

Veritas™ Cluster Server Release Notes

Solaris

5.1 Service Pack 1



Veritas™ Cluster Server Release Notes

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

Product version: 5.1 SP1

Document version: 5.1SP1.1

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

Symantec Corporation
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 support 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/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

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

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/contact_techsupp_static.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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support 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

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support 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 [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec Web site.

<https://sort.symantec.com/documents>

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

docs@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

<https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation>

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

<http://www.symantec.com/connect/storage-management>

Release Notes

This document includes the following topics:

- [About this document](#)
- [Component product release notes](#)
- [About Veritas Cluster Server](#)
- [About Symantec Operations Readiness Tools](#)
- [Important release information](#)
- [Changes in version](#)
- [VCS system requirements](#)
- [Features no longer supported](#)
- [Fixed issues](#)
- [Known issues](#)
- [Software limitations](#)
- [Documentation errata](#)
- [Documentation](#)

About this document

This document provides important information about Veritas Cluster Server (VCS) version 5.1 SP1 for Solaris. Review this entire document before you install VCS.

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

This is Document version: 5.1SP1.1 of the *Veritas Cluster Server Release Notes*. Before you start, ensure that you are using the latest version of this guide. The latest product documentation is available on the Symantec Web site at:

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

Component product release notes

In addition to reading this Release Notes document, review the component product release notes before installing the product.

Product guides are available at the following location in PDF formats:

/product_name/docs

Symantec recommends copying the files to the `/opt/VRTS/docs` directory on your system.

This release includes the following component product release notes:

- *Veritas Storage Foundation Release Notes (5.1 SP1)*

About Veritas Cluster Server

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

About VCS agents

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

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

The Veritas High Availability Agent Pack gives you access to agents that provide high availability for various applications, databases, and third-party storage solutions. The Agent Pack is available through Symantec™ Operations Readiness Tools (SORT).

For more information about SORT, see <https://sort.symantec.com/home>.

For information about agents under development and agents that are available through Symantec consulting services, contact your Symantec sales representative.

VCS provides a framework that allows for the creation of custom agents. Create agents in situations where the Veritas High Availability Agent Pack, the bundled agents, or the enterprise agents do not meet your needs.

For more information about the creation of custom agents, refer to the *Veritas Cluster Server Agent Developer's Guide*. You can also request a custom agent through Symantec consulting services.

About compiling custom agents

Custom agents developed in C++ must be compiled using Forte Developer 6 compilers. The following is the layout of `libvcsagfw.so` in `usr/lib`:

```
/usr/lib/libvcsagfw.so --> . /libvcsagfw.so.2
```

If you use custom agents compiled on older compilers, the agents may not work with VCS 5.1SP1. If your custom agents use scripts, continue linking to `ScriptAgent`. Use `Script50Agent` for agents written for VCS 5.0 and above.

About Symantec Operations Readiness Tools

Symantec™ Operations Readiness Tools (SORT) is a set of Web-based tools and services that lets you proactively manage your Symantec enterprise products. SORT automates and simplifies administration tasks, so you can manage your data center more efficiently and get the most out of your Symantec products. SORT lets you do the following:

- Collect, analyze, and report on server configurations across UNIX or Windows environments. You can use this data to do the following:
 - Assess whether your systems are ready to install or upgrade Symantec enterprise products
 - Tune environmental parameters so you can increase performance, availability, and use
 - Analyze your current deployment and identify the Symantec products and licenses you are using
- Upload configuration data to the SORT Web site, so you can share information with coworkers, managers, and Symantec Technical Support
- Compare your configurations to one another or to a standard build, so you can determine if a configuration has "drifted"
- Search for and download the latest product patches
- Get notifications about the latest updates for:

- Patches
- Hardware compatibility lists (HCLs)
- Array Support Libraries (ASLs)
- Array Policy Modules (APMs)
- High availability agents
- Determine whether your Symantec enterprise product configurations conform to best practices
- Search and browse the latest product documentation
- Look up error code descriptions and solutions

Note: Certain features of SORT are not available for all products.

To access SORT, go to:

<http://sort.symantec.com>

Important release information

- The latest product documentation is available on the Symantec Web site at: <http://www.symantec.com/business/support/overview.jsp?pid=15107>
- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website: <http://entsupport.symantec.com/docs/334829>
- For the latest patches available for this release, go to: <http://sort.symantec.com/>

Changes in version

This section lists the changes for Veritas Cluster Server.

Changes related to the installation

The product installer includes the following changes.

Rolling upgrade support

To reduce downtime, the installer supports rolling upgrades. A rolling upgrade requires little or no downtime. A rolling upgrade has two main phases. In phase

1, the installer upgrades kernel packages on a subcluster. In phase 2, non-kernel packages are upgraded.

All high availability products support a rolling upgrade. You can perform a rolling upgrade from 5.1 or from any RPs to the current release.

You can perform a rolling upgrade using the script-based or Web-based installer. See the *Veritas Cluster Server Installation Guide*.

Installer-related changes to configure LLT private links, detect aggregated links, and configure LLT over UDP

For all high availability products, the installer provides the following new features in this release to configure LLT private links during the VCS configuration:

- The installer detects and lists the aggregated links that you can choose to configure as private heartbeat links.
- The installer provides an option to detect NICs on each system and network links, and sets link priority to configure LLT over Ethernet.
- The installer provides an option to configure LLT over UDP.

See the *Veritas Cluster Server Installation Guide*.

Installer changes related to I/O fencing configuration

In VCS 5.1 or SFHA 5.1, the installer started I/O fencing in disabled mode even if you had not chosen to configure I/O fencing. In 5.1 SP1, if you did not choose to configure I/O fencing during the product configuration, then the installer does not start I/O fencing in disabled mode in VCS and SFHA clusters.

However, if you upgrade VCS or SFHA from 5.1 to 5.1SP1, the installer retains the I/O fencing configuration from the previous version.

Installer supports configuration of non-SCSI3 based fencing

You can now configure non-SCSI3 based fencing for VCS cluster using the installer.

See the *Veritas Cluster Server Installation Guide*.

Web-based installer supports configuring VCS cluster in secure mode

You can now configure the VCS cluster in secure mode using the Web-based installer.

See the *Veritas Cluster Server Installation Guide*.

The installer can copy CPI scripts to any given location using `-copyinstallscripts` option

The installer can copy CPI scripts to given location using `-copyinstallscripts` option. This option is used when customers install SFHA products manually and require CPI scripts stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media.

See the *Veritas Cluster Server Installation Guide*.

Web-based installer supports configuring disk-based fencing for VCS

You can now configure disk-based fencing for the VCS cluster using the Web-based installer.

See the *Veritas Cluster Server Installation Guide*.

The Web-based installer supports adding nodes

The Web-based installer has increased parity with the script-based installer. It now supports the ability to add nodes to a cluster. It also supports configuring secure clusters and fencing configuration.

The installer provides automated, password-less SSH configuration

When you use the installer, it enables SSH or RSH communication among nodes. It creates SSH keys and adds them to the authorization files. After a successful completion, the installer removes the keys and system names from the appropriate files.

When you use the installer for SSH communications, meet the following prerequisites:

- The SSH (or RSH) daemon must be running for auto-detection.
- You need the superuser passwords for the systems where you plan to install VCS.

The installer can check product versions

You can use the installer to identify the version (to the MP/RP/SP level depending on the product) on all platforms. Activate the version checker with `./installer -version system_name`.

Depending on the product, the version checker can identify versions from 4.0 onward.

Upgrade changes

The following lists the upgrade changes in this release.

Supported paths for VCS upgrades that do not require a node reboot

When using the installer program to perform any of the typical upgrade listed in the following upgrade matrix, a node reboot is not required.

Upgrade matrix:

- 5.0MP3 to 5.1SP1
- 5.1 to 5.1 SP1
- 5.1RP1 to 5.1SP1
- 5.1RP2 to 5.1SP1

For supported upgrade matrix, refer to the *Veritas Cluster Server Installation Guide*.

Upgrades that follow any other upgrade paths require a reboot.

Packaging updates

The following lists package changes in this release.

New VRTSamf package

VRTSamf is a new package introduced in this release. The Asynchronous Monitoring Framework (AMF) module, along with the VCS Agent Framework (AGFW) and resource agents provides a way to avoid polling for resource state changes. The AMF module allows the agent to register which resources to monitor and when to wait. The module provides the agent with immediate notification so that action can be taken at the time of the event. AMF enables the VCS agents to monitor a large number of resources with a minimal effect on performance.

VRTSacclib package is no longer shipped with VCS 5.1SP1

The VRTSacclib package was available with VCS 5.1. The package is not shipped with VCS 5.1SP1. The latest VRTSacclib package can be accessed from the Agent Pack release.

New virtualization features

This release introduces the following virtualization features.

Awareness of the Solaris Resource Monitor

This release introduces a new model which enables VCS to work with Solaris Projects. A service group-level attribute named ContainerInfo and a type-level static attribute named ContainerOpts work together to provide Solaris Resource Monitor (SRM) support.

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

Changes to the VCS engine

The HAD can exchange messages up to 64KB size

The size of the messages that HAD supports is increased from 16KB to 64KB. The messages can be exchanged between different HAD processes (running on different systems) or between CLI and HAD processes.

Refer to the following list for the message, object, attribute, and attribute values:

1. Maximum message size = 64KB
2. Maximum object name size = 1KB
3. Maximum attribute name size = 1KB
4. Maximum scalar attribute value size = 4KB
5. Maximum single key (of key-value pair) size = 4KB
6. Maximum single value (of key-value pair) size = 4KB
7. Maximum size of single element of vector or keylist pair = 4KB
8. Maximum user Name size = 1KB
9. Maximum password size = 255b
10. Maximum password encrypted size = 512b

Note: Points 2 through 10 were already supported in 5.1 release.

Support for intelligent monitoring of VCS resources using IMF

VCS now supports intelligent resource monitoring in addition to poll-based monitoring. Intelligent Monitoring Framework (IMF) is an extension to the VCS agent framework. You can enable or disable the intelligent monitoring functionality of VCS agents as needed.

The benefits of intelligent monitoring over poll-based monitoring are as follows:

- Faster notification of resource state changes.

- Reduction in VCS system utilization which enables VCS to effectively monitor a large number of resources.

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

The following agents are IMF-aware in VCS 5.1 SP1:

- Mount
- Process
- Application
- Oracle
- Netlsnr
- CFSMount
- CVMVxconfigd
- CFSfsckd

New attributes

The following sections describes the attributes introduced in VCS 5.1SP1, VCS 5.1, and VCS 5.0MP3.

Attributes introduced in VCS 5.1SP1

Application Agent attributes

- **EnvFile:** This attribute specifies the environment file that must be sourced before running `StartProgram`, `StopProgram`, `MonitorProgram` or `CleanProgram`.
- **UseSUDash:** This attribute specifies that the agent must run `su - user -c <program>` or `su user -c <program>` while running `StartProgram`, `StopProgram`, `MonitorProgram` or `CleanProgram`.

