VERITAS Cluster Server 4.1

Release Notes

Solaris

Third-Party Legal Notices

Apache Software

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work.

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source

code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

  (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

  (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

  (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

  (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Data Encryption Standard (DES)

Support for data encryption in VCS is based on the MIT Data Encryption Standard (DES) under the following copyright:

SNMP Software

SNMP support in VCS is based on CMU SNMP v2 under the following copyright:

VERITAS Cluster Server 4.1 Release Notes

This document provides important information regarding VERITAS Cluster Server (VCS) version 4.1 for Solaris 8, 9, and 10 (32-bit and 64-bit). Please review this entire document before installing VCS.

For the latest information on updates, patches, and software issues regarding this release, see the following TechNote on the VERITAS Technical Support website:
http://support.veritas.com/docs/272714

New Features in VCS 4.1

The features described below are introduced in VCS version 4.1.

VERITAS Security Services (VxSS)

VCS 4.1 integrates with VERITAS Security Services (VxSS) to provide secure communication between cluster nodes and clients, including the Java and the Web consoles. VxSS uses digital certificates and uses SSL to encrypt communication over the public network.

User Management in the Secure Mode

Change in Behavior: If VCS is running in the secure mode, you can add system or domain users to VCS and assign them privileges. You must specify user names in the format username@domain. You cannot assign or change passwords for users when VCS is running in the secure mode.

NFS Lock Failover

VCS 4.1 adds support for failover of NFS 3.0 file locks.

JumpStart Compliance

VCS 4.1 is compliant with Solaris JumpStart technology.

Web Console Features

◆ Support for secure clusters

◆ Support for modifying the system list

◆ Support for overriding static resource type attributes

Java Console Features

◆ Support for secure clusters

◆ Support for overriding static resource type attributes

◆ Simulator Console for managing simulated clusters

Change to DiskGroup Agent Handling of noautoimport Flag

To maintain control of a disk group resource, VCS requires the `noautoimport` flag of the disk group to be explicitly set to true. Previously, the DiskGroup agent took a service group offline if a disk group without `noautoimport` set to true was imported outside VCS.

Change in Behavior: To avoid disruption to applications, the DiskGroup agent now changes the value of the `noautoimport` flag to true when a disk group resource is brought under VCS control. VxVM provides a new command option for changing the value of the `noautoimport` flag to false.

New Bundled Agents

The following bundled agents are added in the VCS 4.1 release. For details, refer to the *VCS 4.1 Bundled Agents Reference Guide*.

◆ CampusCluster

◆ NFSLock

◆ ProcessOnOnly

◆ Zone

New Attributes

The following VCS attributes have been added in the VCS 4.1 release.

- ◆ Resource Type Attributes
  - ContainerName
  - ContainerType
- ◆ Cluster Attribute
  - PanicOnNoMem

Removed Attributes

The following VCS attributes have been removed in the VCS 4.1 release.

- ◆ Cluster Attribute
  - AllowNativeCliUsers
- ◆ Service Group Attributes
  - PreOffline
  - PreOfflining

VCS Agents

Bundled Agents

The following agents are included with VCS. For information on any of the agents listed below, refer to the *VCS 4.1 Bundled Agents Reference Guide*.

Application	CampusCluster	Disk
DiskGroup	DiskReservation	DNS
ElifNone	FileNone	FileOnOff
FileOnOnly	IP	IPMultiNIC
IPMultiNICB	Mount	MultiNICA
MultiNICB	NFS	NFSLock
NIC	NotifierMngr	Phantom
Process	ProcessOnOnly	Proxy
ServiceGroupHB	Share	Volume
VRTSWebApp	Zone	

Enterprise Agents

Enterprise agents are sold separately. Contact your VERITAS sales representative for details about these agents, additional agents under development, and agents available as part of Storage Foundation products or through VERITAS Consulting Services.

Note Before configuring an enterprise agent with VCS 4.1, verify that you have the latest version of the agent.

Supported Enterprise Agents

Available VCS 4.1 enterprise agents are listed below. Refer to this table for supported application and operating system versions. VCS agents support a specified application version on Solaris 10 if the application vendor supports that version on Solaris 10.

