritas High Availability Agent Pack 3Q2009 and later.

Supported platforms for the Simulator

The VCS One Simulator is supported on:

- Windows XP with Service Pack 2 (SP2) or higher, 32-bit
- Windows Vista, 32-bit

Supported web browsers and Flash versions

The VCS One console is the web-based graphical user interface (GUI) used to manage VCS One cluster systems. The VCS One console supports the following web browsers and Flash versions:

- Firefox 3.0, or Internet Explorer 7.0
- Adobe Flash Player version 9.0.124.0 or later

Software limitations

The following software limitations exist in this release.

Backup and restore of VxAT Private Domain Repositories

VCS One provides the following commands to enable backup and restore of the VxAT security repositories.

```
haadmin -backup -vss full_path_to_backup_directory
haadmin -restore -vss full_path_to_backup_directory
```

These commands backup and restore all the Private Domain Repositories (PDRs) on the host where the command is executed. There is no capability to backup or restore individual PDRs. To restore a single PDR, the administrator must manually extract and place the pertinent files from the backup.

Stack size for VCS One agents

On HP-UX 11i v2 systems with PA-RISC architecture, the default stack size for threads is 64 KB. This stack size is not sufficient for VCS One agents and can cause a SIGBUS error.

Workaround: To prevent the issue, ensure that the following patch from HP is applied on HP-UX 11i v2 PA-RISC systems:

PHCO_34718 (or later)

This patch allows the PTHREAD_DEFAULT_STACK_SIZE environment variable to be set to a larger value that becomes the default thread stack size for the applications that run with this environment variable set. To increase the stack size, Symantec has set the PTHREAD_DEFAULT_STACK_SIZE environment variable to 512 KB in the file `/opt/VRTSvcsone/bin/vcsoneenv`.

Do not modify the PTHREAD_DEFAULT_STACK_SIZE environment variable.

Mount resources can cause core dumps

Due to a known Solaris issue, certain system calls create memory leaks that can lead to a core dump. This happens in situations where the Mount resource's `FSType attribute` has a value of *`nfs`*, and is exacerbated when the resource is for a non-global zone and the value of the `SecondLevelMonitor attribute` is *`1`*. [1464953]

With security-enhanced Linux, hadb commands may fail

With security-enhanced Linux, `hadb -up` and `hadb -initdb` commands may fail. [1804444]

The error looks something like this:

```
error while loading shared libraries:
/opt/VRTSvcsone/db/lib/libdbserv11_r.so: cannot restore
segment port after reloc: Permission denied
DBSPAWN ERROR:  -80
Unable to start database server
SQL Anywhere Start Server In Background Utility Version
11.0.1.2044
VCS One ERROR V-97-33-1145 Failed to start the database
server
```

Workaround: Disable SE Linux.

IntentionalOffline for the Oracle and Netlsnr agents is not supported

This release of VCS One does not support the IntentionalOffline feature for the Oracle and Netlsnr agents for any of the client platforms.

Setting the PATH variable to use the command line interface

On the Policy Master, both VCS and VCS One are installed. In some instances, the same command (for example, halog and haclus) exists in both of these products. Be aware of the order of your PATH variable.

To avoid confusion, use the full path name when executing a command.

To set the PATH variable to use the command line interface (CLI) with VCS One, enter:

```
PATH=$PATH:/opt/VRTSvcsone/bin
export PATH
```

The NIS ypstop command removes the NFS entries from the /etc/mnttab files inside of Solaris non-global zones

Running the NIS `ypstop` command removes the NFS entries from the `/etc/mnttab` files inside of Solaris non-global zones. This can cause the Mount agent to fault all NFS resources inside the non-global zones on the host.

Workaround: To avoid this fault, evacuate or shut down all service groups that have NFS Mount resources configured before you run the `ypstop` command.

You cannot run the VCS One installer using c shell (csh)

You can only run the VCS One installer from ksh, bash, or sh shells.

Oracle agent health check may not work (Oracle 11g)

Using Oracle 11g, if you set MonitorOption to 1, health check monitoring may not function when the following message is displayed [ ]:

```
Warning message - Output after executing Oracle Health Check
is:GIM-00009: Message 9 not found.
```

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

Oracle agent health check may not work (Oracle 10g)

Using Oracle 10g, if you set MonitorOption to 1, Oracle agent health check monitoring may not function when the following message is displayed [998494]:

```
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.

VCS One may reject commands when too many are issued simultaneously

Each command issued from a cluster system requires a secure network connection to the Policy Master server. The number of commands that may be in the queue waiting for connection is finite, typically 64. A high number of commands may cause the queue to fill up, causing the subsequent commands to be rejected. Subsequent commands succeed when the queue is no longer full. [432472]

Workaround: Reissue the command at a later time.

Users can log in to the VCS One console without a password when using LDAP server

When using an LDAP server, users can log in to VCS One console without a password. This issue is due to an LDAP server that allows either anonymous bind or unauthenticated bind. [858087]

Workaround: Edit the slapd.conf file to disable anonymous bind and unauthenticated bind on the LDAP server.

To disable anonymous bind and unauthenticated bind on the LDAP server:

1 Shut down the stand-alone LDAP daemon, slapd.

2 Open the file slapd.conf for editing.

3 Add the following lines to the slapd.conf file:

```
disallow bind_anon
disallow bind_anon_cred
disallow bind_anon_bind_simple
```

4 Restart slapd.

The VCS One console displays a Security Information dialog box when you click a link

The VCS One console displays the following Security Information dialog box when you click any link:

```
This page contains both secure and nonsecure items. Do you want
to display the nonsecure items?
```

[914186]

Workaround: Perform the following settings changes in Internet Explorer 6.

To alleviate the issue of the VCS One console displaying the Security Information dialog box on any link click when using Internet Explorer 6:

1 Select **Tools > Internet Option.**

2 From the **Security** tab, select **Custom Level** button.
Scroll to the **Miscellaneous** section in the top box.

3 In **Display Mixed Content**, select **Enable**.

Note: You will not receive the Security Information dialog box for any website and nonsecure items will be displayed on the page.

With Internet Explorer 7, the VCS One console may not refresh

The VCS One console may not always refresh with Internet Explorer because the browser may be displaying a cached web page. [926185]

Workaround: Perform the following settings changes to Internet Explorer 7:

1 Select **Tools > Internet Option > General**.

2 In **Browsing history**, select **Settings.**

3 From **Check for newer versions of Pages**, select **Every time I visit the page**.

If a network error occurs while the database server is attempting to perform an I/O operation, the engine will dump core

If the VCS One database is on network storage and a network error occurs while the database server is trying to perform any I/O operation, the database engine will terminate.

The database engine will be restarted automatically and operations can continue. [970164]

You may only change the case of an editable attribute by editing its XML file

When an editable attribute is case insensitive, such as PrecedenceOrder, you may only change the case of the attribute by editing the XML file that defines the attribute.

For example, the attribute name “Mem” can only be change to “MEM” by editing the xml file.

When you change the configuration by editing the xml file, you must reload the configuration database from the updated XML file for the changes to take effect.

See the *Veritas Cluster Server One User’s Guide* for more information. [1167126]

If a very large number of VCS One clients attempt to connect to the Policy Master at the same time, a TCP/IP socket connection error can occur

There is a default operating system limit to the number of file descriptors (FDs) that can be open at any given time. The number can be changed.

TCP/IP socket FDs are released back to the system after a short delay after closing, which can cause closed socket FDs to linger after the socket has been closed. If the number of open connections is greater than the specified operating system number, a TCP/IP socket connection error can occur. [1211952]

Workaround: To prevent this issue, increase the limit for the number of FDs that can be open at any given time. On most operating systems, you may configure this limit using the `ulimit` tool.

For example:

```
bash-3.00# ulimit -a
core file size        (blocks, -c) unlimited
data seg size         (kbytes, -d) unlimited
file size             (blocks, -f) unlimited
open files                    (-n) 256
pipe size          (512 bytes, -p) 10
stack size            (kbytes, -s) 8192
```

```
cpu time              (seconds, -t) unlimited
max user processes             (-u) 29995
virtual memory         (kbytes, -v) unlimited
```

In the above example, the `open files` attribute on the system is 256. As a result, the TCP/IP socket connection error will occur after 256 client connections have been made to the Policy Master.

On most Linux systems, the default limit is 1024. On Solaris, the default limit is 256.

To prevent the issue, increase the number of FDs that can be open at any given time using the following command:

```
# ulimit -n newnumber
```

Where *newnumber* is the increased number of FDs.

Authenticating a user who does not have a home directory on the system

On UNIX, if a VCS One user does not have a home directory, or the user does not have read and write privileges to the directory, then the user cannot run “ha” commands from the CLI.

By default, the authentication credentials for a VCS One user are stored in the user’s home directory. If the user has no home directory on the system, the credentials may be stored in an alternate location. [1258468]

Workaround:

If a user has no home directory and cannot run “ha” commands from the CLI, perform these steps:

1. Check to see if the user’s home directory is accessible:

   ls -al *users_home_dir*

   Identify whether the owner and group assignments, and permissions allow the user to write to the directory.

   If the user does not have permissions to write to their home directory, proceed to step 2.

2. Manually create the global VRTSat configuration file:

   `/etc/vx/vss/VRTSat.conf`

3. Add the following entries in the VRTSat.conf file:

   ```
   [Security]
   [Security\Authentication]
   [Security\Authentication\Client]
   [Security\Authentication\Client\SSL]
   [Security\Authentication\Credential Manager]
   [Security\Authentication\Credential Manager\Profiles]
   [Security\Authentication\Credential Manager\Profiles\Users]
   ```