RemoteGroup agent attribute

- **ReturnIntOffline:** This attribute can take one of the following three values. These values are not mutually exclusive and can be used in combination with one another. You must set `IntentionalOffline` attribute to 1 for the `ReturnIntOffline` attribute to work.
 - **RemotePartial:** Makes `RemoteGroup` resource to return `IntentionalOffline` when the remote service group is in `ONLINE|PARTIAL` state.
 - **RemoteOffline:** Makes `RemoteGroup` resource to return `IntentionalOffline` when the remote service group is in `OFFLINE` state.

- **RemoteFaulted:** Makes RemoteGroup resource to return IntentionalOffline when the remote service group is in OFFLINE|FAULTED state.

DiskGroup agent attribute

- **Reservation:** Determines if you want to enable SCSI-3 reservation. For more information, please refer to *Bundled Agents Reference Guide*.
In order to support SCSI-3 disk reservation, you must be sure that the disks are SCSI-3 compliant. Since all the disks are not SCSI-3 compliant, reservation commands fail on such disk groups. The Reservation attribute helps in resolving this issue. The Reservation attribute can have one of the following three values:
 - **ClusterDefault:** The disk group is imported with or without SCSI-3 reservation, based on the cluster-level UseFence attribute.
 - **SCSI3:** The disk group is imported with SCSI-3 reservation.
 - **NONE:** The disk group is imported without SCSI-3 reservation. The agent does not care about the cluster-level UseFence attribute.

Note: This attribute must be set to NONE for all resources of type DiskGroup in case of non-SCSI-3 fencing.

IP agent attribute

- **ExclusiveIPZone:** When an IP resource has to be configured for exclusive IP zone, set the value of this attribute to 1 (one). It also requires a valid ContainerInfo to be configured in the service group. The IP resource monitors virtual IP address on interface inside the exclusive IP zone.

IPMultiNICB agent attribute

- **Options:** Value of this attribute is used as the option for the `ifconfig` command. For example, if value of this attribute is set to “deprecated” then “deprecated” option is set on the interface while bringing IPMultiNICB resource online.

NFS agent attribute

- **CleanRmtab:** To clear the `/etc/rmtab` file before starting the mount daemon, set the value of CleanRmtab to 1.

NFSRestart agent attribute

- **Lower:** Defines the position of the NFSRestart resource in the service group. The NFSRestart resource below the Share resource needs a value of 1. The NFSRestart resource on the top of the resource dependency tree has a Lower attribute value of 0.

NIC agent attribute

- **ExclusiveIPZone:** When the NIC resource is to be configured for exclusive IP zone, set the value of this attribute to 1 (one). It also requires a valid `ContainerInfo` to be configured in the service group. NIC resource monitors network interface inside the exclusive IP zone.

RVGPrimary agent attribute

- **BunkerSyncTimeOut:** The timeout value in seconds that signifies the amount of time that a Secondary RVG can wait for the synchronization from the bunker host to complete before taking over the Primary role.

NotifierSourceIP agent attribute

- **NotifierSourceIP:** Lets you specify the interface that the notifier must use to send packets. This attribute is string/scalar. You must specify an IP address that is either DNS resolvable or appears in the `/etc/hosts` file.

SambaServer agent attributes

- **PidFile:** The absolute path to the Samba daemon (smbd) Pid file. This attribute is mandatory if you are using Samba configuration file with non-default name or path.
- **SocketAddress:** The IPv4 address where the Samba daemon (smbd) listens for connections. This attribute is mandatory if you are configuring multiple SambaServer resources on a node.

Zone agent attributes

- **RunFsck:** If the value of this attribute is 1, the Zone agent checks the system consistency for vxfs file systems. It uses the `fsck -y` command on all vxfs file systems that are defined in the zones's xml file. This file is located in `/etc/zones`. Adjust the Zone agent default `OnlineTimeout` value so that zone agent has sufficient time to run the `fsck` command before it brings the zone online.
- **DetachZonePath:** If disabled, Zone agent skips detaching the Zone root during zone resource offline and clean. `DetachZonePath` is enabled (1) by default.
- **ForceAttach:** If disabled, the Zone agent attaches the ZonePath without the `-F` option during zone resource online. `ForceAttach` is enabled (1) by default.

Oracle agent attributes

- **DBAUser:** Database/ASM user with `sysdba/sysasm` permissions respectively.
- **DBAPword:** The encrypted value of the password of `DBAUser`.

ASMinst agent attributes

- **MonitorOption:** Enables or disables health check monitoring.

NetBios agent attribute

- **PidFile:** The absolute path to the Samba daemon (nmbd) PidFile. This attribute is mandatory if you are using Samba configuration file with non-default name or path.

Sybase agent attribute

- **Run_ServerFile:** The attribute specifies the location of the RUN_SERVER file for a Sybase instance. If this attribute is not specified, the default location of this file is accessed while starting Sybase server instances.

Cluster-level attributes

- **AutoAddSystemToCSG:** Indicates whether the newly joined or added systems in the cluster become a part of the SystemList of the ClusterService service group if the service group is confirmed. The value 1 (default) indicates that the new systems are added to SystemList of ClusterService. The value 0 indicates that the new systems are not added to SystemList of ClusterService.
- **CounterMissTolerance:** If GlobalCounter does not update in CounterMissTolerance intervals of CounterInterval, then VCS reports about this issue depending on the CounterMissAction (that is, CounterMissTolerance * CounterInterval) time has elapsed since last update of GlobalCounter then CounterMissAction is performed. The default value of CounterMissTolerance is 20.
- **CounterMissAction:** The action mentioned in CounterMissAction is performed whenever the GlobalCounter is not updated for CounterMissTolerance intervals of CounterInterval.
The two possible values of CounterMissAction are LogOnly and Trigger.
LogOnly logs the message in Engine Log and SysLog. Trigger invokes a trigger which has a default action of collecting the comms tar file. The Default value of Trigger is LogOnly.
- **PreferredFencingPolicy:** The I/O fencing race policy to determine the surviving subcluster in the event of a network partition. Valid values are Disabled, System, or Group.
Disabled: Preferred fencing is disabled. The fencing driver favors the subcluster with maximum number of nodes during the race for coordination points.
System: The fencing driver gives preference to the system that is more powerful than others in terms of architecture, number of CPUs, or memory during the race for coordination points. VCS uses the system-level attribute FencingWeight to calculate the node weight.
Group: The fencing driver gives preference to the node with higher priority service groups during the race for coordination points. VCS uses the group-level attribute Priority to determine the node weight.

Resource type attributes

- **IMF:** Determines whether the IMF-aware agent must perform intelligent resource monitoring.
It is an association attribute with three keys Mode, MonitorFreq, and RegisterRetryLimit.
 - **Mode:** Defines whether to perform IMF monitoring based on the state of the resource. Mode can take values 0, 1, 2, or 3. Default is 0.
 - **MonitorFreq:** Specifies the frequency at which the agent invokes the monitor agent function. Default is 1.
 - **RegisterRetryLimit:** Defines the maximum number of times the agent attempts to register a resource. Default is 3.
- **IMFRegList:** Contains a list of attributes. The values of these attributes are registered with the IMF module for notification. If an attribute defined in IMFRegList attribute is changed then the resource, if already registered, is unregistered from IMF. If IMFRegList is not defined and if any attribute defined in ArgList is changed the resource is unregistered from IMF.
- **AlertOnMonitorTimeouts:** Indicates the number of consecutive monitor failures after which VCS sends an SNMP notification to the user.

Attributes introduced in VCS 5.1

VCS 5.1 introduced the following new attributes. See the *Veritas Cluster Server Administrator's Guide* for more information.

Resource type attributes:

- **ContainerOpts:** Specifies the behavior of the agent in a container environment.
- **CleanRetryLimit:** Number of times to retry the clean function before moving a resource to ADMIN_WAIT state.
- **EPClass:** Enables you to control the scheduling class for the agent functions (entry points) except the online entry point.
- **EPPriority:** Enables you to control the scheduling priority for the agent functions (entry points) except the online entry point.
- **FaultPropogation:** Specifies if VCS should propagate the fault up to parent resources and take the entire service group offline when a resource faults.
- **OnlineClass:** Enables you to control the scheduling class for the online agent function (entry point).
- **OnlinePriority:** Enables you to control the scheduling priority for the online agent function (entry point).

Service group level attribute:

- **ContainerInfo:** Specifies information about the container that the service group manages.

Cluster level attributes:

- **CID:** The CID provides universally unique identification for a cluster.
- **DeleteOnlineResource:** Defines whether you can delete online resources.
- **HostMonLogLvl:** Controls the behavior of the HostMonitor feature.

Attributes introduced in VCS 5.0 MP3

VCS 5.0MP3 introduced the following attributes.

Resource type attributes:

- **FaultPropagation:** Specifies if VCS should propagate the fault up to parent resources and take the entire service group offline when a resource faults.
- **AgentFile:** Complete name and path of the binary for an agent. Use when the agent binaries are not installed at their default locations.
- **AgentDirectory:** Complete path of the directory in which the agent binary and scripts are located. Use when the agent binaries are not installed at their default locations.

Cluster level attributes:

- **DeleteOnlineResource:** Defines whether you can delete online resources.
- **HostMonLogLvl:** Controls the behavior of the HostMonitor daemon. Configure this attribute when you start the cluster. You cannot modify this attribute in a running cluster.
- **EngineShutdown:** Provides finer control over the hastop command.
- **BackupInterval:** Time period in minutes after which VCS backs up configuration files.
- **OperatorGroups:** List of operating system user account groups that have Operator privileges on the cluster.
- **AdministratorGroups:** List of operating system user account groups that have administrative privileges on the cluster.
- **Guests:** List of users that have Guest privileges on the cluster.

System level attributes:

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

Service group level attributes:

- **TriggerResFault:** Defines whether VCS invokes the resfault trigger when a resource faults.
- **AdministratorGroups:** List of operating system user account groups that have administrative privileges on the service group.
- **OperatorGroups:** List of operating system user account groups that have Operator privileges on the service group.
- **Guests:** List of users that have Guest privileges on the service group.

Changes to bundled agents

This section describes changes to the bundled agents for VCS.

New bundled agent

- **Project agent:** This agent brings Solaris projects online, takes them offline, and monitors them.
- **Disk agent:** This agent is used to monitor a physical disk or a slice that is exported to LDomS.
- **VolumeSet agent:** The VolumeSet agent brings online, takes offline, and monitors a Veritas Volume Manager (VxVM) volume set. Use this agent to make a volume set highly available.

Support for Solaris projects

The following agents now support Solaris projects:

- Process agent
- Application agent

Support for Veritas dynamic multi-pathing

The following agent supports Veritas Dynamic Multi-Pathing (DMP):

- Zpool agent

About the ReturnIntOffline attribute of RemoteGroup agent

The ReturnIntOffline attribute can take one of three values: RemotePartial, RemoteOffline, and RemoteFaulted.