Supported VCS Agent	Agent version	VCS version				Application		OS		
		2.0	3.5	4.0	4.1			8	9	10
Sun ONE	4.0	p	p	s	s	Administration Server		s	s	s
						Messaging Server	5.0, 5.1, 5.2			
						Messaging Multiplexor	5.0, 5.1, 5.2			
						Directory Server	5.0, 5.1, 5.2			
						Web Server	4.1, 6.0, 6.1			
						Proxy Server	3.6			
						SOCKS Server	3.6			
Oracle	4.1	p	p	s	s	Oracle	8.0.x, 8*i*, 9*i* R1, 9*i* R2 10g	s	s	s
DB2	4.1	p	p	s	s	DB2 Enterprise Server Edition	7.2, 8.1, 8.2	s	s	s
Sybase	4.0	p	p	s	s	Sybase Adaptive Server	11.x–11.9.2 12.0, 12.5	s	s	s
Informix	1.3.0	s	s	s	s	Informix Dynamic Server	7.1–9.4	s	s	s
True Copy	4.1	n	n	s	s	Hitachi True Copy		s	s	s
SRDF	4.1	n	n	s	s	EMC Symmetrix Remote Data Facility		s	s	s
PPRC	4.1	n	n	s	s	IBM Peer-to-Peer Remote Copy		s	s	s

s – supported configuration   n – not supported   p – supported by previous version of agent

Custom Agents

Compiling Custom Agents

Custom agents developed in C++ must be compiled using SUNWspro 5.0 or Forte Developer 6 compilers. Note that an agent framework library is available for use with custom agents compiled with SUNWspro 4.x compilers.

The following is the layout of `libvcsagfw.so` in `/usr/lib`:

> `/usr/lib/libvcsagfw.so --> . /libvcsagfw.so.2`
>
> > (compatible with SUNWspro5.0 and Forte Developer 6 compilers)
>
> `/usr/lib/libvcsagfw.so.1`
>
> > (compatible with SUNWspro 4.x)

All the agents developed on VCS 1.3 and 2.0 will continue to work since they link with `libvcsagfw.so.1`. If SUNWspro 4.x is used to compile a new custom agent, `libvcsagfw.so` should link to `libvcsagfw.so.1` during link time. After the agent is developed, relink `libvcsagfw.so` to `libvcsagfw.so.2`.

Upgrading Custom Agents

Custom agents developed prior to VCS 1.3 must be upgraded before they can be used with VCS 4.1. See the *VCS 4.1 Agent Developer's Guide* for instructions on how to upgrade custom agents.

Installation Notes

Supported Hardware

The compatibility list contains information about supported hardware and is updated regularly. Visit http://support.veritas.com for the latest information on supported hardware, or contact your VERITAS sales representative.

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

Supported Software

◆ Solaris 8, 9, and 10 operating systems (32-bit and 64-bit)

For each platform, we recommend applying the latest Solaris operating system patches available from Sun. See the following site:

```
http://sunsolve.Sun.com
```

◆ VERITAS Volume Manager (VxVM) 3.5, 4.0, and 4.1

◆ VERITAS File System (VxFS) 3.5, 4.0, and 4.1

System Requirements

Requirements for Cluster Manager Consoles

The minimum requirements on Solaris clients are Ultra5 or greater, 256MB RAM, and 1280x1024 display resolution. The color depth of the monitor must be at least 8-bit (256 colors), although 24-bit is recommended.

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

The following supported Internet browsers have been tested:

◆ Internet Explorer 5.0, 5.5, and 6.0

◆ Netscape 6.2 and 7.0

Patches for Cluster Manager

Patches from Sun for Java 2 Standard Edition (J2SE) are required to use the Java-based graphical user interface, Cluster Manager (Java Console); and the web-based graphical user interface, Cluster Manager (Web Console). Apply the patches for J2SE that are required for your Solaris operating system. Patches are available from Sun at:

```
http://java.sun.com/j2se/1.4.2/download.html
```

Do Not Use Solaris 2.8 Patch 110934-10 or Solaris 2.9 Patch 113713-01

Solaris 2.8 patch 110934-10 and Solaris 2.9 patch 113713-01 prevent the installation of VCS, VxVM, and GLM patches.

By using the showrev -p command, you can display the currently installed patches and their levels. For example, to check for patch 110934-10, enter:

```
# showrev -p | grep 110934
```

If you have patch 110934-10 (Solaris 2.8) or patch 113713-01 (Solaris 2.9) installed, you must remove it using the patchrm command:

```
# patchrm 110934-10
```

After the Solaris patch is removed, VERITAS packages can be installed.