```
"AllowHomelessUsers"=dword:00000001
```

4 Change the permissions of the `VRTSat.conf` file to 755:

```
chmod 755 /etc/vx/vss/VRTSat.conf
```

5 Change the permissions of the `/var/VRTSat` directory to 755:

```
chmod 755 /var/VRTSat
```

6 Create a directory named `profiles` under `/var/VRTSat`:

```
mkdir /var/VRTSat/profiles
```

7 Change the permissions of the `/var/VRTSat/profiles` directory to 1777:

```
chmod 1777 /var/VRTSat/profiles
```

The user with no home directory may now log in and execute “ha” commands successfully from the CLI.

Logging in to the VCS One Simulator on Windows in secure mode is not supported

Administrators cannot log in to the VCS One Simulator in secure mode. [419060]

Jobs can be executed out of order for related events

Business policy automation (BPA) jobs can be executed out of order for related events. These events are recorded in the correct order in the BPA log, but, because the BPA process is multithreaded, these events have the potential to be executed out of order. [1266438]

Do not specify any command with resource variables when configuring the HACOMMAND task action in a job

When configuring the HACOMMAND task action in a job, do not specify any command with resource variables. Commands with resource variables are not supported by the HACOMMAND task action in a job. [1248439]

The Policy Master assumes a host is faulted and fails over the service group to another system

The Policy Master does not distinguish between a host failure and a network link failure. If a host becomes unreachable via all public network links, the Policy Master assumes that the system has faulted. In this situation, the application should set the appropriate permissions when exporting a volume to prevent data corruption. [1290582]

The MonitorOption attribute is not supported in Oracle9*i*

The MonitorOption attribute used by the VCS One agent for Oracle (UNIX) is supported in Oracle 10g and later. It is not supported in Oracle9*i*. [1040129]

VCS One may be unable to fail over the Policy Master if NFS-mounted file systems exist in LD_LIBRARY_PATH

If NFS-mounted directories exist in `LD_LIBRARY_PATH`, VCS One may be unable to fail over the Policy Master in the event of a network outage because most of the commands that depend on `LD_LIBRARY_PATH` hang. [1449646]

Workaround: Do not mount well known paths (such as `/bin` and `/usr/local/bin`) from the network. Instead, use locally available libraries, if possible.

Mount agent support on AIX workload partitions

This release adds support for the Mount agent and other bundled agents in AIX workload partitions (WPARs).

This release, however, does not support the following combination of RunInContainer (RIC) and PassCInfo (PCI) for the Mount agent in WPARs:

RIC=0 and PC1=1

This combination is unsupported only if the mount point is specified relative to the WPAR root file system for NFS mounts. For example, if the file system is mounted in `/wpar/p1/mnt`, but the value specified for the MountPoint attribute is `/mnt`, the RIC=0 and PC1=1 combination is not supported.

If you use an absolute path for the MountPoint attribute, the RIC=0 and PC1=1 combination is supported and there is no issue. [1477678]

Configuring shared AT for a VCS Management Console hosted on the same server as the VCS One Policy Master

When you install the VCS One Policy Master, the installer installs both a shared and an embedded version of the authentication services (AT). If you install the VCS Management Console on the same host, VCS has its own version of the authentication service.

Follow the steps in this section to configure shared AT for a VCS Management Console hosted on the same server as the VCS One Policy Master. [1824617]

1 Check the version of Shared VRTSat binaries Installed

/opt/VRTSat/bin/vssat showversion

vssat version: 5.0.27.1

2 Remove VRTSat package completely. Do one of the following:

- On Solaris, enter the following:

  # **pkgrm VRTSat**

- On Linux, find the package name, and remove the package. Enter the following:

  # **rpm -qa | grep VRTSatClient**

  # **rpm -e --nodeps VRTSatClient**

3 If you receive a warning message about verifying packages, ignore the warning message.

4 Remove VRTSat directories. Enter the following:

 # rm -rf /var/VRTSat

 # rm –rf /var/VRTSat_lhc

5 Install the authentication services. Follow the instructions in <deliverable name>.

Fixed issues

The following issues have been fixed in this release of VCS One.

Table 1-15 Veritas Cluster Server One fixed issues

Incident	Description
898749	The vssat showrootbroker command no longer displays incorrect output if the root broker configuration is changed.
1251552	The web server no longer crashes when you change the web server settings using the `http://host:8181/Configuration.do` link. This issue has been fixed with the addition of embedded Tomcat.
1380019	In the previous release, if you set TargetResName before adding systems to the SystemList of a service group, then TargetResName:*attribute* was not localized. This issue has been fixed.
1487384	In the previous release, there was an issue with the service group dependency logic with a parallel child and failover parent. As a result of this issue, some service groups were not taken offline when they should have been. The same issue occurred when you ran the following command: **`hagrp -offline -propagate sg1 -everywhere`** This issue has been fixed.
922939	You can now upgrade from VCS One 2.0.1 to VCS One 5.0.
1321068	In the previous release, you sometimes encountered errors when you started the Simulator from a browser. This is no longer an issues because VCS One no longer supports starting the Simulator from a browser. You can now start the simulator from a directory by running a batch file.
830742	You can now install and run the VCS and VCS One Simulators on the same system.
1383028	OUValue information is no longer disregarded if a service group is created using a job.
1256766	In the previous release, if you had solely resource privileges, resources were not displayed on the All Resources page. This issue has been fixed.

Table 1-15 Veritas Cluster Server One fixed issues (Continued)

Incident	Description
1390990	Object names in an Organization Tree with many levels are no longer truncated in the Trigger Selection page (Configure Rule window). This issue occurred if you selected Filter By: OU Expression and selected the Select expression radio button. This issue has been fixed.
1213954	In the previous release, if two dbsrv9.exe processes were running, shutting down the Simulator did not always work. This issue occurred when the Simulator started for the first time and the VCS One database process (vcsoned) was started. This issue has been fixed.
1250799	In the previous release, user preferences (such as columns selected, widths, and the number of rows per page) for the GUI tables were not always carried over when the Policy Master switched servers. This issue has been fixed.
1395125	You can now delete a resource from the Resource Dependency view in the web console.
1397541	The fault policy no longer incorrectly changes to FaultPropagateAll on the Configure Fault Policy page of the Service Group wizard.
1316983	In the previous release, the `haconf -verify` command did not check or issue a warning when the VCS One ClusterDomainName did not match the AT ClusterDomainName. Similarly, when you loaded a saved VCS One XML database that used the default ClusterDomainName to a Policy Master that has a different ClusterDomainName set, haconf -verify did not check and issue a warning about the ClusterDomainName mismatch. This issue has been fixed.
1394150	The client no longer has issues connecting to the Policy Master if an older authentication certificate store was not cleaned up before the installation.
1703932	Health check monitoring no longer fails if you set MonitorOption to 1.

Table 1-15 Veritas Cluster Server One fixed issues (Continued)

Incident	Description
1196382	The -createcredential option no longer asks you to enable ssh or rsh when it should not.
1238173	In previous versions of VCS One, on Solaris 5.10, a Web application sometimes locked if Solaris patch 127111-11 was not installed. This is no longer an issue because the patch applies to a version of Solaris that is not supported by the current version of VCS One.
1194851	Autorefresh now works when you invalidate a rule on the VCS One console Rule Detail page.
1015326	In the previous release, a Solaris installation failed to proceed if a long disk name was provided. This issue has been fixed.

Known issues

The following are known issues in this release of VCS One. Known issues are anticipated to be fixed in future releases.

VCS One console issues

VCS One console cannot accept single quote mark in object descriptions

Use of single quote (apostrophe) special character (‘) in any description field causes errors in the VCS One console display. [1004445]

Workaround: From the command line, modify the value of the attribute entered in the field such that the special character (‘) is not used.

Flash 9 or later can cause the web browser to crash on Windows

On Windows, Adobe Flash Player version 9 or later can cause the web browser (Firefox 2.0 or later, or Internet Explorer 7.0) to crash when you perform operations in the AWM, Resource dependency, Group dependency, and Map views in the VCS One console. [540032]

Some wizard screens may go blank

If you are running nspluginwrapper 0.9.91 and 32-bit Flash plug-in version 10.0.32 for Firefox 3 beta 5, some wizard screens, such as group online and group offline screens, may go blank when you click **OK**. [1818640]

Workaround: Update nspluginwrapper to version to 1.2.2, install the 64-bit Flash plug-in for version 10.0.32, and restart Firefox.

Attribute values are displayed incorrectly in the Edit Attribute wizard

When you override default attribute values using the Edit Attribute wizard, the wizard incorrectly displays the default value instead of your override. This is a display issue only. The correct values are stored in the resource. To see the correct values, go to the All Attributes page for that resource. [1789333]

In the Service Group Configuration window, the platform field may not display correctly

In the Service Group Configuration window of the VCS One console, the pull-down arrow for the Platform field may not appear. [852600]

You cannot take a composite service group offline when a resource is in the ONLINE | STATE UNKNOWN state

If a resource is in the ONLINE | STATE UNKNOWN state, the Policy Master does not allow you to take that resource offline. [1804787]

Clear the browser cache before switching to a different Policy Master

If you switch to another Policy Master, you must clear the browser cache and open a new web browser window before logging into the VCS One console. [968580]

The browser does not refresh if the Add Custom View wizard is opened from the Add/Modify Set wizard

In the VCS One console, the browser does not refresh if the **Add Custom View** wizard is opened by clicking the **Add Custom View** button on the last frame of the **Add/Modify Set** wizard.

This issue is due to a technical limitation of JavaScript. JavaScript cannot get a reference to a grandparent of the current window if the parent window is closed. [996672]

Workaround: Manually refresh the web page to view the changes in the VCS One console.

You may not specify event parameters for a job while that job is running

When adding a job using the VCS One console and adding a task for that job using the **Task Details Page**, if **Execute Script** or **Execute Script using SSH** is selected from the **Select Action Type** pull-down menu, you can select the **Use event parameters as arguments** checkbox. However, you are not allowed to define event parameters while the job is running. For this reason, select the **Use event parameters as arguments** option only for jobs that are associated with a rule.

Similarly, when adding a job and a task for that job using the **Task Details Page**, if **Send Syslog** is selected from the **Select Action Type** pull-down menu, you can select the **Prefix event message** checkbox. However, because you are not allowed to define event parameters while the job is running, select this checkbox only for jobs that are associated with a rule. [1206106]

Some “ha” commands are not validated on the Job wizard while adding an HA command on the Task Detail Page

Some “ha” commands are not validated when you select the **Validate** option while selecting **Execute HA Command** in the **Task Detail Page** of the **Job** wizard in the VCS One console. The wizard accepts some “ha” commands as correct even if the syntax is incorrect.

For example, the wizard accepts the following command even though the command is missing the `-any` option:

```
hagrp -online/offline -ou /
```

[1225823]

Autorefresh does not work during a rule invalidation

If you delete an object, such as a service group, from the CLI, no notification of the deletion is sent to the **Rule Detail** screen of the VCS One console.

For example, if you:

1. Create a rule in the VCS One console.
2. Select a group or events for the group.
3. In the **Object Selection** screen, select groups (for example, sg1 and sg2).
4. Complete the rule configuration.
5. From the CLI, delete the service group named sg1.

The **Rule Detail** screen in the VCS One console does not refresh for rule invalidation. [1194851]

Workaround: Press F5 to refresh the screen manually.

The Add/Modify Resources wizard may not open if the number of resources is large

If the number of resources is large (on the order of thousands), wizards such as **Add/Modify Resources** may not open. [1393920]

If you add a user to VCS One without setting a password, anyone can log in as that user with any string

If you add a user to VCS One without setting a password, anyone can log in as that user with any password string. [1323590]

Workaround: It is strongly recommended that users set a password, and not leave the password field blank.

Operational issues

Support for VMware ESX server virtualization technology

VCS One no longer supports ESX. However, references to ESX and its related objects (PFrames and VFrames) may be visible to the user. ESX is not supported in the current release, but will be available in the future. [1709455]

Incorrect error message

The correct message corresponding to message ID 1037 is:

```
Please do the same on all the other VCS One policy master nodes.
```

Due to an error in the message catalog, the message corresponding to message ID 1036 is printed for message ID 1037 also.

Insufficient privilege error message

If you receive an insufficient privilege error for an action on a system, it may be because the system is not anchored to the same organization unit node as the user in whose context the command is run.

The recommended design is to anchor the system to the same organization unit node as the user in whose context the command is run. See “How you manage users using the Organization Tree” in the *Veritas Cluster Server One User’s Guide*.

Sets may not work correctly for root users on the Policy Master

Sets may not work correctly for root users on the Policy Master. This affects all ha commands that take `setname` arguments. [1839060]

Workaround: Root users should avoid using sets on the Policy Master. It’s best not to log on to the Policy Master as root to perform daily operations. If you must log on to the Policy Master as a root user, you should forcibly specify the root username and unixpwd or pam domaintype for every ha command that uses `setname` arguments.

When a default root user adds a set on the Policy Master, the set may not be visible in the GUI or on another Policy Master Node

A set that the root user creates using the haset command on the Policy Master host is associated with the user name `root@`*`pm_hostname`*. This set will not be visible to the root user via the GUI, where the default user name is `root@`*`cluster name`* or to the root user on other Policy Master hosts where the user name is `root@`*`other PM_hostname`*. [1480037, 1836909]

Workaround: To avoid this visibility issue, the root user should use the explicit domain type, unixpwd, when using the haset command. For example:

```
haset -add set -ou / -user root -domaintype unixpwd
hagrp -display -setname -user root -domaintype unixpwd
```

When you add a set, the set is not dynamically updated with extended attribute changes or updates to the organization tree

When you add a set using the `haset -add` command, the set is static. The set is not dynamically updated if the Orgtree or the referenced extended attribute (EA) changes. [1463742]

For example, add the following set:

```
haset -add mysolsystems -ou /LOB=MYBIZUNIT/Dept=MYDEPT -ea
OS=Solaris10
```

If another user deletes **`Dept=MYDEPT`** from the Orgtree, then **`MYDEPT`** is not automatically removed from the **`mysolsystems`** definition. The same is true for extended attribute changes. If someone removes **`Solaris10`** from the OS attribute, the **`mysolsystems`** set definition is not automatically updated.

Workaround: The OU and EA components are only validated when you create, modify, or use a set. To validate changes in the above example, do one of the following:

- Delete the set and add it again, redefining the attributes. For example, enter the following, (substituting your own attribute definitions):

  ```
  haset - delete mysolsystems
  haset -add mysolsystems -ou /LOB=MYBIZUNIT/Dept=<NEW
  DEPARTMENT> -ea Platform=Solaris
  ```

- Modify the set. For example, enter the following, (substituting your own attribute definitions):

  ```
  haset -modify mysolsystems -ou /LOB=MYBIZUNIT/
  Dept=<NEW DEPARTMENT> -ea Platform=Solaris
  ```

- Use the set. For example, enter the following, (substituting your own attribute definitions):

  ```
  hasys -display mysolsystems -ou /LOB=MYBIZUNIT/
  Dept=MYDEPT -ea Platform=Solaris
  ```

  When you display the set, you see an error message if MYDEPT is renamed or deleted from the Orgtree. You can then modify the set with the updated information.

With security-enhanced Linux, VCS One controlled mount fails, while manual mount of volume succeeds

Security-enhanced Linux must be disabled, because the Security-enhanced (SE) Linux support is provided for evaluation purposes only and the Security policy files are not currently available for the Veritas product stack. Problems such as the mount issue in the subject title can result when Security-enhanced Linux is enabled.

Workaround: To disable SE Linux at boot time on both SUSE Linux Enterprise Server 9 (SLES 9) and Red Hat Enterprise Linux 4 (RHEL 4), set the kernel boot parameter `selinux` to `0` (`selinux=0`) and reboot the machine. Assuming the system has been configured for booting from the machine *`machine_name`*, edit the file `/boot/`*`machine_name`*`/menu.lst` to include `selinux=0` on the kernel line. Then reboot the machine to ensure the setting takes effect.

Semaphores initialized by database are not cleaned

The VCS One database and the clients communicate using the shared memory protocol. In the case where the client or database processes are killed using SIGKILL, the semaphores are not cleaned up. Once the number of initialized semaphores exceeds the operating system limit, the database does not come up. [343871]

Workaround: Make sure the database and client processes are terminated properly.

In the Add Extended Attribute wizard, you must click twice on the combo box to select the default value

When you add or remove keys from an enumerated extended attribute, you must click twice to get the focus out of the table and select the value in the default value combo box. [1587659]

Deleting a NIC may cause failover issues (Solaris only)

When you delete a NIC from a MultiNICB resource, only the groupname is removed from that NIC. All IP addresses are left on the NIC. As a result, the virtual IP addresses on that NIC are no longer under IPMP. [1822396].

Workaround: Manually remove the IP addresses from the NIC and plumb them to the NICs you want to use.

Modifying the ClusterAddress attribute using C shell (csh) may result in errors

If you use csh, modifying the ClusterAddress attribute may result in errors. The reason for the errors is that VCS One and csh interpret square bracket characters "[" and "]" differently. [1804504]

The issue occurs when you use the following commands:

- **`haclus -modify ClusterAddress -add [ipaddr]:port`**
- **`haclus -modify ClusterAddress -delete [ipaddr]:port`**

Workaround: When you use the above commands, include double quotation marks around text, such as **`"[ipaddr]:`*`port`*`"`**, that contains square brackets.

The harule command does not work if you do not use the default port for the authentication server

You must enable the default port for the authentication server (14159) for the `harule` command to work. The `harule` command allows you to add, delete, modify, enable, disable, and list notification rules. Rules are triggered by a Policy Master event or by a scheduled event. [1834928]

You cannot use the GUI to edit a disaster recovery IP address

You cannot use the GUI to edit the Cluster DRAddress attribute. [1810021]

Workaround: To edit a disaster recovery IP address, you must use the `haadmin` command.

Refer to the *Veritas Cluster Server One User's Guide* for instructions.

Harmless “duplicate tcp line” messages can be suppressed

On Red Hat Linux, when a TCP connection is rapidly closing and re-connecting on the same address/port pair, several messages may appear that contain the text:

```
warning, got duplicate tcp line.
```

These messages are harmless and do not impact performance. Refer to the Red Hat Knowledgebase link:

http://kbase.redhat.com/faq/FAQ_80_6180.shtm

[422083]

Workaround: These messages may be suppressed by changing the values of the kernel parameters `tcp_tw_recycle` and `tcp_tw_resuse` in the file `/etc/sysctl.conf` to 0. After changing the parameter values in the file, execute the `sysctl -p` command to put them to effect.

haconf -verify fails to warn about attribute defined twice

If, by mistake, a user defines an attribute twice in a VCS One configuration file, the `haconf -verify` command does not give a warning. Instead, it causes the second definition to override the first. For example:

```
<group name=”g2”>
   <attributes>
      <attribute name=”CompatibleGroups”>
          <val key=”ALLGROUPS”></val>
      </attribute>
      <attribute name=”Load”>
         <val key=”cpu”>10</val>
         <val key=”memory”>10</val>
      </attribute>
      <attribute name=”SystemList”>
         <val key=”vcssun31”>0</val>
         <val key=”vcssun32”>1</val>
      </attribute> <attribute name=”Load”>
         <val key=”cpu”>0</val>
   </attribute> </attributes>
</group>
```

The Load attribute has two values, the second overriding the first. [570978]

Workaround: Be careful to define an attribute value only once.

Inability to contact DNS server may cause “ha” commands to hang

When “ha” commands are issued after a network failure, they may hang for a long time if the DNS server cannot be reached. The commands require the DNS server for authentication functionality. [602987]

Workaround: Perform the following two actions:

1 On each Policy Master system, specify the Policy Master virtual IP address in the file `/etc/hosts`.

2 Edit the file nsswitch.conf and precede “dns” with the word “files” such that it contains the line: `hosts: files dns`.

VCS may not shut down if you change a system from run level 3

If you change a system from run level 3 to run level 1, 2 or single user, VCS will not shut down and any resources managed by VCS may fail when the underlying resources disappear. [635269]

Workaround: Take the system down to run level 0 and then bring it up to single user or run level 1, 2.

haconf may fail

In some situations, haconf may return a failure or dump core. [995630]

Workaround: Reissue the command.

The LinkStatus attribute value in the disaster recovery panel sometimes toggles between UP and DISABLED

If EnableConnections is set to 1 on the Initiator cluster and 0 on the Acceptor cluster, then the Initiator cluster periodically attempts to connect to the Acceptor cluster. This causes the LinkStatus attribute value for the connections between the clusters to toggle between UP and DISABLED. The toggling happens in the GUI. It also happens in the CLI if you invoke the CLI frequently. [1740009]

Workaround: Set EnableConnections to 1 on the Acceptor cluster.

Do not use commas in an extended attribute value

If a single extended attribute (EA) value contains a comma, the value is interpreted as multiple values when the VCS One database is reloaded. To avoid this issue, do not use commas in an extended attribute value. [932599]

Ensure that VCS One group administrators also have system administrator privileges

Ensure that VCS One group administrators also have system administrator privileges for those systems where their service group can fail over. [1000394]

Built-in and extended attribute names should be enclosed in double quotes if they contain escape sequences for special characters

Ensure that attribute values/validations (both built-in and extended) that contain escape sequences for special characters are enclosed in quotation marks (“).

For example:

```
<attribute name="StartProgram"><scalar>"start in bg -- &amp;amp;"
</scalar></attribute>
```

[1005373]

VCS One commands will not work if the system needed to perform the action is unavailable

VCS One commands may be accepted by the Policy Master, but will not work if the system needed to perform the action does not have a heartbeat or has faulted. [1010240]

Workaround: To work around this issue, reissue the command after the needed system is running again.

In some situations, hadb -up may result in errors

In some situations, `hadb -up` may result in errors. These errors are Sybase ASA errors from the dbspawn utility. Examples of the errors are below. [1011122]

Example 1

```
DBSPAWN ERROR = -81
```

Frequency of occurrence: Very low

Cause: Unknown.

Workaround: To work around this issue, do one of the following:

- Start the server again using `hadb -up`.

Or:

- Copy the database files to a backup directory to ensure the current configuration is saved. Then, run `hadb -reloaddb` *`backup_dir`* from the backup directory.

Or:

- If the above two actions do not work and if an XML backup is available, then run these commands:

```
hadb -initdb
hadb -up
haconf -loaddb XML_backup_dir
```

Example 2

```
DBSPAWN ERROR = -80
```

Frequency of occurrence: Very low

Cause: Starting and stopping the database immediately may sometimes result in this issue.

Workaround: See the workaround in Example 1 above.

Example 3

```
DBSPAWN ERROR = -832
```

Frequency of occurrence: Low

Cause: When system semaphores are exhausted, the max semaphore OS limit is reached. This occurs when database clients (vcsoned/haconf) are killed abruptly using SIGKILL/SIGSTOP.

Workaround: To work around this issue, do one of the following:

- Manually delete the semaphores using ipcrm (UNIX).

Or:

- Reboot the node.

If resource variables are used, the ExportACL attribute for the NetAppExport agent does not get the values for other systems in SystemList

Resource variables are associated with specific systems in the ArgListValues that are passed to the agent. As a result, if resource variables are used in the ExportACL attribute, ExportACL does not get the values for the other systems in the SystemList when passed to the NetAppExport agent. For example, the NetAppExport agent will not get the value for system A as part of a snapshot for System B for ExportACL. [1004445]

Workaround: You can avoid this issue if ExportACL is explicitly defined without using resource variables.

On Linux, changing the system clock to an earlier date or time may cause Policy Master notifications to be delayed

On Linux, if you change the system clock to an earlier date or time when the VCS One console is running, notifications from the Policy Master may be delayed for a duration equal to the amount of time the system clock has been set back. You may see stale data for this duration. After the duration, the console will refresh and any notifications from the Policy Master will appear. [1014469]

A fault with NetApp Filer caused “ha” commands to hang

If the VCS One configuration database resides on a NetApp Filer and the NetApp Filer faults and goes down, “ha” commands hang for a period of several minutes, the pmexport agent goes into a monitor timeout state, and the PMSG faults. This occurs only under certain conditions. [1021318]

Before a business policy automation (BPA) event is generated, all of the attribute values affected by the event must be fully populated

If VCS One generates a BPA event before all the attribute values are fully populated, the script may fail through a BPA rule. This can happen after the database has been reloaded. For example, if VCS One generates a SYS_JOINED event, the script may fail if the SysInfo attribute is not fully populated before the BPA job runs. [1838091]

Workaround: Stop and restart the client.

Business policy automation (BPA) jobs time out after 1000 seconds

BPA jobs have a maximum time limit of 1000 seconds. [1840291]

The business policy automation (BPA) job wizard hangs until the job completes

If you use the BPA job wizard, and a job takes a long time to complete, the job wizard does not refresh. Although the job wizard seems to hang, the jobs continue to run in the background.

Workaround: Wait for the few minutes for the job to finish and the GUI to return.[1840296]

Group compatibility privilege is effective only at /

With this release, group compatibility privilege is effective only at /. This means that the compatibility privilege granted at other OU nodes does not have any effect. You may not modify group compatibility at OUValues other than / even if you have the privilege to do so at those OUValues, unless you also have the privilege at /. [1024724]

Symbolic links in /opt/VRTS/bin have different owner than binaries in /opt/VRTSvcsone/bin

The binaries in `/opt/VRTSvcsone/bin` have root:sys as the owner but the symbolic links in `/opt/VRTS/bin` have the owner as `root:other`. [1029460]

hagetcf requires an absolute path

The hagetcf command asks you to enter the path where the configuration can be saved. The default path is `/var/tmp`. If you supply a relative path, the command will fail.

For example, entering "." to specify the current directory results in an error message similar to the following:

```
VCS One ERROR V-97-1-17430 Directory './vcsoneconf.01May2007_154928'
does not exist
```

[1037594]

Workaround: To work around this issue, supply an absolute path (for example, /tmp).

VCS One CLI commands may sometimes hang on a client system if the socket connection uses an IP address configured using the IP resource on the client system as its source IP address

VCS One CLI commands may open a socket connection using an IP address configured using the IP resource on VCS One client systems. If the IP resource is down on the client node, the CLI commands will not be able to resolve the IP

address configured by the IP resource. In this situation, the VCS One CLI commands can hang indefinitely. [1038213, 1126275]

Workaround: Specify a local IP address on the client system as the source IP to bind to while connecting to the Policy Master on an IP address specified in vcsone.conf. Doing so prevents the socket connection from using any other IP address as the source IP address.

1. Specify the source IP for a given Policy Master IP in vcsone.conf:

   PM_IPS=[*pm_ip*]:*port*:[*src_ip*]

   Each PM_IPS record can have an additional source IP separated by a colon (":").

2. Specify the source IP (*src_ip*) the same way you would specify the Policy Master IP. That is, enclose the IP in square brackets "[]" to indicate an IPv6 IP.

By default, the OfflineMonitorInterval is set to zero

By default, the OfflineMonitorInterval attribute is set to zero. Therefore, resources are not monitored after they go offline. [1124752]

Workaround: To work around this issue, you may change the value of OfflineMonitorInterval using the hatype command.

Specify the disk name for the first system in the system list

If the name of the shared disk is not the same on all the systems, when prompted to enter the disk name when installing the Policy Master, enter the disk name for the first system in the system list. [1149268]

Engine logs fill up with message 40502 when earlier client versions connect to the Policy Master

When earlier versions of the client connect to the Policy Master, the engine logs fill up with message 40502. [1201279]

Workaround: To prevent this issue, ensure that earlier versions of the client are removed before installing this release of VCS One. Earlier client versions include Veritas Application Director 1.0, Veritas Application Director 1.1, and Veritas Application Director 1.1 Platform Expansion.

Parallel service group with a disabled resource

If a parallel service group contains a disabled resource then the online anywhere command always attempts to bring the service group online on the same system and the `hagrp -online -everywhere` command brings the group online on one system only. [1250599]

The group state appears incorrectly as ONLINE

When all OnOff type resources in a group have AutoStart = 0, the group state incorrectly appears as ONLINE even if any single resource is ONLINE. The group state should appear as PARTIAL in this situation. [1252792]

If vcsoneclientd issues a warning about a non-available SysIPAddress, “ha” commands will not work in a local zone

If the SystemIPAddrs attribute is not configured in vcsone.conf and the host name of the VCS One client is not resolvable to an IP address, then vcsoneclientd issues a warning message in the vcsoneclientd logs stating that there are no IP addresses available for the Policy Master to ping vcsoneclientd.

If you see this warning in the vcsoneclientd log files, then the Solaris local zone entry points stop working and “ha” commands will not work. This issue occurs because “ha” commands issued from the local zone entry points use the same set of IP addresses to communicate with vcsoneclientd running on a global zone. [1278703]

Workaround: To resolve this issue, do one of the following two things:

- Configure the SystemIPAddrs in the vcsone.conf file.
  In the /etc/VRTSvcsone/vcsone.conf file on the client node, add the following line to the file:
  ```
  SystemIPAddrs=10.10.10.10:11.11.11.11
  ```
- Ensure that the local host name of the client can be resolved by DNS to an IP address so that this IP address can be used by “ha” commands inside the local zone to communicate with vcsoneclientd running on the global zone.
  Log in to the client node and run the following command:
  nslookup *hostname*

Do not use spaces in user and user group names

VCS One does not support the use of spaces in user and user group names. [1228073]

When a system joins the server farm, AgentVersionInfo error messages appear in the engine logs

When a system joins the server farm, the following error messages appear in the engine logs:

```
VCS One ERROR V-97-1-17369 [system_name::AgentVersionInfo]
Attribute key ‘agent_name’ does not exist
VCS One ERROR V-97-1-17363 [system_name::AgentVersionInfo]
Attribute key ‘agent_name’ already exists
```

Workaround: To prevent the issue, execute the following command locally on the system:

haagent -update *agent*

This command adds the agent version to the AgentVersionInfo attribute.

[1297798]

Remove the user from the VCS One configuration when the user is removed from an external directory

If a user is removed from an external directory, for example, Active Directory or LDAP, but is not also removed from the VCS One configuration, the rules owned by that user will still execute. Whenever you remove a user from an external directory, also remove the user from the VCS One configuration. [1364434]

hagrp -online group -everywhere is not supported

In BPA, `hagrp -online group -everywhere` is not supported. The command displays the following error in the web console:

```
VCS One Error v-97-11-1178 Command is not a valid or supported
HACommand
```

[1367271]

If you delete an object that is used in a job, the policy is marked “Invalid”

If you delete an object that is used in a job, both the job and its associated policies are marked “Invalid” and the job is not executed. If you delete an object that is used in a policy, such as conditions or event selections, only the policy is marked as “Invalid”.

If the object referenced in the Execute HACommand task is deleted, BPA does not recognize the deletion and may leave the job and associated policies marked as “Valid”. [1367271]

Setting up Policy Master communication for local zones may not work

If the home directory of the root user in a global zone is different from the home directory of the root user in local zones running on the same node, the VCS One resource action for setting up Policy Master communication for the local zone does not work. One example of such scenario is when LDM (logical domain manager) is running in the global zone. [1835533]

The VCS One database transaction log file may fill up disk space, causing database corruption and VCS One failure

The VCS One database transaction log file continues to grow over time. (It has been observed to reach approximately 3 to 4 gigabytes.) As a result, it may use up all the free disk space. This issue may result in database corruption and VCS One failure. [1391882]

Workaround: Periodically, take a full database backup to a different device or partition, using the following command:

```
haadmin -backup -db backup_dir
```

This command backs up the database and transaction log files, and then truncates the transaction log file that is in use. Only a full back up truncates the transaction file.

In addition, ensure that there is ample disk space for the transaction log file to grow between backups.

In some situations, the Policy Master log page is empty in the web console

In some situations, the Policy Master log page is empty in the web console. If you encounter this issue, the system may have exceeded its open file descriptor limit. To determine whether this is the case, open the following file and look for a “too many open files” error:

```
/var/VRTSvcsone/log/vcsonems-rca.log
```

[1393726]

Workaround: If the error is present, run the following command to view the current file descriptor limit value:

```
ulimit -n
```

Next, set a considerably higher file descriptor limit value:

```
ulimit -n new_value
```

If Policy Master switches servers during client installation, the installer may fail or produce an error

If the Policy Master switches servers during client installation, the installer may fail or produce an ssh error. This occurs only if the Policy Master switches server during the question and answer part of the installation.

Note that it is assumed that ssh communications has been set up and works correctly outside of the installer between the installation and Policy Master servers. [1394597]

Workaround: If the installer produces an ssh error during the installation and the Policy Master has switched servers, abort and restart the installer. The ssh issues will be resolved when you re-run the installer.

If the installer fails after the question and answer part of the installation and the Policy Master has switched servers, re-run the installation. Note that the failure occurs during the credential setup, but the client software should have installed correctly on each server.

Volume resources in ONLINE|UNABLE TO OFFLINE state

If the Volume resources are in ONLINE|UNABLE TO OFFLINE state on any node, deport the disk group on that node by issuing the following command:

```
vxdg deport dgname
```

Then, probe the corresponding volume and the disk group resources. [1281657]

Error message displayed for AuthBrokerMap has incorrect command syntax

The error message displayed for the AuthBrokerMap attribute has the incorrect syntax for `haclus -modify`. In the error message, `domaintype:domainname` should be replaced with `domaintype domain-broker`.

The correct command syntax is:

```
/opt/VRTSvcsone/bin/haclus -modify AuthBrokerMap -add nis
mynis_broker.com
```

The correct command syntax is also available in the *Veritas Cluster Server One Command Reference Guide*. [1403659]

A set based on a location in the Organization Tree no longer works when you remove the location

You can create a set to manage a collection of objects at any location in the Organization Tree. If you remove that location, however, any set based on that location no longer works.

When you remove the location, the command line displays an error. The GUI does not, but the set will be invalid the next time you invoke it. [1463761]

VCS One does not initiate failover following a web server crash

When the VCSOneWeb resource in the Policy Master Service Group (PMSG) crashes, VCS One does not initiate failover. This is because the VCSOneWeb resource is not set as a critical resource by default. [1513083]

Workaround: Make the VCSOneWeb resource a critical resource so that the PMSG will fail over if the web server crashes. Enter the following:

```
/opt/VRTSvcs/bin/haconf -makerw
/opt/VRTSvcs/bin/hares -modify VCSOneWeb Critical 1
/opt/VRTSvcs/bin/haconf -dump -makero
```

You cannot change or set the SourceFile attribute value for the haset command

Changing or setting the SourceFile attribute value for the haset command has no effect. [1663946]

For more information about the haset command, see *Veritas Cluster Server One Command Reference Guide*.

Policy Master issues

After backing up and restoring a Policy Master, HA commands may not work

After backing up and restoring a Policy Master on a clean system, HA commands may not work. [1819159]

Workaround: Set up trust between the client node and the authentication broker. On each Policy Master node, enter the following:

```
/opt/VRTSvcsone/bin/haat setuptrust -b
policy_master_virtual_ipaddress:BrokerPort -s low -j client
```

Then, confirm that the HA command works.

Running hagrp -modify -refreshvars may cause the Policy Master to dump the core on Solaris

If you run `hagrp -modify -refreshvars` on Solaris, the Policy Master may dump the core if a group attribute is used as a variable. [1859644]

When the Policy Master fails over or restarts, the group states displayed in the CLI may not update right away

When the Policy Master fails over or restarts, the state of the groups displayed in the CLI may not update until all of the group resources are probed.

Workaround: To find out if the group state has been updated, check the ProbesPending attribute. If that attribute value is not 0, then the group resources are not yet updated. You can also view the group state in the GUI. If the group state has not been updated, it shows in the GUI as "stale." [1278400]

Policy Master cannot connect to database if previous .odbc.ini file exists

When the Policy Master is restarted, a previous .odbc.ini file in the current working directory of the database client (Policy Master or `haconf`) system prevents the connection to the Policy Master database. For example, the error may resemble:

```
VCS One ERROR V-97-7-17 Unable to connect to database server.
```

Workaround: Look for the .odbc.ini file in the current working directory of the database client, and, if it exists, move it outside of the directory and attempt to reconnect.

System connection to Policy Master fails if time setting lag is more than 30 minutes

The Symantec Product Authentication Service program may reject connections from cluster systems that have a time setting greater than 30 minutes behind the Policy Master time setting. The failure may be logged with a message that resembles:

```
VCS One ERROR V-97-19-12358 Failed to obtain the credential from
Local cache, please ensure that the System credential is
deployed on the node and the System does not lag behind the PM
node
```

Workaround: Use the NTP utility to correct the system's time.

On Solaris, a single Policy Master may not start automatically after rebooting

On Solaris, if the runlevel3 VCS script file in the `/etc/rc3.d` directory has the same sequence of numbers as the other files (that is, if for some reason, S99vcs and S99sunwccccrr_b both have the same sequence number, 99, in the Policy Master host, VCS One and VCS will not automatically start after rebooting. [1016563]

Workaround: Manually restart VCS One and VCS after rebooting. Start VCS using the `-onenode` option.

A time difference between the Policy Master and authentication broker may prevent a user from logging into the web console

If an external node is used as an authentication broker and there is a time difference of one and a half hours between the Policy Master node and the authentication broker node, then logging into the web console fails. [1193573]

Workaround: Change the time of either the Policy Master or authentication broker node.

The search pane does not expand correctly when you search a group resource dependency graph or group dependency graph

If you open a service group resource dependency graph and a group dependency graph, click the **Search** button to open the search pane, and then click the **Search** button several more times, the search pane does not expand properly. [1543609]

If a job script is running while the Policy Master is switching over to another node, a user privilege error occurs

If a script is running while the Policy Master is switching over to another node, the script continues to run on the first node and is not invoked again on the new Policy Master node. Because the user executing the job is not recognized on the new Policy Master node, a user privilege error occurs.

Similarly, if a script task in a job times out, it is not killed. It must be killed manually.

These issues occur because outstanding requests are not preserved and continued on the target node when the Policy Master switches over.

[1321011]

Workaround: To prevent these issues, ensure than no jobs are in progress when the Policy Master is switched to another node.

Scripts configured in a job are not killed when the scripts time out

If a script configured in a job does not finish within the specified timeout period, the job will fail, but the script continues to run. In this situation, you need to kill

the script manually. If many scripts are hanging, it could potentially result in the Policy Master node running out of resources. To avoid this issue, whenever a job fails due to a script timeout, kill the script manually. [1362168]

If you host Policy Master storage on a NetApp filer

During a simultaneous outage of all systems that are configured to be able to host the VCS One Policy Master, VCS One may not be able to clear locks on the NetApp filer. If the locks are not cleared, the subsequent restart of the Policy Master may be affected.

The following document from NetApp addresses this situation:

https://now.netapp.com/Knowledgebase/solutionarea.asp?id=ntapcs1386

[1401796]

On Solaris, the donating server may not be able to reconnect when the Policy Master switches servers if IPMP is in use

When the Policy Master is clustered on Solaris, IP multipathing (IPMP) is in use, and the Policy Master is switched from one server to another, the donating server may, in some circumstances, not be able to reconnect to the Policy Master when it comes up on the receiving server. The system appears as faulted if the VCS One client is installed. [1507271]

Workaround: This issue is due to an invalid ARP table entry. You can resolve the issue by deleting the offending entry using the following command:

```
arp -d PM_Virtual_IP_address
```

After the command completes, the donating server reconnects.

The Policy Master resource monitor may fail if the root user uses csh

If the root user uses csh, the Policy Master resource monitor may fail. If this happens, the `ps` command output does not match what is set for MonitorProcess. [1804513]

Workaround: Switch the root shell from csh to sh.

In certain situations when an off-host resource is configured, you may get a Policy Master error message

If you create a resource and immediately assign a control group to the resource to convert it to an off-host resource, you may get an error message. [1830937]

The error message may look similar to the following:

```
VCS One INFO V-97-1-53234 Configuration version number on
Policy Master for system_name is 166, VCS One Client
Daemon has 165
```

`VCS One WARNING V-97-1-11080 Rejected NetAppExport agent from system_name because no resource of type NetAppExport exists on system_name`

Workaround: Ignore the error message, or put a sleep of 3 seconds between creating the resource and assigning control group.

Simulator issues

VCS One Simulator user credential is valid for eight hours

After logging into the VCS One Simulator, a user's authentication credentials are valid for eight hours. When the credential is no longer valid, some operations in the Simulation Panel of the VCS One management console continue to succeed, such as taking groups online and offline, but some user actions fail, such as faulting systems or groups and starting systems. When an operation fails, a user receives a message resembling:

```
Command: hasim -faultsys solsys1
Result: Could not connect to proxysim.
```

Workaround: Log back into the VCS One Simulator.

Network connection error messages during VCS One Simulator startup are harmless

When you start the VCS One Simulator from the command line, it is possible to see messages that resemble:

`V-97-1-10057 ClentHandle::net_recvb failed Error (-4)`

Such error messages may appear when the Policy Master attempts to initiate a control connection to the VCS One Simulator during the time the Simulator is attempting to register with the Policy Master. When the registration is complete, the Simulator successfully responds to subsequent attempts by the Policy Master, so the initial error messages are harmless. [568368]

Cannot add WebLogic9, WebSphere5, and WebSphereMQ6 resources

If you start the Simulator using default configurations, you cannot add resources of the following types:

- WebLogic9 and
- WebSphere5
- WebSphereMQ6

[1393669]

Workaround: Add the lines below in main.xml and then load the configuration:

```
<include>WebLogic9Types.aix.xml</include>
<include>WebLogic9Types.linux.xml</include>
<include>WebLogic9Types.sun.xml</include>
```

```
<include>WebLogic9Types.windows.xml</include>
<include>WebSphere5Types.aix.xml</include>
<include>WebSphere5Types.linux.xml</include>
<include>WebSphere5Types.sun.xml</include>
<include>WebSphereMQ6Types.aix.xml</include>
<include>WebSphereMQ6Types.linux.xml</include>
<include>WebSphereMQ6Types.sun.xml</include>
```

After adding these lines to main.xml, you can load the configuration and start the Simulator.

Authentication issues

Deleting a VCS One client system does not delete the security principal and credential

When deleting a client system or a user from the VCS One configuration, the security principal and credential are not deleted. [1271612]

Workaround: To completely delete a client system, including the security principal and credential, from the VCS One configuration, perform the following steps:

1. To delete a client system, enter the following command:

   ```
   # /opt/VRTSvcsone/bin/hasys -delete system_name
   ```

2. From the active Policy Master system, remove the security principals by entering the following command:

   ```
   # /opt/VRTS/vcsone/bin/haat deleteprpl -t ab -d VCSONE_USERS \
   -p system_name
   ```

3. From the client system, remove the security credentials by entering the following command:

   ```
   # /opt/VRTSvcsone/bin/haat deletecred -d vx:VCSONE_USERS \
   -p system_name
   ```

To completely delete a user, including the security principal and credential, from the VCS One configuration, perform the following steps:

1. To delete a user, enter the following command:

   ```
   # /opt/VRTSvcsine/bin/hauser -delete user_name
   ```

2. From the active Policy Master system, remove the security principals by entering the following command:

   ```
   # /opt/VRTS/vcsone/bin/haat deleteprpl -t ab -d VCSONE_USERS \
   -p principal_name
   ```

   where *principal_name* is the user name.

3. From the client system, remove the security credentials by entering the following command:

```
# /opt/VRTSvcsone/bin/haat deletecred -d vx:VCSONE_USERS \
-p principal_name
```

where *principal_name* is the user name.

VCS One client issues

On AIX, vcsoneclientd may be unable to start

On an AIX system on which the VCS One client is installed, vcsoneclientd cannot start after the system is rebooted, if the entry `install_assist` exists in the `/etc/inittab` file. The `install_assist` entry prevents the vcsoneclientd startup and shutdown scripts from being executed. [1231089]

Workaround: To prevent this issue from occurring, comment out the `install_assist` line in the `/etc/inittab` file:

```
# : install_assist:2:wait:/usr/sbin/install_assist </dev/\
console >/dev/console
# 2>&                                                  1
```

Client remains in the STOPPING state if system has unprobed resources

If you attempt to stop VCS One and the system has unprobed resources, the client service (vcsoneclientd) remains in the STOPPING state. Use the `hastop -local -force` option to forcibly stop the service. [1397421]

Installation and uninstallation issues

User-modified types

If you changed any VCS One 2.0.1 types, those changes will be lost when you upgrade to VCS One 5.0.

Changes to user-modified types are lost when you upgrade from VCS One 2.0.1 to 5.0

If you are upgrading to VCS One 5.0, any changes to VCS One 2.0.1 types will be lost.

Upgrading from VCS One 2.0.1 to 5.0 may fail if you only configure one NIC

If you use the `./installvcsonepm -migrate` option to upgrade from VCS One 2.0.1 to VCS One 5.0, the operation may fail if you only configure one NIC. [1843891]

Workaround: Configure more than one NIC in the pmnic resource. If you cannot configure multiple NICs, follow these steps to export your 2.0.1 configuration, upgrade the Policy Master node to 5.0, and import the configuration to VCS One 5.0.

For more details, see the upgrade instructions in *Veritas Cluster Server One Installation Guide*.

1. Export your VCS One 2.0.1 configuration.
2. Install VCS One 5.0 on the Policy Master system.
3. Import the VCS One 2.0.1 configuration to the 5.0 Policy Master system.
4. Stop the VCS One 2.0.1 Policy Master.
5. Configure the VCS One 5.0 Policy Master using the VCS One 2.0.1 cluster ID and virtual IP address.

Installing the Policy Master on Solaris with zones configured is not supported

This release of VCS One does not support installing the Policy Master on Solaris with zones configured. On Solaris, the Policy Master must be installed on a system free of zones.

When VCS and VCS One are installed on the same machine, there are installation and uninstallation considerations

When VCS and VCS One are installed on the same machine, the symlinks in `/opt/VRTS/bin` point to the binaries of the product you install last. If you uninstall VCS or VCS One, the symlinks—such as hares and hagrp—are removed from the `/opt/VRTS/bin` directory.

Workaround: Access the VCS binaries and commands from `/opt/VRTSvcs/bin` and the VCS One binaries from `/opt/VRTSvcsone/bin`.

[1835526]

Removing directories from a local zone on Solaris

When you uninstall VCS One from a global zone, the `/.vcsoneprofile` and `/var/VRTSvcsone/data` directories are not deleted from your local zones. [1828364]

Workaround: Manually remove the directories from your local zones. Enter the following:

```
$> /usr/bin/rm -f /.vcsoneprofile
$> /usr/bin/rm -fr /var/VRTSvcsone
```

When you install VCS One, IPv6 must be enabled to use rcp from a Solaris 8 system to a non-Solaris system

When installing and uninstalling, IPv6 must be enabled to run the `rcp` command from a Solaris 8 system to a non-Solaris system. [545197]

Workaround: To enable IPv6 on a Solaris 8 system, execute the following commands, where *`interface`* is the name of the NIC device:

1 Log in as root on the Solaris 8 system.

2 Run the following command:
ifconfig *interface* inet6 plumb up

3 Create the file `hostname6.`*`interface`* to enable IPv6 each time the system boots:
touch /etc/hostname6.*interface*

Some SSH implementations may cause VCS One installations to fail

The SSH protocol is required for installation of the VCS One client node software. To function successfully during a VCS One installation, `ssh` and `scp` commands must:

- Be passwordless.
- Return 0 for successful command execution.
- Not leave residual processes after successful command execution; this can be verified by using the command: `ps -ef` and scanning the output for any `ssh` or `scp` processes.
- Not make use of banners.

Some implementations of `ssh` and `scp` commands on Solaris fail to meet the above requirements and may cause installations to fail. [574207]

On Linux, if the incorrect netmask is used to plumb the base IP address, the network connection may be lost

If you are installing the Policy Master on Linux, and the incorrect netmask is used to plumb the Base IP address, the network may not work. [1833357]

Workaround: Symantec recommends using MultiNICA Performance Mode in the Policy Master Service Group (PMSG). MultiNICA Performance Mode requires a unique Base IP address with the correct netmask addresses plumbed on the required NICs.

Refer to the *Veritas Cluster Server One Bundled Agents Reference Guide* for information about MultiNICA Performance Mode.

Upgrading VCS One 2.0.1 Windows clients to VCS One 5.0 is not supported

You can upgrade your VCS One 2.0.1 UNIX Policy Master and client systems to VCS One 5.0. However, upgrading VCS One 2.0.1 Windows clients to VCS One 5.0 is not supported. [1827731]

If your VCS One 2.0.1 Policy Master uninstallation is interrupted, you may have problems installing VCS One 5.0

If your VCS One 2.0.1 Policy Master uninstallation is interrupted, the database uninstallation may not be clean. Later, if you want to install the VCS One 5.0 Policy Master, you may have installation problems. [1806831]

Workaround: If you have an `/opt/VRTSvcsone/db` directory, delete it and try the installation again.

When installing VCS One with Storage Foundation, a warning message is logged

When installing VCS One with Storage Foundation, the following warning message is logged:

```
SF WARNING: lwp_default_stksize is set more than once in /etc/
system
```

You may safely ignore this warning message. [934936]

After installing VCS One with Storage Foundation and rebooting, GAB/LLT errors appear

After installing VCS One with Storage Foundation, GAB/LLT errors appear when you first reboot the system. These error messages are expected since configuration has not yet been performed.

You may safely ignore the messages. [935001]

Installing many clients from the same installation session may be time consuming

Installing more than 8 to 12 clients from the same installation session may be time consuming. [1048075]

Workaround: To work around this issue, start installation sessions from different windows to reduce the installation time for a large number of nodes.

You may get installation errors if you use csh

Installation errors may occur if the root user has csh as the default shell. [1804490]

Workaround: Switch the root shell from csh to sh.

When installing the VCS One client on AIX 5.*x*, the xlC.rte version must be 8.0.0.8

If the version of xlC.rte is not 8.0.0.8, installing the VCS One client on AIX 5.*x* fails with the following error:

```
CPI ERROR V-9-0-0 Error in configuring VxSS
```

Before installing the VCS One client on an AIX 5.*x* system that already has Symantec Product Authentication Service (AT) installed, ensure that the xlC.rte version is 8.0.0.8. [1172993]

Installing the Policy Master using Storage Foundation for storing configuration information may produce an error

If you install the Policy Master using Storage Foundation for storing configuration information, the following error messages may appear (this situation is rare):

```
UX:vxfs mount.vxfs: ERROR: V-3-22168: Cannot open portal device:
No such file or directory
UX:vxfs mount.vxfs: ERROR: V-3-25255: mount.vxfs: You don't have
a license to run this program
```

[1279667]

Workaround: If these error messages appear during installation, perform the following work around:

1. Check if the `vxportal` module is loaded:
   `lsmod | grep vxportal`
   If it is not listed, proceed to the next step.
2. Run the following command:
   `/etc/vx/vxfs-startup`
3. Verify that the `vxportal` module is now loaded:
   `lsmod | grep vxportal`
   The `vxportal` module should now be listed.
4. Mount the volume manually. Do one of the following:
   - On Linux, enter the following:
     `mount -t vxfs /dev/vx/dsk/`*`vcsone_dg_name`*`/`*`volume_name`*`/`*`mount_point_name`
   - On Solaris, enter the following:
     `mount -F vxfs /dev/vx/dsk/`*`vcsone_dg_name`*`/`*`volume_name`*`/`*`mount_point_name`

You may now proceed with the installation.

Ignore Perl warning message if you install Storage Foundation after VCS One

If you install Storage Foundation 5.0 using the Storage Foundation installer on a Linux system where the VCS One Policy Master or client is installed, the following warning message appears:

```
CPI WARNING V-9-1-1267 SF version 5.0 includes VRTSperl version
5.0.2.1.  A more recent version of VRTSperl, 5.8.8.0, is already
installed on system1.
CPI WARNING V-9-1-1271 In this situation VRTSperl version
5.8.8.0 will not be installed or downgraded on system1.
SF version 5.0 may not operate correctly with this more recent
rpm.
The VRTSperl rpm must be removed manually before version 5.0.2.1
can be installed.
```

```
Do you want to continue? [y,n,q,?] (n)
```

If you encounter this warning message, answer “yes” (or “y”) to continue and do not downgrade the perl version. [1258357]

The Policy Master is not supported on SLES 9 x64

The installer script on software disc 2 for SUSE Linux Enterprise Server 9 x64 displays an option to install the VCS One Policy Master. This option, however, is not supported. This release of VCS One does not support the Policy Master on this platform. [1386212]

Certain installer script options are for internal use only

The `installer` and `installat` scripts include the following options, which are for internal use only:

`-start`, `-stop`, `-nooptionspkgs`, `-noextrapkgs`, `-installpkgs`, `-requiredpkgs`, `-nohapkgs`, `-serial`

In addition the `installer` script includes the following option for the client, which is for internal use only:

`-nolic`

Do not use these options. [1394206]

On Solaris 10, the installer uses an incorrect path to in.mpathd in an IPMP configuration

On Solaris 10, the VCS One installer uses an incorrect path to `in.mpathd` in an IP multipathing (IPMP) configuration. As a result, the MultiNICB resource alternates between having a state of ONLINE and UNKNOWN. [1451578]

Workaround: To avoid this issue, correct the path for `in.mpathd` in the `types.cf` file. In `types.cf`, edit the `in.mpathd` so that it appears as indicated below in bold.