These values are not mutually exclusive and can be used in combination with one another. You must set the IntentionalOffline attribute of RemoteGroup resource to 1 for the ReturnIntOffline attribute to work.

About the RemotePartial option

Select the RemotePartial value of this attribute when you want the RemoteGroup resource to return an IntentionalOffline when the remote service group is in an ONLINE | PARTIAL state.

About the RemoteOffline option

Select the RemoteOffline value of this attribute when you want the RemoteGroup resource to return an IntentionalOffline when the remote service group is in an OFFLINE state.

About the RemoteFaulted option

Select the RemoteFaulted value of this attribute when you want the RemoteGroup resource to return an IntentionalOffline when the remote service group is in an OFFLINE | FAULTED state.

Configuring RemoteGroup resources in parallel service groups

When a RemoteGroup resource is configured inside parallel service groups, it can come online on all the cluster nodes, including the offline nodes. Multiple instances of the RemoteGroup resource on cluster nodes can probe the state of a remote service group.

Note: The RemoteGroup resource automatically detects whether it is configured for a parallel service group or for a failover service group. No additional configuration is required to enable the RemoteGroup resource for parallel service groups.

A RemoteGroup resource in parallel service groups has the following characteristics:

- The RemoteGroup resource continues to monitor the remote service group even when the resource is offline.
- The RemoteGroup resource does not take the remote service group offline if the resource is online anywhere in the cluster.
- After an agent restarts, the RemoteGroup resource does not return offline if the resource is online on another cluster node.
- The RemoteGroup resource takes the remote service group offline if it is the only instance of RemoteGroup resource online in the cluster.
- An attempt to bring a RemoteGroup resource online has no effect if the same resource instance is online on another node in the cluster.

Support for Exclusive IP zone in networking agents

NIC and IP agents support Exclusive IP zone. This attribute is added to both NIC and IP agents.

For more details, See “[New attributes](#)” on page 15.

Changes to SambaServer and NetBios agents

The SambaServer and NetBios agents contain the following changes:

- VCS SambaServer and NetBios agents now support multiple resource instances on a node.
- These agents now support non default Samba configuration file and pid file names.

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

Changes to database agents

Changes to the Oracle agent

- Oracle agent now supports IMF monitoring.
- The VCS agent for Oracle is Solaris Project (SRM)-aware.
The Oracle resource is an SRM-aware resource which has a predefined, default value for the ContainerOpts attribute. The ContainerOpts attribute determines whether the SRM-aware resource can run under Solaris Project. It also determines whether the container information that is defined in the service group’s ContainerInfo attribute is passed to the resource.
See the *Veritas Storage Foundation and High Availability Solutions Virtualization Guide*.

Changes to the Sybase agent

- The Sybase agent supports a new optional attribute Run_ServerFile. The attribute specifies the location of the RUN_SERVER file for a Sybase instance. If this attribute is not specified, the default location of the RUN_SERVER file is accessed while starting Sybase server instances.
- The VCS agent binaries for Sybase are now a part of VRTSvcssea package. This package also includes the VCS agent binaries for DB2 and Oracle.
- The agent supports a new attribute WaitForRecovery. If this attribute is enabled, during the online function, the agent waits until recovery is completed and all databases that can be made online are brought online.

Changes to LLT

This release includes the following new features and changes to LLT:

- LLT startup time through the LLT init script is now optimized to use a constant time. LLT takes less than 16 seconds to start irrespective of the number of links specified in `/etc/llttab` file.

In the previous releases, LLT took around $(5 * \text{number_of_links_specified_in_the_}/etc/llttab_file)$ seconds to start.

- The `lltstat` command includes the following new options:

- `lltstat -nv active`

This command filters the output of `lltstat -nv` to display the status of only the active nodes in the cluster.

- `lltstat -nv configured`

This command filters the output of `lltstat -nv` to display the status of only the configured nodes in the cluster. Configured nodes include active nodes and any additional nodes which are listed in the `/etc/llthosts` file.

See the `lltstat` manual page for more information.

- Support for different link speeds for LLT links

LLT now removes the restriction to use private NICs with same media speed. You can now use different media speed for the private NICs and configure the NICs with lesser speed as low-priority links to enhance LLT performance.

- Support for destination-based load balancing

LLT now also provides destination-based load balancing where the LLT link is chosen based on the destination node id and the port. With destination-based load balancing, LLT sends all the packets of a particular destination on a link.

See the *Veritas Cluster Server Installation Guide* and the *Veritas Cluster Server Administrator's Guide* for more details.

Changes to GAB

This section lists the new features and changes related to GAB in this release.

- GAB logging daemon

GAB implements a distributed network protocol. For situations when GAB decides to take the drastic action of killing its userland client process or panicking a node to resolve an issue, data from the affected node alone may not suffice for a meaningful support analysis. The new `gablogd` daemon attempts to address this issue. GAB starts this daemon by default at GAB configuration time.

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

Changes to I/O fencing

This section covers the new features and changes related to I/O fencing in this release.

Support for preferred fencing

Traditional fencing prevents a split-brain condition by allowing only one of multiple sub-clusters to continue its operation in case a network partition disrupts regular communication between nodes. The preferred fencing feature gives preference to one sub-cluster over other sub-clusters in determining the surviving sub-cluster. This preference is based on factors such as which of the sub-clusters is running higher priority applications or the total importance of nodes which form that sub-cluster or both.

See the *Veritas Cluster Server Installation Guide* and the *Veritas Cluster Server Administrator's Guide* for more details.

Enhancements to server-based fencing

This release includes the following enhancements and new features related to server-based fencing:

- Single CP-server based fencing
Support to use a single highly available CP server that is configured on an SFHA cluster to provide server-based fencing support for multiple application clusters

Support to migrate between fencing modes when the cluster is running

The `vxfsnwap` utility now supports migrating between disk-based and server-based fencing configurations in a cluster that is running.

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

Changes to global clustering

VCS global clustering monitors and manages the replication jobs and clusters at each site. In the event of a site outage, global clustering controls the shift of replication roles to the Secondary site, bring up the critical applications and redirects client traffic from one cluster to the other.

Before Release 5.1SP1, if there was a disaster at the Primary site or a network disruption, the applications were taken offline on the original Primary and failed

over to the Secondary. When the original Primary returned or the network disruption was corrected, you had the following options:

- Manually resynchronize the original Primary with the data from the new Primary, once the original Primary comes back up. The applications are only active on the new Primary site.
- Automatically resynchronize the original Primary with the data from the new Primary, once the original Primary comes back up. The applications are only active on the new Primary site.

Beginning in Release 5.1SP1, you have a third option. Applications can be active on both the original Primary and Secondary sites. After the original Primary returns or the network disruption is corrected, you have the option of specifying which site is the Primary going forward. This option is called the primary-elect feature, and it is enabled through the VCS global clustering.

The key difference between the primary-elect feature and the other options is that if a network disruption occurs, applications continue to run on the Primary site and they are also failed over to the Secondary. This feature lets you maintain application availability on both sites while the network is down.

VCS system requirements

This section describes system requirements for VCS.

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

VCS requires that all nodes in the cluster use the same processor architecture and run the same operating system.

For example, in a cluster with nodes running Solaris, all nodes must run Solaris SPARC or Solaris x64.

All nodes in the cluster must run the same VCS version. Each node in the cluster may run a different version of the operating system, as long as the operating system is supported by the VCS version in the cluster.

See [“Hardware compatibility list”](#) on page 26.

See [“Supported Solaris operating systems”](#) on page 27.

Hardware compatibility list

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

<http://www.symantec.com/docs/TECH74012>

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

Supported Solaris operating systems

This release of the Veritas products is supported on the following Solaris operating systems:

- Solaris 9 (32-bit and 64-bit, SPARC) with Update 7, 8, and 9
Symantec VirtualStore is only supported on Solaris 9 (SPARC Platform 64-bit).

Note: In the next major release, Veritas products will not support Solaris 9.

- Solaris 10 (64-bit, SPARC or x86_64) with Update 6, 7, 8, and 9
Solaris 10 (SPARC and x86_64) with Update 9 requires VRTSvxvm patch 142629-08 (SPARC) or 142630-08 (x86_64)
Symantec VirtualStore is only supported on Solaris 10 (SPARC or X86 Platform 64-bit).

For the most up-to-date list of operating system patches, refer to the Release Notes for your product.

For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:

<http://entsupport.symantec.com/docs/334829>

Supported software for VCS

VCS supports the following volume managers and file systems:

- Veritas Storage Foundation (SF): Veritas Volume Manager (VxVM) with Veritas File System (VxFS)

VCS 5.1 SP1 supports the following versions of SF:

- SF 5.1 SP1
 - VxVM 5.1 SP1 with VxFS 5.1 SP1
- SF 5.1
 - VxVM 5.1 with VxFS 5.1

Note: VCS supports the previous version of SF and the next version of SF to facilitate product upgrades.

Supported VCS agents

[Table 1-1](#) lists the agents for enterprise applications and the software that the agents support.

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

Agent	Application	Application version	Solaris version
DB2	DB2 Enterprise Server Edition	8.1, 8.2, 9.1, 9.5, 9.7	SPARC: Solaris 9, 10; x64: Solaris 10
Oracle	Oracle	11gR1, 10gR2, 11gR2	SPARC: Solaris 9, 10; x64: Solaris 10
Sybase	Sybase Adaptive Server Enterprise	12.5.x, 15.x	SPARC: Solaris 9, 10; x64: Solaris 10

See the *Veritas Cluster Server Installation Guide* for the agent for more details.

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

Features no longer supported

No longer supported agents and components

VCS no longer supports the following:

- Configuration wizards
- CampusCluster agent
- NFSLock agent.
Use the NFSRestart agent to provide high availability to NFS lock records.
- nfs_restart trigger.
Use the NFSRestart agent to provide high availability to NFS lock records.
- ServiceGroupHB agent.

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

- SANVolume agent
- VRTSWebApp
- Oracle 8.0.x, Oracle 8.1.x, and Oracle 9i - not supported by the updated Oracle agent.
- VCS documentation package (VRTSvcsdc)
The VCS documentation package (VRTSvcsdc) is deprecated. The software disc contains the documentation for VCS in Portable Document Format (PDF) in the *cluster_server/docs* directory.
Symantec recommends copying pertinent documents from the disc to your system directory */opt/VRTS/docs* for reference.
- hahbsetup tool. This tool is removed as no supported feature requires this tool.
- VRTScutil package. This package is no longer supported.

Fixed issues

This section covers the incidents that are fixed in this release.

This release includes fixed issues from the 5.1 Service Pack (SP) 1 Rolling Patch (RP) 2 release. For the list of fixed issues in the 5.1 SP1 RP2 release, see the Veritas Storage Foundation and High Availability Solutions 5.1 SP1 RP2 Release Notes.

See the corresponding Release Notes for a complete list of fixed incidents related to that product.

LLT, GAB, and I/O fencing fixed issues

[Table 1-2](#) lists the fixed issues for LLT, GAB, and I/O fencing.