For Solaris 2.8, you can use patch 110934-08 or lower. If you do not have or cannot obtain patch 110934-08, do not install 110934-10. You can successfully install the VERITAS packages without either patch.

The latest status of patches 110934-10 and 113713-01 for use with specific VERITAS products is available at http://support.veritas.com.

Installing or Upgrading to VCS 4.1

Refer to the *VERITAS Cluster Server 4.1 Installation Guide* for instructions on how to install VCS 4.1 and how to upgrade to VCS 4.1 from earlier versions of VCS. The *VCS 4.1 Installation Guide* is in the cluster_server/docs directory of the software disc.

Obtaining License Keys for VCS

VCS is a licensed software product. For information on obtaining licence keys for VCS, refer to the *Getting Started Guide* or the *VCS 4.1 Installation Guide.*

VCS Packages

The following packages for VCS are in the `/cluster_server/pkgs` directory:

- ◆ `VRTSat`, VERITAS Authentication Service
- ◆ `VRTScpi`, VERITAS Common Product Installer
- ◆ `VRTScscm`, VCS Cluster Manager (Java Console)
- ◆ `VRTScscw`, VCS Configuration Wizards
- ◆ `VRTScsim`, VCS Simulator
- ◆ `VRTScutil`, VERITAS Cluster Utility
- ◆ `VRTSgab`, Group Membership and Atomic Broadcast
- ◆ `VRTSllt`, Low Latency Transport
- ◆ `VRTSperl`, VERITAS Perl
- ◆ `VRTSvcs`, VERITAS Cluster Server
- ◆ `VRTSvcsag`, VCS Bundled Agents
- ◆ `VRTSvcsdc`, VCS Documentation
- ◆ `VRTSjre`, VCS JRE redistribution
- ◆ `VRTSvcsmg`, VCS Message Catalogs
- ◆ `VRTSvcsmn`, VCS Manual Pages
- ◆ `VRTSvcsw`, Cluster Manager (Web Console)
- ◆ `VRTSvlic`, VERITAS License Utilities
- ◆ `VRTSvxfen`, VCS Fencing Driver
- ◆ `VRTSweb`, VERITAS Web GUI Engine

The following packages for VCS are in the `/windows/WindowsInstallers` directory:

- ◆ `WindowsClusterManager`, Cluster Manager for Windows clients
- ◆ `WindowsSimulator`, VCS Simulator for Windows clients
- ◆ `WindowsWebConsole`, VCS Web Console for Windows clients

Software Limitations

The following limitations apply to VCS version 4.1.

Cluster Manager (Java Console)

Java Console for VCS 4.x is Required

Cluster Manager (Java Console) from VCS versions earlier than 2.0 cannot be used to manage VCS 4.x clusters. VERITAS recommends always using the latest version of Cluster Manager. See the *VERITAS Cluster Server 4.1 Installation Guide* for instructions on upgrading Cluster Manager.

Running Java Console on a Non-Cluster System is Recommended

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

Print Option in Java Console Help Requires Configured Printer

A Solaris system running Cluster Manager (Java Console) must have a printer configured if the printing option is to be used. If a printer is not configured to the system on which the Java Console runs, the Java Console may hang when the "Print" button is clicked in the online JavaHelp. This is a known problem related to components of JavaHelp.

Cluster Manager (Web Console)

Cluster Name Should Not Include Single or Double Quotes

If a cluster name includes single or double quotes, some cluster views and operations in the Web Console will not function correctly.
Workaround: Verify that the ClusterName attribute for the cluster includes only valid characters.

Changes to UserStrGlobal for ClusterService May Disrupt Cross-Product Navigation

The Web Console uses the UserStrGlobal attribute of the ClusterService service group. Changes to this attribute may disrupt cross-product navigation through the Web Console.
Workaround: Do not edit the default value of UserStrGlobal for the ClusterService service group.

IBM Home Page Reader Does Not Enable Service Group Priority and Startup Options

The Priority and Startup options are not enabled when a service group is configured using IBM Home Page Reader.
Workaround: If necessary, edit the Priority and AutoStartList attributes after adding the service group.

Undocumented Commands, Command Options, and Libraries

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

Upgrades from Pre-2.0 Versions of VCS Using installvcs Utility

The `installvcs` utility does not configure Cluster Manager (Web Console), SNMP, and SMTP during upgrades of VCS from versions before 2.0. To use these features, you must manually configure them in the `main.cf` file after upgrading. Refer to the *VCS 4.1 User's Guide* for information on manually creating a ClusterService service group in which to configure these resources.