```
type MultiNICB (
        static int MonitorInterval = 10
        static int OfflineMonitorInterval = 60
        static str ArgList[] = { UseMpathd, MpathdCommand,
ConfigCheck,
MpathdRestart, Device, NetworkHosts, LinkTestRatio, Ig
noreLinkStatus, NetworkTimeout, OnlineTestRepeatCount,
OfflineTestRepeatCount,
NoBroadcast, DefaultRouter, Failback, GroupName
 }
        static str Operations = None
        int UseMpathd
        str MpathdCommand = "/usr/lib/inet/in.mpathd -a"
        int ConfigCheck = 1
        int MpathdRestart = 1
```

Bundled agent issues

Agents may dump core when shutting down on RHEL 4

Veritas VCS One bundled agents may dump core when shutting down if multiple agent threads attempt to exit simultaneously. This problem occurs on Red Hat Enterprise Linux Version 4 (RHEL 4), Updates 1 and 2. [536782]

Workaround: Red Hat can provide a patch to Updates 1 and 2 that resolves this issue (Red Hat Issue-Tracker 82911).

The Agent Pack installer can uninstall agents even when they are running

The Agent Pack installer script can uninstall the following agent packages even if their corresponding agent processes are running. During the pre-uninstallation check for these agents, the script does not check whether the agent processes are running.

This issue applies to the following agents:

- Oracle agent
- Sybase agent
- WebSphere MQ6 agent
- WebLogic9 agent
- WebSphere Application Server agent

[1024748]

The DiskGroup agent may malfunction if you run vxconfigid in DEBUG mode

Running the `vxconfigd` command in DEBUG mode may cause the DiskGroup agent to malfunction. [1125380]

Network agents do not support IPv6 addresses

The VCS One network agents (IP, NIC, IPMultiNIC, IPMultiNICB, MultiNICB, and DNS) do not support IPv6 addresses. The network agents may not work as expected if IPv6 addresses are configured on the system. [1129614]

If you use NFS mount points

If the NFS server is not accessible during the monitoring of an NFS mount, the Mount agent may hang. [1288578]

Workaround: To avoid this issue, for any Mount resource that monitors an NFS mount point, if the value of the Mount agent AccessPermissionChk attribute value is not zero, ensure that the SecondLevelMonitor attribute value is 1.

hasys may display an incorrect agent version

The version displayed for an agent in the output of the following command may not be the correct version:

```
hasys -value sys AgentVersionInfo
```

This issue arises if an agent instance (INST1) has an *agent*.xml file with an agent version that was reported to the Policy Master and stored in the AgentVersionInfo system-level attribute. If you then modify the AgentDirectory attribute to use an agent instance from a different directory (INST2) and that agent's directory does not have an *agent*.xml file, the new agent instance incorrectly displays the version value from INST1. [1287435]

Workaround: To avoid this issue, ensure that the agent's directory contains an *agent*.xml file and that the *agent*.xml file indicates the correct version number for the agent.

The Application agent may not be able to monitor process IDs in the PidFile attribute

If the value of the PidFile attribute for any application contains leading spaces, the Application agent may not be able to parse the file and extract the process ID of the daemon. [1387123]

Workaround: Use the MonitorProgram attribute instead of PidFile. The administrator may write a script that extracts the process ID out of the PidFile attribute and checks that the process ID exists using the ps command. This script may be configured as the MonitorProgram attribute of the application.

For information on how to configure the MonitorProgram attribute, see the *Veritas Cluster Server One Bundled Agents Reference Guide*.

In rare circumstances, vcsoned may hang

In rare circumstances, the Policy Master daemon, vcsoned, may hang after logging the message:

```
Server Farm logger started
```

[1390012]

The LDom agent's CfgFile attribute does not work properly with LDoms 1.0.3

With LDoms 1.0.3, the LDom agent does not create an LDom using the CfgFile attribute value during the online agent function if the LDom does not already exist on the node. This issue occurs because the XML format for the LDom configuration file for LDoms 1.0.3 is different from the format used in prior LDoms versions. [1428091]

Workaround: Perform one of the following two steps to resolve the issue:

- Create the LDom manually on all nodes.

Or:

- Change line 126 in the `/opt/VRTSvcsone/bin/LDom/online` file from:

  ```
  local_xmlldomname=`grep ldom_name ${ldomconfig} | cut -f2 -d"<"
  | cut -f2 -d">"`
  ```

  To:

  ```
  local_xmlldomname=`grep -w VirtualSystem_Type ${ldomconfig} |
  cut -d'"' -f4`
  ```

To create the configuration file for an LDom, run the following command:

```
$ ldm list-constraints -x ldom_name > ldom_name.xml
```

Copy the configuration file to either a shared disk so that all nodes can access it or to all nodes.

In a Solaris LDom environment, the Mount agent may stop heartbeating with the VCS One client, which can cause a core dump

The Mount agent may stop heartbeating with the VCS One client daemon (vcsoneclientd). As a result, vcsoneclientd sends a signal to the Mount agent to obtain a core file. The core that the agent generates results when it stops heartbeating with vcsoneclientd.

This issue occurs only in a Solaris logical domain (LDom) environment where vcsoneclientd runs inside of an I/O domain. That is, the I/O domain has been configured as a client system in the VCS One server farm. This issue is not observed in a non-LDom Solaris environment.

After the agent dumps core, vcsoneclientd starts a new instance of the agent that works without an issue until the next time this event occurs. In a test environment, Symantec has found that the frequency of the core dumps is anywhere between 30 minutes and two hours.

Over a period of time, the diagnostics directory in `/var/VRTSvcsone/diag/` (or the directory configured using the VCS_LOG environment variable) and `/var/core` fills up with the core files generated by the agent. To free up space in the `/var` file system, manually delete the older core files.

There is no workaround for this issue. [1464956]

Fencing issues

I/O fencing on VCS One client system may appear to fail

On some Linux-based VCS One client systems that have been I/O fenced, block writes, which are buffered before being written to the shared disk, may appear to have been successful. In fact, when the writes are reported as failing, as they should, the information is written to the console and may escape notice. [583236]

Workaround: To verify this, you may elect to write to the corresponding raw device, in which case writes that are properly I/O fenced are reported immediately. See Linux operating system documentation for information about the raw command.

Enterprise agents

Oracle and Netlsnr enterprise agents display or ship unsupported action entry points in VCS One configuration

The Oracle and Netlsnr enterprise agents display or ship unsupported action entry points in the VCS One configuration. [1840535]

Oracle unsupported action entry points (under the directory `/opt/VRTSagents/ha/bin/Oracle/actions`):

- DBRestrict
- DBResume
- DBSuspend
- DBTbspBackup
- DBUndoRestrict
- VRTS_GetInstanceName
- VRTS_GetRunningServices
- getid.vfd
- owner.vfd
- home.vfd
- pfile.vfd

Netlsnr unsupported action entry points (under the directory `/opt/VRTSagents/ha/bin/Netlsnr/actions`):

- VRTS_GetInstanceName
- VRTS_GetRunningServices
- tnsadmin.vfd

Documentation

The following sections contain important information about VCS One product documentation.

Email your comments about the documentation to:

clustering_docs@symantec.com

Finding product documentation

Product documents are in Adobe Portable Document Format (PDF) on the software discs.

To access product documentation

- Go to the `docs` subdirectory under the platform-specific directory on any VCS One software disc.
  All VCS One product documentation is included in this location except the *Veritas Cluster Server One Getting Started Guide* (getting_started.pdf). This guide is available at the top level of each VCS One software disc.

Note: Product documentation is not installed with the product. Symantec recommends that you copy the documentation to the `/opt/VRTS/docs` directory for future reference.

About the guides

Table 1-16 lists the titles and file names of the VCS One guides.

Table 1-16 Veritas Cluster Server One documentation set

Document	File name
Veritas Cluster Server One Getting Started Guide	getting_started.pdf
Veritas Cluster Server One Release Notes	vcsone_notes.pdf
Veritas Cluster Server One Installation Guide	vcsone_install.pdf
Veritas Cluster Server One User's Guide	vcsone_users.pdf
Veritas Cluster Server One Command Reference Guide	vcsone_commands.pdf
Veritas Cluster Server One Bundled Agents Reference Guide	vcsone_bundled_agents.pdf
Veritas Cluster Server One Agent Developer's Guide	vcsone_agent_dev.pdf

Table 1-17 shows the guides that are included with VCS One and the recommended order in which to read them.

Table 1-17 Read the VCS One guides in this order

Read in this order	Title	Description
1	Veritas Cluster Server One Getting Started Guide	Provides an overview of the product and the contents of the software discs
2	Veritas Cluster Server One Release Notes	Describes new features, system requirements, known issues, and fixed issues
3	Veritas Cluster Server One Installation Guide	Contains installation instructions and sample installation output
4	Veritas Cluster Server One User's Guide	■ Defines the components, architecture, and theory of operations ■ Outlines VCS One cluster design principles ■ Explains how to use VCS One

Table 1-18 shows the reference guides that are included with VCS One. These guides do not need to be read in a particular order.

Table 1-18 VCS One reference guides

Title	Description
Veritas Cluster Server One Command Reference Guide	Contains information about VCS One commands
Veritas Cluster Server One Bundled Agents Reference Guide	Contains information about the agents that are packaged (bundled) with VCS One
Veritas Cluster Server One Agent Developer's Guide	Explains how to create a custom agent

Table 1-18 VCS One reference guides (Continued)

Title	Description
Examples of enterprise agent guides ■ *Veritas Cluster Server One Agent for Oracle Installation and Configuration Guide* ■ *Veritas Cluster Server One Agent for DB2 Installation and Configuration Guide*	These guides explain how to install and configure enterprise agents. Enterprise agents are not bundled with VCS One. They are included with the Agent Pack.

Online manual pages

On UNIX systems, online manual pages are installed under the following directory:

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

A note about online help

If you notice a discrepancy between information in online help and in the PDF documentation, the information in the PDF documentation is the most current.

Getting help

For technical assistance, visit http://www.symantec.com/business/support/assistance_care.jsp and select phone or email support.