Table 1-2 LLT, GAB, and I/O fencing fixed issues

Incident	Description
1908938	[GAB] In a large cluster, cascaded lowest node failures result in GAB panic during sequence space recovery.
1840826	[GAB] Prevent 'gabconfig -c' while port 'a' is in the middle of iofence processing.

Table 1-2 LLT, GAB, and I/O fencing fixed issues (*continued*)

Incident	Description
1861439 1849527	[LLT] Removing the LLT links from a single node in a four-node cluster causes other nodes to panic.
2066020	[LLT] The <code>dlpiping</code> utility exits with an error similar to "dlpiping: send ECHO_REQ failed."
2005045	[LLT] The <code>hastart</code> command fails to start HAD on one of the nodes with message "GabHandle::open failed errno = 16" in syslog after HAD is stopped on all the nodes in the cluster simultaneously.
1859023	[LLT] The <code>lltconfig -T query</code> command displays a partially incorrect output
1846387 2084121	[Fencing] The <code>vxfenswap</code> and the <code>vxfentsthdw</code> utilities fail when rsh or ssh communication is not set to the same node.
1922413	[Fencing] The <code>vxfentsthdw</code> utility should detect storage arrays which interpret NULL keys as valid for registrations/reservations.
1847517	[Fencing] The <code>vxfenswap</code> utility has an incorrect usage message for <code>-n</code> option
1992560	[Fencing] The <code>vxfentsthdw</code> utility uses <code>scp</code> to communicate with the local host.
1512956	[Fencing] The <code>vxfenclearpre</code> utility displays error messages
2143933	[VxCPS] For a four-node cluster, the installer fails to configure server-based fencing which uses three CP servers as its coordination points. The process fails while registering the CP clients on the third CP server.
2151166	[VxCPS] Need strict host name matching in coordination point installer.
1886802	[VxCPS] The <code>hamsg</code> command does not load localized messages defined in the <code>VRTSvcCPS.bmc</code> file.

Bundled agents fixed issues

[Table 1-3](#) lists the fixed issues for bundled agents.

Table 1-3 Bundled agents fixed issues

Incident	Description
246635	The IPMultiNICB agent does not support the Outsourcing Source Packet Address (OSPA) functionality. OSPA can be configured by using the <code>ndd ip_enable_group_ifs</code> command.
251704	The index number of the virtual interfaces changes after a failover. As a result applications using the interfaces may face communication failure.
252354	Application agent does not pass the value of CleanReason to the script that the Agent executes as per the value of the CleanProgram attribute.
426856	MultiNICB monitor does not store the PID in a cookie and traverses /proc directory in every monitor cycle. This leads to high CPU load in cases where there are a lot of other processes running on the system.
1967957	MultiNICB agent improperly deprecates the base interface even when the CheckConfig attribute is set to 0.
1969191	If you restart HAD, online Share resources may go offline.
2001039	In a frozen local service group, if a resource goes offline outside VCS control, a RemoteGroup resource also goes offline.
2016492	For a MultiNICB resource, if you change the value of the Device attribute, the resource goes into UNKNOWN state.
2017266	Share Agent reports an ONLINE resource as OFFLINE after hashadow restarts the High Availability Daemon (HAD) module.
2019198	MultiNICB does not check if any interface out of its control is configured in the same subnet.

Table 1-3 Bundled agents fixed issues (*continued*)

Incident	Description
2019904	The OS determines the interface that the notifier uses to send packets. The user must be optionally able to specify the interface. This is an enhancement.
2045972	If you upgrade to VCS 5.1, Application resources may go to the FAULTED state.
2064974	The Application agent tries to delete an uninitialized pointer during a clean entry point, and dumps a core file.
2101510	Mount Agent does not unmount any loopback mounts before taking them offline.
2101530	Local zone VxFS mounts that need FSKC (the file system check command) cause the zone to not come online.
2101559	Zone agent does not verify multi-user milestone.

VCS engine fixed issues

[Table 1-4](#) lists the fixed issues for VCS engine.

Table 1-4 VCS engine fixed issues

Incident	Description
254693	If the OnlineRetryLimit and PreOnline attributes are set for a group, then the group does not fail over in case of a fault.
970971	At unfreeze of a failover group, VCS does not evaluate the group for Concurrency violation.
1074707	A global group goes online on a remote site despite a concurrency violation. This behavior is observed if a related group resource goes intentionally online on the remote site.
1472734	VCS must log an alert message to increase the value of the ShutdownTimeout attribute on a multi-CPU computer.
1634494	If the GlobalCounter attribute does not increase at the configured interval, VCS must report the failure.

Table 1-4 VCS engine fixed issues (*continued*)

Incident	Description
1765594	If you configure the VxAT under Service Management Facility (SMF) as well as under VCS, and run the <code>shutdown -i6 -g0 -y</code> command, then SMF marks VCS to be in MAINTENANCE state.
1829709	In the Japanese locale, some messages do not appropriately appear.
1859387	When a parent group completely faults in a system zone, an online-local-hard (OLH) child group fails over to another system. This behavior is observed only if the child group is marked for manual failover in campus cluster. That is, the value of the AutoFailover attribute for the group is equal to 2.
1861740	The Subject line of the SMTP notification email must contain the Entity name. This is an enhancement.
1866434	When hashadow attempts to restart the High Availability Daemon (HAD) module, if the <code>/var/VRTSvcs/lock/.hadargs</code> file does not exist, hashadow gets the SIGSEGV signal.
1874261	VCS sets the MonitorOnly attribute of the resources in a frozen service group to 0. This behavior occurs even if the ExternalStateChange attribute is not set to OfflineGroup for a resource that goes intentionally offline.
1874533	If a resource, with the ExternalStateChange attribute set to OfflineGroup, goes intentionally offline, VCS sets the MonitorOnly attribute of all resources in a frozen service group to 0. VCS must set the MonitorOnly attribute only when required.
1915908	The <code>hares</code> command lets you have the "." special character in a resource name.
1958245	Notifier Agent is unable to get the local IP address in the linked-based IPMP.
1971256	If a service group faults during failover, then VCS may not honor the Prerequisites/Limits attributes on the target system.

Table 1-4 VCS engine fixed issues (*continued*)

Incident	Description
1979656	A non-root user is unable to see the output of the <code>hastatus -sum</code> command, if you set the default scheduling class to Fair Share Scheduler.
2022123	The <code>notifier</code> command must let you specify the originating source IP address. This is an enhancement.
2061932	If you override a static attribute for a resource with an empty type definition, then VCS dumps duplicate entries for the attribute in the configuration file.
2081676	In a branded zone, the <code>hastatus -sum</code> command does not work.
2081725	After a child group autostarts, VCS does not bring a partially-online parent to ONLINE state.
2083232	If you configure an online-local dependency between two parallel groups, then the parent service group does not AutoStart on all nodes.
2084961	If the VCS configuration includes a file with an absolute pathname, then you cannot load templates from the cluster manager GUI.
2111296	In rare cases, VCS tries to bring online a failover service group that is already online on another node.
2128658	If you add a script-based WAN heartbeat, the heartbeat agent generates a core file and fails to report status.

Enterprise agents fixed issues

[Table 1-5](#) lists the fixed issues for enterprise agents.

Table 1-5 Enterprise agents fixed issues

Incident	Description
776230	The Sybase agent offline script must support the databases that require a longer time to shut down. This is an enhancement.

Table 1-5 Enterprise agents fixed issues (*continued*)

Incident	Description
1916021	When a user other than the user that installed the Oracle database starts the Oracle agent inside a container, the agent does not report the correct state of resources.
1954724	The Oracle agent monitor inside a zone does not work when Oracle directories inside the zone are NFS / NAS mounted .
1972780	When a user other than the user that installed the Oracle database starts the ASMInst agent inside a container, the agent does not report the correct state of resources.
2101542	[Pri:2][Case:320-128-825][Datalink Corp][VCS Oracle agent unable to determine the online state of oracle database in local zone]
2101553	[312-019-554 for X M RADIO]: Netlsnr offline got 'lost'
2101581	[VCS][240-903-088][BT] WebLogic/ WebSphereMQ issuing too many hares commands
2117378	When the monitor entry function encounters an invalid process ID (PID) in a PID file, the function fails to detect the exit status of the process. This behavior occurs if the PID has an empty line below it. The function also accordingly fails to detect the correct state of a failed DB2 Connect instance.

VCS 5.1 RP1 fixed issues

Table 1-6 Veritas Cluster Server 5.1 RP1 fixed issues

Fixed issues	Description
1975424	In a zone, if there are multiple IPMultiNICB resources on the same subnet, issues occur with the source address of IP packets.
1972789	ASMInstAgent Monitor problem inside a zone where the Oracle home directory is NFS / NAS mounted inside the zone.
1972770	ASMInstAgent does not detect the state of the instance correctly inside local zones.
1968572	Postpatch script throws an error while installing in the non-global zone though LLT and GAB are hollow packages.

Table 1-6 Veritas Cluster Server 5.1 RP1 fixed issues (*continued*)

Fixed issues	Description
1962548	ASMinstAgent dumps core.
1954723	Oracle Agent Monitor problem occurs inside a zone where the Oracle home directory is NFS / NAS mounted inside the zone.
1950427	ASMDGAgent should disable and enable diskgroups in offline and online EPs for 11g R2.
1941647	The <code>haalert</code> command hangs if engine is not in running state.
1922411	<code>vxfcntlshdw</code> should detect storage arrays which interpret NULL keys as valid for registrations/reservations.
1916022	Changes made to Oracle agent via incident 1722109 do not honour ContainerName attribute.
1916004	ASMagent connecting as sysdba instead of sysasm for 11gR2
1915909	The <code>hares</code> command lets you create resources which has the "." special character
1911287	Group stuck at OFFLINE STOPPING state when there is no IP address to be cleaned in IPMultiNICB.
1874267	If ExternalStateChange is not set to OfflineGroup, do not set MonitorOnly to 0.
1870424	LLT should give error if an attempt is made to configure more than 8 links (LLT_MAX_LINK) under LLT
1848114	IPMultiNICB:Resource does not come online when failing over from a panicked node.
1504123	GCO failover does not work when a user name includes "!".

VCS 5.1 RP2 fixed issues

Table 1-7 Veritas Cluster Server 5.1 RP2 fixed issues

Fixed issues	Description
1937834	Partial parent group comes online after the child service group autostarts and an issue occurs in a service group failover after a node panics.