Stopping Systems in Clusters with I/O Fencing Configured

The I/O fencing feature protects against data corruption resulting from a failed cluster interconnect, or "split brain." See the *VCS User's Guide* section titled "VCS Communications, Membership and I/O fencing" for a description of the problems a failed interconnect can create and the protection I/O fencing provides.

I/O fencing uses SCSI-III Persistent Reserve keys to implement data protection. Keys are placed on I/O fencing coordinator disks and on data disks. The VCS administrator must be aware of several operational changes needed when working with clusters protected by I/O fencing. Specific shutdown procedures ensure keys are removed from coordinator disks and data disks to prevent possible difficulties with subsequent cluster startup.

Using the `reboot` command rather than the `shutdown` command bypasses shutdown scripts and can leave keys on the coordinator disks and data disks. Depending on the order of reboot and subsequent startup events, the cluster might warn of a possible split brain condition and fail to start up.
Workaround: Use the `shutdown -r` command to perform a graceful reboot for systems, instead of using the `reboot` command.

System Names in VCS

The name of a system specified in the VCS configuration file, `main.cf`, must not use the fully qualified form; that is, it must not include periods. The name in `main.cf` must be consistent with the name used in `/etc/nodename` and `/etc/llthosts`. If the name listed in `/etc/nodename` is fully qualified, VCS uses only the first segment of the name. If you create the file `/etc/VRTSvcs/conf/sysname` such that it contains the system name to be used by `main.cf`, VCS uses it to verify the system name.

Cluster Address for Global Cluster Requires Resolved Virtual IP

The Virtual IP address must have a DNS entry if virtual IP is used for heartbeat agents.

Link to VCS Traffic Director from the TDService Group in VCS

Navigation from the TDService Group Summary page in the VCS Web Console takes you to the System Overview page in VCS Traffic Director. There, you can select a domain from the list of configured VCS Traffic Director domains.

MultiNICB Agent on Solaris 8 Requires Solaris Patch

If you are running MultiNICB Agent on Solaris 8, you must have the Solaris 8 10/00 patch (Solaris 8 update 2). Obtain it from `http://www.sun.com/patches`.

Using Agents in NIS

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

Networking Agents Do Not Support IPv6 Protocol

The VCS 4.1 bundled IP, NIC, IPMultiNICB, and MultiNICB agents do not support the IPv6 enhanced IP protocol made available in Solaris 8.

Volume Agent Clean May Forcibly Stop Volume Resources

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

VCS Does Not Provide a Bundled Agent for Volume Sets

VCS 4.1 does not provide a bundled agent to detect Volume Manager volume sets, Problems with volumes and volume sets can only be detected at the DiskGroup and Mount resource levels.

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

Fire Drill Does Not Support Volume Sets

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

Manually Removing VRTSat Package Erases User Credentials

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

▼ **To save user credentials**

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

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

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

▼ **To restore user credentials**

1. Navigate to the SnapShot directory:

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

2. Restore the files:

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

Systems in a Cluster Must Have Same System Locale Setting

VCS 4.1 does not support clustering of systems with different system locales. All systems in a cluster must be set to the same locale.

Hardware Replication Agents are Not Localized

VCS 4.1 enterprise agents for IBM PPRC, EMC SRDF, and Hitachi TrueCopy are not localized with this release.

Service Group Dependency Limitations

No Failover for Some Instances of Parent Group

In service groups in which the group dependency is configured as parallel parent/failover child, online global, remote soft or firm, the parent group may not online on all nodes after a child group faults.

Online Local Firm Dependency Violation

If the parent group and the child group are online on node 1, and if the child group faults, VCS begins to take the parent group offline. However, this occurs at the same time the child group is failing over to node 2. If the parent group fails to go completely offline and the child group goes online on node 2, thus resulting in a dependency violation.

Online Remote Firm Dependency Violation

If the parent group is online on node 1 and the child group is online on node 2 and faults, the child group selects node 1 as its failover target. This scenario results in a dependency violation because the parent group fails to go offline on node 1.

Concurrency Violation with Online Firm Dependencies

The concurrency violation trigger cannot offline a service group if the group has a parent online on the system with local firm dependency. The concurrency violation continues until the parent is manually taken offline.
Workaround: In this situation, VCS sends notification that the violation trigger failed to offline a service group that is in concurrency violation. The administrator can manually offline the parent group and then the child group.

Known Issues

The following issues have been reported for VCS version 4.1.

Cluster Manager Installation on Windows XP

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

Workaround: Select Retry rather than Cancel in the error dialog. The installer continues to install Cluster Manager correctly.

License Package Not Completely Removed From Local Zones

Some files from the VERITAS licensing package (VRTSvlic) may not be removed from a local zone that was created after VRTSvlic was originally installed. An error message is displayed if all files are not removed.

Workaround: After the package removal process ends, run the following command from the global zone to remove any remaining VRTSvlic files:

  # **rm -rf *zonepath*/root/var/sadm/pkg/VRTSvlic**

If you are upgrading a product and local zones are configured, instead of using the installer upgrade procedure (or running the script from the command line), perform the upgrade in steps: Uninstall the product, uninstall the infrastructure packages using the uninstallinfr script, and then reinstall the product.

Global Service Groups

Cross-Cluster Switch May Cause Concurrency Violation

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

Group Does Not Go Online on AutoStart Node

Upon cluster startup, if the last system on which the global group is probed is not part of the group's AutoStartList, then the group will not AutoStart in the cluster. This issue affects only global groups. Local groups do not experience this behavior
Workaround: Ensure that the last system to join the cluster is a system in the group's AutoStartList.

Declare Cluster Dialog May Not Display Highest Priority Cluster as Failover Target

When a global cluster fault occurs, the Declare Cluster dialog enables you to fail groups over to the local cluster. However, the local cluster may not be the cluster assigned highest priority in the cluster list.
Workaround: To bring a global group online on a remote cluster, do one of the following:

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

◆ From the Web Console, use the Operations links available on the Service Groups page to bring the global group online on a remote cluster.

Cluster Manager (Web Console)

Cluster Manager or myVCS May Generate Null Pointer Error

You cannot log in to the Web Console or configure myVCS if CmdServer is not running on the systems in the cluster. The message "Error 500. NullPointerException" appears in the browser.
Workaround: Verify that the CmdServer process is running on the cluster systems using the ps -ef | grep CmdServer command. If CmdServer is not running, start it by typing /opt/VRTSvcs/bin/CmdServer at the command line. Once CmdServer is running, you can log in to Cluster Manager or configure myVCS.

Netscape Browser May Not Display Attribute ScreenTips Completely

The Netscape browser may not display the entire ScreenTip for an attribute in the VCS Web Console.
Workaround: If the ScreenTip for an attribute is not completely visible, open the attribute dialog box to view the full description.

The myVCS Page May Not Display Correctly After Initial Configuration

The Netscape browser may not display the entire ScreenTip for an attribute in the VCS Web Console.
Workaround: If the myVCS page or any Cluster Manager page does not display correctly, refresh the page.

LLT Module on Solaris 10 May Not Unload

When uninstalling VCS 4.1, LLT may not unload. This issue is specific to Solaris 10.
Workaround: If LLT does not unload, you must reboot the system.

Volume Agent May Hang

Under extreme conditions, the volume agent may hang. This behavior has been observed under the following circumstances:

◆ Failover for the JNI Fibre Channel driver (JNIfcaPCI) was set to 0. Note this is *not* failover for VCS. The JNI driver has a variable called "failover" that defines the number of seconds after the target is declared offline and before it is declared failed. When target is declared failed, all pending commands are flushed back to the application. This failover value is set in the file `/kernel/drv/fca-pci.conf`. Setting failover to 0 means that the target is never declared failed. With failover for the JNI driver set to 30 seconds, VCS agent behavior was normal.

◆ Fibre cable was disconnected from the switch (to simulate failure of the Fibre drives).

In general, an agent can hang when it attempts to cancel a service thread executing a C++ entry point that has timed out if that entry point has issued a blocking call that is not a valid cancellation point.

AutoStart May Violate Limits and Prerequisites Load Policy

The load failover policy of Service Group Workload Management may be violated during AutoStart when all of the following conditions are met:

◆ More than one autostart group uses the same Prerequisites.

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

◆ The offline group is probed before the online group is probed.

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

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

Erroneous Message in Engine Log File

When VCS tries to mount a `vxfs` file system for the first time, you may receive a misleading message resembling the following:

```
/dev/vx/dsk/sharedg/vol03 is not a vxfs file system
```

Before VCS can mount a `vxfs` file system for the first time, the `fsck` utility needs to run. The message shown above is displayed, `fsck` is run, and the file system is mounted.