Table 1-7 Veritas Cluster Server 5.1 RP2 fixed issues (*continued*)

Fixed issues	Description
1952087	IPMultiNICB resource goes offline after mpathd failback.
1967955	MultiNICB agent sets base interface DEPRECATED and NOFAILOVER flags even if CheckConfig is set to 0.
1969999	SNMP Traps receiver displays trimmed output.
1970639	Issue occurs with Mount Agent handling loopback mounts.
1979662	Issue occurs while executing the <code>hastatus -sum</code> command for a non-root user with FSS.
1980252	Memory leak occurs in LTT during unloading.
1982648	Enhanced NFS agent must clear <code>/etc/rmtab</code> before starting mountd.
1986311	Issue occurs while accessing a freed pointer in <code>vxfsend</code> .
2009127	Message ID errors occur in the Samba family of agents.
2011416	Memory leaks occur in <code>llt_dlp_i_setup</code> and <code>llt_closenode</code> paths.
2016490	MultiNICB agent displays Unknown status after changing existing NIC device.
2017344	MultiNICB agent faces issues when running the <code>haping</code> command for IPv6 addresses.
2019202	MultiNICB agent checks for interface out of its control which is configured in same subnet.
2019899	Notifier faces issues in binding to a specific source IP address.
2021018	New attribute must support <code>fsck</code> during zone boot for <code>vxfs</code> file systems for Zone agent.
2025380	Share agent brings resource offline when HAD is restarted by <code>hashadow</code> .
2031922	Errors occur in <code>dlpiping</code> utility while working in server mode.
2031931	Issue occurs while executing the <code>lltconfig -a set 1 link1 <ip-address></code> command.
2035239	Application agent floods <code>engine</code> log with "Container is not up" messages.
2059631	LLT links go off/on repeatedly after configuring LLT over <code>udp</code> in IPv6.

Table 1-7 Veritas Cluster Server 5.1 RP2 fixed issues (*continued*)

Fixed issues	Description
2064973	Application agent deletes an uninitialized pointer during a clean entry point.
2066986	HAD is killed in a heavily loaded system .
2077022	Unwanted Solaris patch messages are logged into engine log while zone resource goes online.
2077375	Parallel group in PARTIAL state autostarts when engine restarts.
2077396	VCS dumps core under heavy load system which results in node panic.
2078802	The <code>halogin</code> command fails when you bring a zone resource online for branded zones.
2079596	Zone resource takes a long time to go down when the zone root file system is forcefully unmounted .
2079601	Zone agent does not fault when its zone root no longer exists.
2079854	Fencing support required for non SCSI-3 capable environments .
2079868	Mismatching ContainerInfo displayed at group level and resource level.
2079977	Zone agent must remove UserNames added during online to allow successful <code>_had</code> snapshot of remote node(s).
2081674	The <code>hastatus -sum</code> command faces issues in a branded zone .
2081741	The <code>hastart</code> command faces issue which fails with error message <code>GabHandle::open failed errno = 16</code> .
2086251	GAB driver must be enhanced to prevent <code>gabconfig -c</code> while port 'a' is in the middle of iofence processing. Else, system may panic.
2086273	The <code>gabfd</code> static array contains a stale entry if open succeeds and registration fails.
2086280	Node panics after running the GTX tc.
2089193	CP server which gets killed when CP client of higher version attempts to communicate with CPServer running version 5.1.
2092199	Packaging issue occurs in VCS where shutting down a branded zone fails.
2092201	Zone agent must not run the <code>zlogin halogin</code> command if the user is already created or if <code>./vcspwd</code> file is already present.

Table 1-7 Veritas Cluster Server 5.1 RP2 fixed issues (*continued*)

Fixed issues	Description
2096212	The Netlsnr agent issue occurs inside a zone where the agent fails to monitor listener if the Oracle home directory is NFS/NAS mounted inside the zone.
2097029	Zone agent must not detach zone root by adding attribute DetachZonePath which defaults to 1.
2102776	Zone agent must handle Sun bug 6757506 where zoneadm list fails causing Zone resource to fault.
2102777	RemoteGroup resource must support remote groups that are a parallel SG.
2083268	RFC check with DNS agent must be disabled..
2111294	Some VCS nodes in a group are online and some are not.
2116161	LVMVG goes not come online.
2119570	Issue occurs in Oracle detailed monitoring when sending SNMP notification on WARN signal.
2120020	DB2 resource generated excessive logging in engine_A.log.
2125442	HAD must bring online the failover service group only if it is offline on all nodes after the service group is unfrozen.
2126871	Memory leak occurs in MultiNICB agent.
1937834	Partial parent group must auto-start after child comes online, and service group must fail over after node panic.
2066967	Heartbeating logic between engine and agfw must improve during snapshotting and during steady cluster operations.
2071549	Under heavy load, HAD may wait indefinitely in waitpid() when user requests to run some command through "hacli". This may cause GAB to kill HAD.
2077363	Overriding static attribute for any resource with empty type definition creates duplicate entries in main.cf
2077375	Parallel group in PARTIAL state autostarts in case of engine restart.
2079617	NFSRestart agent must remain online if HAD is forcefully stopped and restarted.
2079622	nfs splitbrain test: Delay forced import of disk group agent to avoid errors to client nodes.

Table 1-7 Veritas Cluster Server 5.1 RP2 fixed issues (*continued*)

Fixed issues	Description
2079664	ClusterService Group autopopulates system list
2080703	Memory leak occurs when running the <code>hareg -group</code> command.
2084977	A stack overflow occurs when a file name is very long.
2089182	The <code>vxcpsserv</code> process memory keeps growing when you run <code>cpsadm</code> commands.
2102764	RemoteGroup resource appears OFFLINE even after applying patch for issue 1834858.
2110465	<code>vxfcntlpre</code> cannot clear keys from coordinator disks and data disks when there is a preexisting split brain.

Known issues

This section covers the known issues in this release.

See the corresponding Release Notes for a complete list of known issues related to that product.

See [“Documentation”](#) on page 67.

NFS cluster I/O fails when storage is disabled

The I/O from the NFS clusters are saved on a shared disk or a shared storage. When the shared disks or shared storage connected to the NFS clusters are disabled, the I/O from the NFS Client fails and an I/O error occurs.

Workaround: If the application exits (fails/stops), restart the application.

Issues related to installation

This section describes the known issues during installation and upgrade.

Installation precheck can cause the installer to throw a license package warning (2320279)

If the installation precheck is attempted after another task completes (for example checking the description or requirements) the installer throws the license package warning. The warning reads:

```
VRTSvlic not installed on system_name
```

Workaround:

The warning is due to a software error and can be safely ignored.

Manual installation or uninstall of kernel component packages and patches require boot archive updates

After manually installing and uninstalling the packages or the patches corresponding to kernel components such as LLT, GAB, and VXFEN, make sure to update the boot archive. [2159242]

- In case of primary boot environment, run the following command:

```
# bootadm update-archive
```

- In case of an alternate root environment, run the following command:

```
# bootadm update-archive -R [altrootpath]
```

See the `bootadm` manual page for Solaris.

While configuring authentication passwords through the Veritas product installer, the double quote character is not accepted (1245237)

The Veritas product installer prompts you to configure authentication passwords when you configure Veritas Cluster Server (VCS) as a secure cluster, or when you configure Symantec Product Authentication Service (AT) in authentication broker (AB) mode. If you use the Veritas product installer to configure authentication passwords, the double quote character (") is not accepted. Even though this special character is accepted by authentication, the installer does not correctly pass the characters through to the nodes.

Workaround: There is no workaround for this issue. When entering authentication passwords, do not use the double quote character (").

Errors observed during partial upgrade of SFHA

While upgrading the VCS packages during an SFHA upgrade from 5.0 MP3 RP2 to 5.1SP1, CPI failed to uninstall the I/O fencing packages (VRTSvxfen, VRTSllt, and VRTSgab). [1779129]

Workaround

Before upgrading SFHA from 5.0 MP3 RP2 to 5.1SP1, you must apply the I/O fencing hotfix 5.0MP3RP2HF2.

Manual upgrade of VRTSvlic package loses keyless product levels (2115662)

If you upgrade the `VRTSvlic` package manually, the product levels that were set using `vxkeyless` may be lost. The output of the `vxkeyless display` command will not display correctly.

To prevent this, perform the following steps while manually upgrading the VRTSvlic package.

To manually upgrade the VRTSvlic package

1. Note down the list of products configured on the node for keyless licensing.

```
# vxkeyless display
```

2. Set the product level to NONE.

```
# vxkeyless set NONE
```

3. Upgrade the VRTSvlic package.

```
# pkgrm VRTSvlic
```

This step may report a dependency, which can be safely overridden.

```
# pkgadd -d VRTSvlic.pkg
```

4. Restore the list of products that you noted in step 1.

```
# vxkeyless set product[,product]
```

Issues with keyless licensing reminders after upgrading VRTSvlic (2141446)

After upgrading from 5.1 to 5.1SP1, some keyless licenses may be left in the system. As a result, you may see periodic reminders being logged if the VOM server is not configured.

This happens if you were using keyless keys before upgrading to 5.1SP1. After the upgrade, you install real keys and run `vxkeyless set NONE`. In this case, the keyless licenses may not be completely removed and you see warning messages being logged after two months (if VOM server is not configured). This does not result in any functionality impact.

To resolve this issue, perform the following steps:

1. Note down the list of products configured on the node for keyless licensing. Run `vxkeyless display` to display the list.

2. Set the product level to *NONE* with the command:

```
# vxkeyless set NONE
```

3. Find and delete the keyless licenses left over in the system. To do this, perform the following steps for every key stored in `/etc/vx/licenses/lic:`

- Verify if the key has `VXKEYLESS` feature Enabled using the following command:

```
# vxlicrep -k <license_key> | grep VXKEYLESS
```

- Delete the key if and only if `VXKEYLESS` feature is Enabled.

Note: When performing the search, do not include the `.vxlic` extension as part of the search string.

4. Restore the previous list of products with the command:

```
# vxkeyless set product1[,product]
```

Upgrade or uninstallation of VCS may encounter module unload failures

When you upgrade or uninstall VCS, some modules may fail to unload with error messages similar to the following messages:

```
fdd failed to stop on node_name  
vxfs failed to stop on node_name
```

The issue may be observed on any one or all the nodes in the sub-cluster.

Workaround: After the upgrade or uninstallation completes, follow the instructions provided by the installer to resolve the issue.

Installer is unable to split a cluster that is registered with one or more CP servers

Splitting a cluster that uses server-based fencing is currently not supported. [2110148]

You can split a cluster into two and reconfigure VCS on the two clusters using the installer. For example, you can split a cluster `clus1` into `clus1A` and `clus1B`.

However, if you use the installer to reconfigure the VCS, the installer retains the same cluster UUID of `clus1` in both `clus1A` and `clus1B`. If both `clus1A` and `clus1B`

use the same CP servers for I/O fencing, then the CP server allows registration only from the cluster that attempts to register first. It rejects the registration from the cluster that attempts next. Thus, the installer reports failure during the reconfiguration of the cluster that uses server-based fencing.

Workaround: None.

The installer enters an infinite loop because the cluster is already running in secure mode while configuring server-based fencing (2166599)

During server-based fencing configuration with a secure cluster, if vxfen fails to start and you retry server-based fencing configuration, the installer keeps asking to enter another system to enable security after you manually start VCS.

Workaround:When vxfen fails to start in customized mode for server-based fencing with a secure cluster, do not choose to retry configuring fencing, choose the default option, then vxfen starts in disabled mode. You can also retry fencing configuration using `-fencing` option.

System moves to low system resources while bringing large number process resources online (2061338)

When large number of resource like Process resources (1500 in number) is configured on a Linux system (kernel version 2.6.18-92.el5) than agent gets killed. The reason for is fork failure and fork return with an error number 513. A bug against Red Hat "Issue #822253" exists. Red Hat has confirmed that this is their issue. This issue doesn't appear on kernel version 2.6.18-194.el5 which they claim to have the fix for this issue.

Installed 5.0 MP3 without configuration, then upgrade to 5.1 SP1, installer can not continue (2016346)

If you install 5.0MP3 without configuration, you cannot upgrade to 5.1SP1. This upgrade path is not supported.

Workaround: Uninstall 5.0 MP3, and then install 5.1 SP1.

Operational issues for VCS

Issues with configuration of resource values

If you configure a resource that has more than 425 values in its **ArgListValues**, the agent managing that resource logs a message such as:

```
VCS WARNING V-16-2-13806 Thread(1437547408) ArgListValues overflow;  
Cannot append values more than upper limit of (425).
```

Normally, the number of values in **ArgListValues** for a resource must not exceed 425. However, in case of a keylist, association or vector type of attribute appears in the ArgList for a resource-type. Since these attributes can take multiple values, there is a chance for the resource values in **ArgListValues** to exceed 425.

The CmdServer process may not start in IPv6 environments in secure clusters

In an IPv6 environment on secure clusters, the CmdServer process may not start. In addition, security may not function correctly. If it does not start on a particular node, modify that node's /etc/hosts file so that the localhost resolves to ::1.

Workaround: In the /etc/hosts file, add the following:

```
::1          localhost
```

Issues related to the VCS engine

Missing host names in engine_A.log file

The GUI does not read the engine_A.log file. It reads the engine_A.ldf file, gets the message id from it, and then queries for the message from the bmc file of the appropriate locale (Japanese or English). The bmc file does not have system names present and so they are read as missing. [1736295]

Systems with multiple CPUs and copious memory shut-down time may exceed the ShutdownTimeout attribute

The time taken by the system to go down may exceed the default value of the ShutdownTimeout attribute for systems that have a large numbers of CPUs and memory. [1472734]

Workaround: Increase the value of the ShutdownTimeout attribute based on your configuration.

Parent group faulting in zone 1 results in the child group being automatically failed over to zone 2

Parent group faulting in zone 1 results in the child group being automatically failed over to zone 2. [1859387]

Error messages displayed while uninstalling VCS 5.1SP1 patch (2128536)

Description: The following messages may be displayed while uninstalling the VCS 5.1SP1 patch.

```
Pkgadd failed. See /var/tmp/<*.log> for details  
Patchrm is terminating.  
WARNING: patchrm returned <7> for global zone  
Done!
```

Resolution: This is an ignorable error/warning message and the patch is uninstalled successfully.

VCS Engine logs messages when it eventually connects to a remote cluster

Description: In a global cluster, if a local cluster fails to connect with a remote cluster in the first attempt but succeeds eventually, then you may see the following warning messages in the engine logs. [2110108]

```
VCS WARNING V-16-1-10510 IpmHandle: pen Bind Failed.  
unable to bind to source address 10.209.125.125. errno = 67
```

Workaround: There is currently no workaround for this issue. This issue has no impact on any functionality.

Agent framework can reject `hares -action` command

When a probed resource is disabled and later enabled then, the agent framework can reject `hares -action` command till the agent successfully monitors the resource.

New nodes get added to SystemList and AutoStartList attributes of ClusterService even if AutoAddSystemToCSG is disabled

The AutoAddSystemToCSG attribute determines whether the newly joined or added systems in a cluster become part of the SystemList of the ClusterService service group if the service group is configured. The value 1 (default) indicates that the new systems are added to SystemList of ClusterService.

AutoAddSystemToCSG has an impact only when you execute the `hasys -add` command or when a new node joins the cluster. [2159139]

However, when you use the installer to add a new node to the cluster, the installer modifies the SystemList and AutoStartList attributes irrespective of whether

AutoAddSystemToCSG is enabled or disabled. The installer adds the new system to the SystemList and AutoStartList. To add nodes, the installer uses the following commands that are not affected by the value of AutoAddSystemToCSG:

```
# hagr -modify ClusterService SystemList -add newnode n
# hagr -modify ClusterService AutoStartList -add newnode
```

Workaround

The installer will be modified in future to prevent automatic addition of nodes to SystemList and AutoStartList.

As a workaround, use the following commands to remove the nodes from the SystemList and AutoStartList:

```
# hagr -modify ClusterService SystemList -delete newnode
# hagr -modify ClusterService AutoStartList -delete newnode
```

Issues related to the bundled agents

Entry points that run inside a zone are not cancelled cleanly

Cancelling entry points results in the cancellation of only the `zlogin` process. The script entry points that run inside a zone are forked off using the `zlogin` command. However, the `zlogin` command forks off an `sh` command, which runs in the context of the Solaris zone. This shell process and its family do not inherit the group id of the `zlogin` process, and instead get a new group id. Thus, it is difficult for the agent framework to trace the children or grand-children of the shell process, which translates to the cancellation of only the `zlogin` process. [1179695]

Workaround: Oracle must provide an API or a mechanism to kill all the children of the `zlogin` process that was started to run the entry point script in the local-zone.

Solaris mount agent fails to mount Linux NFS exported directory

The Solaris mount agent mounts the mount directories. At this point, if it tries to mount a Linux NFS exported directory, the mount fails showing the following error:

```
nfs mount: mount: <MountPoint>: Not owner
```

This is due to system NFS default version mismatch between Solaris and Linux.

The workaround for this is to configure `MountOpt` attribute in mount resource and set `vers=3` for it.

Example

```
root@north $ mount -F nfs south:/test /logo/
nfs mount: mount: /logo: Not owner
root@north $
Mount nfsmount (
    MountPoint = "/logo"
    BlockDevice = "south:/test"
    FSType = nfs
    MountOpt = "vers=3"
)
```

The zpool command runs into a loop if all storage paths from a node are disabled

The Solaris Zpool agent runs `zpool` commands to import and export zpools. If all paths to the storage are disabled, the zpool command does not respond. Instead, the zpool export command goes into a loop and attempts to export the zpool. This continues till the storage paths are restored and zpool is cleared. As a result, the offline and clean procedures of Zpool Agent fail and the service group cannot fail over to the other node.

Workaround: You must restore the storage paths and run the zpool clear command for all the pending commands to succeed. This will cause the service group to fail over to another node.

VolumeSet messages do not display in the engine log on Japanese locale

The VolumeSet messages do not get displayed in the engine log on Japanese locale.

Workaround: None.

Issues related to the VCS database agents

VCS agent for Oracle: Health check monitoring is not supported for Oracle database 11g R1 and 11g R2 (1985055)

Health check monitoring is not supported for Oracle database 11g R1 and 11g R2.

Workaround: Set `MonitorOption` attribute for Oracle resource to 0.

VCS agent for Oracle: Health check monitoring does not work with Oracle 10.2.0.4

The health check monitoring in Oracle agent does not work with Oracle 10.2.0.4 due to incompatibility of the health check APIs provided by Oracle. [2101570]

Resolution: Disable health check monitoring by setting the MonitorOption attribute to 0 (zero).

VCS agent for Oracle: Make sure that the ohasd has an entry in the init scripts

Make sure that the ohasd process has an entry in the init scripts so that when the process is killed or the machine is rebooted, this automatically restarts the process.[1985093]

Workaround: Respawn of ohasd process. Add the ohasd process in the `/etc/inittab` file to ensure that this process is automatically restarted when killed or the machine is rebooted.

VCS agent for Oracle: Intentional Offline does not work

Due to issues with health check monitoring, Intentional Offline does not work for VCS agent for Oracle.

The ASMInstAgent does not support having pfile/spfile for the ASM Instance on the ASM diskgroups

The ASMInstAgent does not support having pfile/spfile for the ASM Instance on the ASM diskgroups.

Workaround:

Have a copy of the pfile/spfile in the default `$GRID_HOME/dbs` directory to make sure that this would be picked up during the ASM Instance startup.

VCS agent for ASM: Health check monitoring is not supported for ASMInst agent

The ASMInst agent does not support health check monitoring.

Workaround: Set the MonitorOption attribute to 0.

Concurrency violation due to process startup on failover node is not detected when detail monitoring is set for Oracle resources [2917558]

Inside a failover service group, when the administrator starts an Oracle resource on a node and if the Oracle instance is online on any other node within the cluster, the instance would come up. However, the database does not get mounted. In such circumstances, this startup attempt is detected by basic monitoring. If detail monitoring is enabled, this startup attempt does not get detected.

Workaround: No workaround.

Issues related to the agent framework

English text while using 'hares -action' command (1786742)

Description: The output of hares -action is displayed in English text and not in your configured locale.

Resolution: No resolution.

Agent framework cannot handle leading and trailing spaces for the dependent attribute

Agent framework does not allow spaces in the target resource attribute name of the dependent resource.

Workaround

Do not provide leading and trailing spaces in the target resource attribute name of the dependent resource.

The agent framework does not detect if service threads hang inside an entry point

In rare cases, the agent framework does not detect if all service threads hang inside a C entry point. In this case it may not cancel them successfully. [1511211]

Workaround: If the service threads of the agent are hung, send a kill signal to restart the agent. Use the following command: `kill -9 hung_agent's_pid`. The `haagent -stop` command does not work in this situation.

The ArgListValues attribute values for dependent resources may not populate correctly when a target resource is deleted and re-added

For resource attributes, deleting a resource prevents a dependent attribute's value from refreshing in the dependent resource's value.

For example, you have resource (*rD*), which depends on a resource's attribute value (*rT:Attr_rt*). When you delete the target resource (*rT*), and re-add it (*rT*), the dependent resource (*rD*) does not get the correct value for the attribute (*Attr_rt*). [1539927]

Workaround: Set the value of the reference attribute (*target_res_name*) to an empty string.

```
# hares -modify rD target_res_name ""
```

Where *rD* is the name of the dependent resource, and *target_res_name* is the name of the reference attribute that contains the name of the target resource.

Set the value of the reference attribute (*target_res_name*) to the name of the target resource (*rT*).

```
# hares -modify rD target_res_name rT
```

Agent performance and heartbeat issues

Depending on the system capacity and the number of resources configured under VCS, the agent may not get enough CPU cycles to function properly. This can prevent the agent from producing a heartbeat synchronously with the engine. If you notice poor agent performance and an agent's inability to heartbeat to the engine, check for the following symptoms.

Navigate to `/var/VRTSvcs/diag/agents/` and look for files that resemble:

```
FFDC_AGFWMMain_729_agent_type.log   FFDC_AGFWTimer_729_agent_type.log core
FFDC_AGFWSvc_729_agent_type.log     agent_typeAgent_stack_729.txt
```

Where *agent_type* is the type of agent, for example Application or FileOnOff. If you find these files, perform the next step.