Engine May Hang in Leaving State

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

Monitoring PidFiles May Give False Concurrency Violation

When using PID Files to monitor application resources, the Application agent may report a false concurrency violation after a system crash. The PID files created by an application contain the PIDs for processes that are monitored by the Application agent. These files remain even after a node running the application crashes.

When restarting the node, the operating system may assign the PIDs listed in the PID files to other processes running on the node. If the Application agent monitors the resource using the PidFiles attribute only, the agent may discover the processes running and report a false concurrency violation. This scenario could result in some processes that are not under VCS control being killed.

Error Handling by VCS Enterprise Agent for Oracle

The VCS enterprise agent for Oracle provides enhanced handling of Oracle errors encountered during detailed monitoring. The agent uses the reference file `oraerror.dat`, which consists of a list of Oracle errors and the actions to be taken. Refer to the *VCS Enterprise Agent 4.1 for Oracle Installation and Configuration Guide* for a description of the actions.

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

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

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

Non-Specific Oracle Error Message When Number of Allowed Connections Exceeded

VCS uses the `svrmgrl` command to connect to Oracle. In Oracle 8*i*, the `svrmgrl` command gives a non-specific Oracle error message when a system reaches the maximum number of connections: `ORA-01034` (database unavailable) rather than the more specific `ORA-00020` (connections exceeded). As a result, the Oracle agent fails over the service group even though the error can be safely ignored.
Workaround: If exceeding the number of connections is common in your environment, reduce severity of the action in the `oraerror.dat` file from FAILOVER to WARN.

VCS in Japanese Locales

The following issues apply to VCS 4.1 in a Japanese locale.

Installer Does Not Create User Account and Password

The product installer does not ask for a VCS user account and password in a Japanese locale. Only the English installer provides this function.
Workaround: Use the `hauser` command to create VCS user accounts after installation is complete.

Web Server Configuration Page Offers Two Locale Options

The VCS Java Console uses a Web server component called VRTSweb. The configuration page for the Web server offers two Japanese locale options. Both options have UTF-8 encoding, and there are no functional difference between the two.
Workaround: Select either Japanese locale when configuring the Web server component.

The getcomms Command Does Not Create Diagnostic File

The `getcomms` command does not successfully create a `.tar` diagnostic file in a Japanese locale.
Workaround: Change the system environment to LANG=C before running the `getcomms` command.

Fixed Issues and Enhancements

Fixed issues and software enhancement requests are referenced by incident number and described briefly below.

Fixes and Enhancements in VCS 4.1

Incident Number	Description
254859	HAD assert failure when remaining node in 3-nodes cluster is stuck in LEAVING state.
256656	Support CVM-VVR with GCO option.
256715	Application agent hangs when tried to kill a thread calling getpwnam_r.
256739	Mount agent does not work on layered mount points.
256823	The `hasim` command works only when issued with full path even if PATH variable set.
257920	DB2 resources cannot be cleaned or taken offline if the InstanceHome is lost.
258158	Modify DiskGroup behavior when noautoimoprt is set to off.
259670	Add support for overriding attribute s from Cluster Manager.
260093	If vxdg import returns error, parse the return code to determine appropriate action.
263481, 277410	The `hastop -all` command should offline remote global parent groups online on other systems before offlining child group.
265690	Add ProcessOnOnly agent to online and monitor the VxSS security process.

Fixes and Enhancements in VCS 4.0 MP1

Incident Number	Description
i139968	Sun's thread_create default stack size has been increased.
i140725	In some scenarios, when HAD reboots specific nodes, HAD does not dump core.
i142169	Some unidirectional traffic with LLT now performs normally.
i142236	In some scenarios, FromQ and TargetCount are properly cleaned.
i143716	Resolved LLT connect issues when bcasthb disabled.
i143829	For LLT over UDP, behavior is normal when disconnecting a single link when arp and bcast are active.
i144076	The DiskGroup agent monitor now checks "enabled" and "booted" modes.
i144121	Netlsnr online script starts the 8.1.5 Listener resource normally.
i144489	The option -vv for llstat is now included in command line syntax.
i144953	The Mount agent can handle file system checkpoints.
i145328	The Mount agent supports NFS.
i145496	Db2udb agent returns UNKNOWN states in appropriate cases.
i145832	Improved LLT performance reduces the chance of delivery threads to miss wakeups due to a race condition.
i145960	The HAD process no longer writes to /dev/console, it uses the syslog() API for logging event messages, thus avoiding heartbeat failures.
i146046	Fix to db2nps utility that was causing DB2 Enterprise agent performance issues.
i146091	MultiNICB agent does not add default route of ffffffff for an empty DefaultRouter value.
i146369	You can now configure the number of HAD restarts before GAB panic.
i147547	Addressed a potential security flaw.