Navigate to `/var/VRTSvcs/log/` and check the `engine_*.log` file for messages that resemble:

```
2009/10/06 15:31:58 VCS WARNING V-16-1-10023 Agent agent_type
not sending alive messages since Tue Oct 06 15:29:27 2009
2009/10/06 15:31:58 VCS NOTICE V-16-1-53026 Agent agent_type
ipm connection still valid
```

```
2009/10/06 15:31:58 VCS NOTICE V-16-1-53030 Termination request sent to
agent_type agent process with pid 729
```

Workaround: If you see that both of the above criteria are true, increase the value of the AgentReplyTimeout attribute value. (Up to 300 seconds or as necessary.) [1853285]

Issues related to Live Upgrade

The VRTSvcsea package removal fails while removing it from the alternate disk during live upgrade (2096925)

Description: This is because the pre-remove script of VRTSvcsea checks if any of the following agent is running:

- ASMDG
- ASMInst
- Db2udb
- Netlsnr
- Oracle
- Sybase
- SybaseBk

Therefore, even if agents are running from the first disk, we cannot remove the package from second disk.

Resolution: Stop any of the running agents before removing the package.

Live Upgrade may fail on Solaris 9 if packages and patches are not current (2052544)

Live Upgrade may fail on a Solaris 9 host if a VxFS file system is in `/etc/vfstab`.

Workaround: On the Solaris 9 host, install the Live Upgrade packages `SUNWlucfg`, `SUNWluu`, and `SUNWlur` from a Solaris 10 image. After you install the packages, install the latest Live Upgrade patch.

For more information on required packages and patches, visit the following site and search on "Live Upgrade requirements."

<http://wikis.sun.com>

Issues related to VCS in Japanese locales

This section covers the issues that apply to VCS 5.1 in a Japanese locale.

The GetSafeMsg() returns error when one of the parameters is already localized

Some log messages that use the date-string parameter may not print correctly in non-English locales. [1715258, 1825966]

The gcoconfig script displays error messages in English

The gcoconfig script incorrectly displays English error messages. [1416136]

The hahbsetup command displays messages and warnings in English

The hahbsetup command incorrectly displays messages and warnings in English. [1652562]

The hares -action command displays output in English

The hares -action command incorrectly displays output in English. [1786747]

Listener startup message on ja_JP.PCK locale may not be displayed correctly in the engine log (2075471)

Description: When you start the listener resource in VCS on ja_JP.PCK locale, the `lsnrctl start` command output is not shown correctly in the engine log. This happens because the converted output from the command generates special characters which are not handled by `halog` command.

Resolution: You can ignore this message as it does not have any functionality impact for the listener resource.

Issues related to global clusters

The engine log file receives too many log messages on the secure site in global cluster environments

When the WAC process runs in secure mode on one site, and the other site does not use secure mode, the engine log file on the secure site gets logs every five seconds. [1539646]

Workaround: The two WAC processes in global clusters must always be started in either secure or non-secure mode. The secure and non-secure WAC connections will flood the engine log file with the above messages.

Application group attempts to come online on primary site before fire drill service group goes offline on the secondary site

The application service group comes online on the primary site while the fire drill service group attempts to go offline at the same time, causing the application group to fault. (2107386)

Workaround: Ensure that the fire drill service group is completely offline on the secondary site before the application service group comes online on the primary site.

Issues related to LLT

This section covers the known issues related to LLT in this release.

LLT port stats sometimes shows recvcnt larger than recvbytes

With each received packet, LLT increments the following variables:

- recvcnt (increment by one for every packet)
- recvbytes (increment by size of packet for every packet)

Both these variables are integers. With constant traffic, recvbytes hits and rolls over `MAX_INT` quickly. This can cause the value of recvbytes to be less than the value of recvcnt. [1788315]

This does not impact the LLT functionality.

LLT may incorrectly declare port-level connection for nodes in large cluster configurations

When ports get registered and unregistered frequently on the nodes of the cluster, LLT may declare that a port-level connection exists with another peer node. This occurs in some corner cases even though a port is not even registered on the peer node. [1809827]

Issues related to I/O fencing

This section covers the known issues related to I/O fencing in this release.

All nodes in a sub-cluster panic if the node that races for I/O fencing panics

At the time of a network partition the lowest node in each sub-cluster races for the coordination points on behalf of that sub-cluster. If the lowest node is unable to contact a majority of the coordination points or the lowest node itself unexpectedly panics during the race, then all the nodes in that sub-cluster will panic. [1965954]

Coordination Point agent does not provide detailed log message for inaccessible CP servers

The Coordination Point agent does not log detailed information of the CP servers that are inaccessible. When CP server is not accessible, the agent does not mention the UUID or the virtual IP of the CP server in the engine log. [1907648]

Preferred fencing does not work as expected for large clusters in certain cases

If you have configured system-based or group-based preferred fencing policy, preferred fencing does not work if all the following cases are true:

- The fencing setup uses customized mode with one or more CP servers.
- The application cluster has more than eight nodes.
- The node weight for a single node (say galaxy with node id 0) is more than the sum total of node weights for the rest of the nodes.
- A network fault occurs and the cluster partitions into two with the single node (galaxy) on one part and the rest of the nodes on the other part.

Under such circumstances, for group-based preferred fencing, the single node panics even though more high priority services are online on that node. For system-based preferred fencing, the single node panics even though more weight is assigned to the node. [2161816]

See the *Veritas Cluster Server Administrator's Guide* for more information on preferred fencing.

Server-based I/O fencing fails to start after configuration on nodes with different locale settings

On each (application cluster) node, the vxfen module retrieves and stores the list of the UUIDs of coordination points. When different nodes have different locale settings, the list of UUIDs on one (application) node does not match with that of

the other (application) nodes. Hence, I/O fencing does not start after configuration. [2112742]

Workaround: Start I/O fencing after fixing the locale settings to use the same values on all the (application) cluster nodes.

Reconfiguring VCS with I/O fencing fails if you use the same CP servers

When you reconfigure an application cluster that uses server-based I/O fencing (customized fencing mode), the installer does not remove the application cluster information from the CP servers before the reconfiguration. As a result, if you reconfigure the application cluster and choose to configure I/O fencing in customized mode using the same CP servers, then reconfiguration of server-based fencing for the application cluster fails. [2076240]

Workaround: Manually remove the application cluster information from the CP servers after you reconfigure VCS but before you reconfigure server-based I/O fencing for the application cluster.

See the *Veritas Cluster Server Administrator's Guide* for instructions to remove the application cluster information from the CP servers.

CP server cannot bind to multiple IPs (2085941)

Coordination point server (CP server) binds only to a single virtual IP and listens on the same. Application clusters cannot access the CP server if it fails to establish connection to this virtual IP. Therefore, if the connection fails because of the subnet in which the virtual IP of the CP server exists, you cannot access the CP server even if there is another subnet through which the client can connect to the CP server over a different IP.

Resolution: No known resolution for this issue.

Delay in rebooting Solaris 10 nodes due to vxfen service timeout issues

When you reboot the nodes using the `shutdown -i6 -g0 -y` command, the following error messages may appear:

```
svc:/system/vxfen:default:Method or service exit
timed out. Killing contract 142
svc:/system/vxfen:default:Method "/lib/svc/method/vxfen stop"
failed due to signal Kill.
```

This error occurs because the vxfen client is still active when VCS attempts to stop I/O fencing. As a result, the vxfen stop service times out and delays the system reboot. [1897449]

Workaround: Perform the following steps to avoid this vxfen stop service timeout error.

To avoid the vxfen stop service timeout error

- 1 Stop VCS. On any node in the cluster, run the following command:

```
# hstop -all
```

- 2 Reboot the systems:

```
# shutdown -i6 -g0 -y
```

VXFEN service goes to maintenance mode when restarted if the VCS engine is running

On Solaris 10, if you restart the vxfen service when the VCS engine is running, then the vxfen service goes into maintenance mode. You must stop the VCS engine before you restart or disable the vxfen service, and then enable the vxfen service. [2116219]

Issues related to Symantec Product Authentication Service with VCS

This section covers the known issues related to Symantec Product Authentication Service (AT) in this release.

The vcsat and cpsat commands may appear to be hung

The following commands may appear to be hung when you invoke them from the command shell:

- /opt/VRTScps/bin/cpsat
- /opt/VRTSvcs/bin/vcsat

This issue occurs when the command requires some user interaction. [1841185]

Workaround:

- To fix the issue for vcsat, run the commands as follows:

```
# export EAT_HOME_DIR=/opt/VRTSvcs
# /opt/VRTSvcs/bin/vssatvcs command_line_argument
# unset EAT_HOME_DIR
```

- To fix the issue for cpsat, run the commands as follows:

```
# export EAT_HOME_DIR=/opt/VRTScps
# /opt/VRTScps/bin/vssatcps command_line_argument
# unset EAT_HOME_DIR
```

VCS may report AT error during system reboot

When you reboot the systems using the `shutdown -i6 -g0 -y` command, VCS reports the following AT error in the `/var/adm/messages` file and the `/var/VRTSvc/log/engine_A.log` file, and VCS faults the VxSS service group.[1765594]

```
VCS ERROR V-16-1-13067 (host_name) Agent is calling clean
for resource (vxatd) because the resource became OFFLINE
unexpectedly, on its own.
VxSS State s245sf2 |OFFLINE|FAULTED|
VxSS State s245sf3 |ONLINE|
```

Workaround: This error occurs due to a timing issue and this message may be safely ignored.

Veritas Cluster Server agents for Veritas Volume Replicator known issues in 5.1 SP1

No known issues exist for Veritas Storage Foundation Cluster File System in the 5.1SP1 release.

Issues with bunker replay

When `ClusterFailoverPolicy` is set to `Auto` and the `AppGroup` is configured only on some nodes of the primary cluster, global cluster immediately detects any system fault at the primary site and quickly fails over the `AppGroup` to the remote site. VVR might take longer to detect the fault at the primary site and to complete its configuration changes to reflect the fault.

This causes the `RVGPrimary` online at the failover site to fail and the following message is displayed:

```
RVGPrimary:RVGPrimary:online:Diskgroup bunkerdname
could not be imported on bunker host hostname. Operation
failed with error 256 and message VxVM
VVR vradmin ERROR V-5-52-901 NETWORK ERROR: Remote server
unreachable...
```

```
Timestamp VCS ERROR V-16-2-13066 (hostname) Agent is calling  
clean for resource (RVGPrimary) because the resource  
is not up even after online completed.
```

Resolution: To ensure that global clustering successfully initiates a bunker replay, Symantec recommends that you set the value of the `OnlineRetryLimit` attribute to a non-zero value for RVGPrimary resource when the primary site has a bunker configured.

Issues related to AMF driver

AMF driver fails to unload with the Mount Agent running

If Mount Agent uses IMF to monitor mounts of type VxFS, then you cannot unload AMF driver as long as Mount Agent is running. [2262747]

Workaround: Stop the mount agent before you unload the AMF driver.

Issues related to IMF

Could not register process and skipping inactive event messages seen in engine log (2700482)

You may see the following error messages in the engine log:

```
2012/02/12 20:08:55 VCS ERROR V-16-10001-20565  
Application:appl:imf_register:Could not register process  
(/ApplicationTest/app_test_start) as part of resource (appl), errno <17>
```

Where `errno <17>` indicates that the event is already registered with AMF.

However, at this stage the `amfstat` output does not show this event as registered. After running the `amfstat` command, the following messages are logged in `amfconfig -p dbglog`.

```
809261 proff_event.c:240 AMF_TR skipping inactive  
event (30017f3c740) 809261 proff_event.c:327 AMF_TR The number  
of proff events changed between ioctl's ask_cnt=1 I=0
```

Once VCS gets into this state, IMF registration for the particular resource does not succeed, unless the AMF driver is unconfigured and reconfigured. However, traditional monitoring continues for that resource and the overall functionality remains unaffected.

Workaround: No workaround.

Software limitations

This section covers the software limitations of this release.

See “[Documentation](#)” on page 67.

Limitations related to the VCS engine

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

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

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

Limitations related to the bundled agents

Programs using networked services may stop responding if the host is disconnected

Programs using networked services (for example, NIS, NFS, RPC, or a TCP socket connection to a remote host) can stop responding 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 stop responding and possibly time out.

For example, if the host is configured to use NIS maps as a client, basic commands such as `ps -ef` can hang if there is network disconnect.

Symantec recommends creating users locally. To reflect local users, configure:

```
/etc/nsswitch.conf
```

Limitations of the DiskGroup agent

Volumes in disk group are started automatically if the Veritas Volume Manager default value of `AutoStartVolumes` at system level will be set to ON irrespective of the value of the `StartVolumes` attribute defined inside the VCS. Set `AutoStartVolumes` to OFF at system level if you do not want to start the volumes as part of import disk group.

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. [1827036]

Volume agent clean may forcibly stop volume resources

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

False concurrency violation when using PidFiles to monitor application resources

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

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

Volumes in a disk group start automatically irrespective of the value of the StartVolumes attribute in VCS

Volumes in a disk group are started automatically if the value of the system level attribute autostartvolumes in Veritas Volume Manager is set to On, irrespective of the value of the StartVolumes attribute in VCS.

Workaround

If you do not want the volumes in a disk group to start automatically after the import of a disk group, set the autostartvolumes attribute to Off at the system level.

Limitations related to IMF

- IMF registration on Linux for “bind” file system type is not supported.
- In case of SLES11 SP1:

- IMF should not be enabled for the resources where the BlockDevice can get mounted on multiple MountPoints.
- If FSType attribute value is nfs, then IMF registration for “nfs” file system type is not supported.

Limitations related to the VCS database agents

DB2 RestartLimit value

When multiple DB2 resources all start at the same time with no dependencies, they tend to interfere or race with each other. This is a known DB2 issue.

The default value for the DB2 agent RestartLimit is 3. This higher value spreads out the re-start of the DB2 resources (after a resource online failure), which lowers the chances of DB2 resources all starting simultaneously. [1231311]

Limitation with intentional offline functionality of VCS agent for Oracle

The Oracle resource never faults after an intentional offline.

Intentional offline functionality of VCS agent for Oracle requires you to enable health check monitoring. The agent uses Oracle's Health Check API to find the state of the database. If the API returns a graceful shutdown for the database, then the agent marks the resource state as INTENTIONAL OFFLINE. Later if the Oracle agent's online function does not succeed, the agent does not mark the resource as FAULTED. The state remains as INTENTIONAL OFFLINE because the agent receives the database state from the API as graceful shutdown during each monitor cycle. [1805719]

Limitations related to global clusters

- 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.
- Total number of clusters in a global cluster configuration can not exceed four.
- Cluster may not be declared as faulted when Symm heartbeat agent is configured even when all hosts are down.
The Symm agent is used to monitor the link between two Symmetrix arrays. When all the hosts are down in a cluster but the Symm agent is able to see the replication link between the local and remote storage, it would report the

heartbeat as ALIVE. Due to this, DR site does not declare the primary site as faulted.

Engine hangs when you perform a global cluster upgrade from 5.0MP3 in mixed-stack environments

If you try to upgrade a mixed stack VCS environment (where IPv4 and IPv6 are in use), from 5.0MP3 to 5.1SP1, HAD may hang.

Workaround: When you perform an upgrade from 5.0MP3, make sure no IPv6 addresses are plumbed on the system.[1820327].

Use VCS installer to install or upgrade VCS when the zone root is on VxFS shared storage

You must use the VCS installer program to install or upgrade VCS when the zone root is on Veritas File System (VxFS). [1215671]

Systems in a cluster must have same system locale setting

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

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

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

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

Workaround:

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

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

If the secondary node has crashed or restarted, you must manually reattach the fire drill site to the target disk group that is imported at the primary site using the following command: `/opt/VRTSvcs/bin/hares -action $targetres joindg -actionargs $fdsitename $is_fenced -sys $targetsys.`

Limitations with DiskGroupSnap agent

The DiskGroupSnap agent has the following limitations:

- If you use the Bronze configuration for the DiskGroupSnap resource, you could end up with inconsistent data at the secondary site in the following cases: [1391445]
 - After the fire drill service group is brought online, a disaster occurs at the primary site during the fire drill.
 - After the fire drill service group is taken offline, a disaster occurs at the primary while the disks at the secondary are resynchronizing.

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

Cluster Manager (Java console) limitations

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

Use the VCS 5.1 Java Console to manage clusters

Cluster Manager (Java Console) from versions lower than VCS 5.1 cannot be used to manage VCS 5.1SP1 clusters. Symantec recommends using the latest version of Cluster Manager.

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

Run Java Console on a non-cluster system

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

Cluster Manager does not work if the hosts file contains IPv6 entries

VCS Cluster Manager fails to connect to the VCS engine if the `/etc/hosts` file contains IPv6 entries.

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

VCS Simulator does not support I/O fencing

When running the Simulator, be sure the `UseFence` attribute is set to the default, “None”.

The operating system does not distinguish between IPv4 and IPv6 packet counts

In a dual-stack configuration, when you use packet counts and the IPv6 network is disabled, the NIC agent might not detect a faulted NIC. It might not detect a fault because while the IPv6 network is down its packet count still increases. The packet count increases because the operating system does not distinguish between the packet counts for IPv4 and IPv6 networks. The agent then concludes that the NIC is up. If you are using the same NIC device for IPv4 as well as IPv6 resources, set `PingOptimize` to 0 and specify a value for the `NetworkHosts` attribute for either the IPv6 or the IPv4 NIC resource. [1061253]

Limitations related to I/O fencing

This section covers I/O fencing-related software limitations.

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 *Veritas Cluster Server Administrator's Guide* for a description of the problems a failed interconnect can create and the protection I/O fencing provides.

I/O fencing uses SCSI-3 PR keys to implement data protection. Keys are placed on I/O fencing coordinator points 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 points 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 points and data disks. Depending

on the order of reboot and subsequent startup events, the cluster may warn of a possible split brain condition and fail to start up.

Workaround: Use the shutdown -r command on one node at a time and wait for each node to complete shutdown.

Documentation errata

The following sections, if present, cover additions or corrections for Document version: 5.1SP1.1 of the product documentation. These additions or corrections may be included in later versions of the product documentation that can be downloaded from the Symantec Support website and the Symantec Operations Readiness Tools (SORT).

See the corresponding Release Notes for documentation errata related to that component or product.

See [“Documentation”](#) on page 67.

See [“About Symantec Operations Readiness Tools”](#) on page 9.

Veritas Cluster Server Installation Guide

In the *Upgrading using Live Upgrade* chapter, use the `vxlustart` command instead of the `vcslustart` command in all instances.

Veritas Cluster Server Administrator's Guide

This section covers the documentation errata in the *Veritas Cluster Server Administrator's Guide*.

Correction for setting up a disaster recovery fire drill

Topic: Setting up a disaster recovery fire drill

Issue: The content below is incorrect:

After the fire drill service group is taken offline, reset the value of the ReuseMntPt attribute to 1 for all Mount resources.

Use the following corrected information:

After the fire drill service group is taken offline, reset the value of the ReuseMntPt attribute to 0 for all Mount resources.

Documentation

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

Documentation set

[Table 1-8](#) lists the documents for Veritas Cluster Server.

Table 1-8 Veritas Cluster Server documentation

Title	File name
<i>Veritas Cluster Server Installation Guide</i>	vcs_install_51SP1_sol.pdf
<i>Veritas Cluster Server Release Notes</i>	vcs_notes_51SP1_sol.pdf
<i>Veritas Cluster Server Administrator's Guide</i>	vcs_admin_51SP1_sol.pdf
<i>Veritas Cluster Server Bundled Agents Reference Guide</i>	vcs_bundled_agents_51SP1_sol.pdf
<i>Veritas Cluster Server Agent Developer's Guide</i>	vcs_agent_dev_51sp1pr4.pdf
<i>Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide</i>	vcs_vvr_agent_51SP1_sol.pdf
<i>Veritas Cluster Server Application Note: Dynamic Reconfiguration for Oracle Servers</i>	vcs_dynamic_reconfig_51SP1_sol.pdf
<i>Veritas Storage Foundation and High Availability Solutions Virtualization Guide</i>	sfha_virtualization_51SP1_sol.pdf
<i>Veritas Cluster Server Agent for DB2 Installation and Configuration Guide</i>	vcs_db2_agent_51SP1_sol.pdf
<i>Veritas Cluster Server Agent for Oracle Installation and Configuration Guide</i>	vcs_oracle_agent_51SP1_sol.pdf
<i>Veritas Cluster Server Agent for Sybase Installation and Configuration Guide</i>	vcs_sybase_agent_51SP1_sol.pdf

[Table 1-9](#) lists the documentation for Veritas Volume Replicator.

Table 1-9 Veritas Volume Replicator documentation

Document title	File name
<i>Veritas Volume Replicator Administrator's Guide</i>	vvr_admin_51SP1_sol.pdf
<i>Veritas Volume Replicator Planning and Tuning Guide</i>	vvr_planning_51SP1_sol.pdf
<i>Veritas Volume Replicator Advisor User's Guide</i>	vvr_advisor_users_51SP1_sol.pdf

Table 1-10 lists the documentation for Symantec Product Authentication Service (AT).

Table 1-10 Symantec Product Authentication Service documentation

Title	File name
<i>Symantec Product Authentication Service Release Notes</i>	vxat_notes.pdf
<i>Symantec Product Authentication Service Administrator's Guide</i>	vxat_admin.pdf

Manual pages

The manual pages for Veritas Storage Foundation and High Availability Solutions products are installed in the `/opt/VRTS/man` directory.

Set the `MANPATH` environment variable so the `man(1)` command can point to the Veritas Storage Foundation manual pages:

- For the Bourne or Korn shell (`sh` or `ksh`), enter the following commands:

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

- For C shell (`csh` or `tcsh`), enter the following command:

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

See the `man(1)` manual page.