VCS Documentation

Documentation for VCS is included on the *VERITAS* software discs in Adobe Portable Document Format (PDF). The installation guide for VCS is in the directory `cluster_server/docs`. Release notes for VCS are in the directory `cluster_server/release_notes`.

◆ `vcs_install.pdf`, *Installation Guide*

◆ `vcs_notes.pdf`, *Release Notes*

  VERITAS recommends copying the installation guide and release notes from the CD to the `/opt/VRTS/docs` directory so that they are available on your system for reference.

Additional documentation for VCS is in the `VRTSvcsdc` package:

◆ `vcs_agent_dev.pdf`, *Agent Developer's Guide*

◆ `vcs_bundled_agents.pdf`, *Bundled Agents Reference Guide*

◆ `vcs_users.pdf`, *User's Guide*

◆ `vcs_appnote_f15k.pdf`, *Application Note: Sun Fire 12K/15K Dynamic Reconfiguration*

◆ `vcs_appnote_s6800.pdf`, *Application Note: Sun Fire 6800 Dynamic Reconfiguration*

◆ `vcs_appnote_e10k.pdf`, *Application Note: Sun Enterprise 10000 Dynamic Reconfiguration*

VERITAS Documentation Disc

Documentation is available in HTML format on the searchable VERITAS Documentation Disc included with your software purchase.

VERITAS Documentation Online

Visit the Web site for VERITAS Cluster Server for UNIX:

  http://support.veritas.com/menu_ddProduct_CLUSTERSERVER.htm

to download VERITAS Cluster Server documentation for current and previous releases.

Hard-Copy Documentation Set

Copies of VERITAS software guides are available for purchase through the VERITAS Web Store™ at http://www.veritas.com/webstore.

The following guides for VCS 4.1 on Solaris are available:

◆ *Installation Guide*

◆ *User's Guide*

◆ *Agent Developer's Guide*

◆ *Bundled Agents Reference Guide*

◆ *Application Note: Sun Fire 12K/15K Dynamic Reconfiguration*

◆ *Application Note: Sun Fire 6800 Dynamic Reconfiguration*

◆ *Application Note: Sun Enterprise 10000 Dynamic Reconfiguration*

Manual Pages

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

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

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

For C shell (csh or tcsh), type:

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

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

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Support Web Site

For technical assistance, visit the VERITAS Technical Services Web site at
http://support.veritas.com. From there you can:

◆ Contact the VERITAS Technical Services staff and post questions.

◆ Download the latest patches and utilities.

◆ View the VERITAS Cluster Server Frequently Asked Questions (FAQ) page.

◆ Search the knowledge base for answers to technical support questions.

◆ Receive automatic notice of product updates.

◆ Learn about VERITAS Cluster Server training.

◆ Read white papers related to VERITAS Cluster Server.

◆ Access the latest product documentation and technical notes.

Subscribing to VERITAS Email Notification Service

Subscribe to the VERITAS Email notification service to be informed of software alerts,
newly published documentation, beta programs, and other services.

Go to http://support.veritas.com. Select a product and click "E-mail Notifications" on the
right side of the page. Your customer profile ensures you receive the latest VERITAS
technical information pertaining to your specific interests.

Accessing VERITAS Telephone and Fax Support

Telephone support for VERITAS Cluster Server is only available with a valid support
contract. To contact VERITAS for technical support, dial the appropriate phone number
listed on the Support Guide included in the product box and have your product license
information ready for quick navigation to the proper support group.

The address for the VERITAS telephone support directory is http://support.veritas.com.
Select a product and click "Contact Support" on the right side of the page.

Contacting VERITAS Licensing

For license information, call 1-650-527-0300 or fax 1-650-527-0952.

Troubleshooting Problems

VERITAS Technical Services provides diagnostic tools to assist you in troubleshooting problems associated with the product. These tools are available on disc or can be downloaded from the VERITAS FTP site. See the VRTSspt readme file in the /support directory for details.