

Veritas™ Cluster Server Release Notes

Linux

5.1 Service Pack 1 Platform Release 4



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 PR4

Document version: 5.1SP1PR4.0

Legal Notice

Copyright © 2011 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	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

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](#)
- [Configuration changes specific to RHEL6](#)
- [Changes introduced in Veritas Cluster Server 5.1SP1PR4](#)
- [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 PR4 for Linux. 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: 5.1SP1PR4.0 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 Cluster Server Release Notes* (5.1 SP1 PR4)

About Veritas Cluster Server

Veritas™ Cluster Server (VCS) by Symantec 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 "[About Symantec Operations Readiness Tools](#)" on page 9.. For information about agents under development and agents that are available through Symantec consulting services, contact your Symantec sales representative.

Intelligent Monitoring Framework (IMF) is an extension to the VCS Agent Framework, that allows the VCS agents to register the resources to be monitored so as to receive immediate notification of resource state changes without having to periodically poll the resources.

The following VCS agents are IMF-aware:

- Mount
- Process
- Application
- DB2

Note: Intelligent Monitoring Framework (IMF) is supported for VxFS and CFS mounts only.

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 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://www.symantec.com/docs/TECH75506>
- For the latest patches available for this release, go to: <http://sort.symantec.com/>

Configuration changes specific to RHEL6

This section describes configuration changes specific to Red hat Enterprise Linux (RHEL) 6.

Changes related to NFSv4 exports

Prior to RHEL6 for NFSv4 exports, the OS did not assign the root of the pseudo file system exported to NFS clients. Hence, it was required to put `fsid=0` option in one of the Share resources to make the Share path as a root. For RHEL6, this is not mandatory. By default, `/` is the root of the pseudo file system exported to NFS clients.

Changes introduced in Veritas Cluster Server 5.1SP1PR4

This section lists the changes in Veritas Cluster Server 5.1SP1PR4.

Changes related to the installation

The product installer includes the following changes.

Using the installer for Veritas Dynamic Multi-pathing (DMP)

You can use the script- or Web-based installer to install, configure, and uninstall Veritas Dynamic Multi-pathing. You can enable DMP using the DMP license or using any Storage Foundation license key.

Using the installer for Symantec Virtual Store (SVS)

You can use the script- or Web-based installer to install, configure, and uninstall Symantec VirtualStore. You can enable SVS using an SVS license.

The new VRTSamf is now included in all high availability products

The new VRTSamf is now included in all high availability products. The asynchronous monitoring framework (AMF) allows the more intelligent monitoring of resources, lower resource consumption, and increased availability across clusters.

See the *Veritas Cluster Server Installation Guide*.

The VRTScutil and VRTSacclib are no longer in use

For all high availability products, the VRTScutil and VRTSacclib are no longer required.

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 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 installer can automatically detect and configure LLT links

The installer detects link connection status among all cluster nodes and chooses the most suitable links for LLT communication. It then can set the priority of the LLT private heartbeat links based on their media speed. Aggregated and bonded NICs are supported.

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.

The `installsfha` and `uninstallsfha` scripts are now available

The `installsfha` and `uninstallsfha` scripts are now available in the `storage_foundation_high_availability` directory to directly install, uninstall, or configure the Storage Foundation and High Availability product.

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.

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.

New attributes

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

Attributes introduced in VCS 5.0 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.

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:

- **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).

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 5.1SP1

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.

LVMVolumeGroup agent attribute

- EnableLVMTagging: This attribute enables the LVM Tagging if the value of this attribute is set to 1. By default, the value of this attribute is "0", hence LVMTagging is disabled.

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.

MultiNICA agent attribute

- Mii: if this attribute is set to 1, the agent uses ethtool and Mii hardware registers to determine the health of the network card.

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.
- **SambaTopDir:** Parent path of Samba daemon and binaries.

ASMIInst 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.

Changes to bundled agents

This section describes changes to the bundled agents for VCS.

New bundled agents

VCS has the following new agents:

- **CoordPoint**—Monitors coordination points in I/O fencing configurations.

The following Veritas Volume Replicator agents are now bundled as well:

- **RVG**—Brings the RVG online, monitors read and write access to the RVG, and takes the RVG offline.
- **RVGPrimary**—Attempts to migrate or takeover a Secondary to a Primary upon an application failover.
- **RVGSnapshot**—Creates and destroys a transactionally consistent space-optimized snapshot of all volumes in a VVR secondary replicated data set.
- **RVGShared**—Monitors the RVG in a shared environment.
- **RVGLogowner**—Assigns and unassigns a node as the logowner in the CVMcluster.
- **RVGSharedPri**—Attempts to migrate or takeover a Secondary to a Primary when a parallel service group fails over.

See the *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide*.

New bundled agent

- **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 Veritas dynamic multi-pathing

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

- **LVMVolumeGroup 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.

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.

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 VRTSvcs 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.

Support for Non-SCSI3 fencing

In environments that do not support SCSI-3, non-SCSI-3 fencing provides reasonable data protection by causing the winning side to delay by a configurable amount (`loser_exit_delay`, default 55). Additionally, Symantec has enhanced the fencing component to help panic the losing side quickly. Together, these enhancements help narrow down the window of potential data corruption drastically.

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 version. However, the nodes can have different update levels for a specific RHEL version, or different service pack levels for a specific SLES version.

Note: The system from where you install VCS must run the same Linux distribution as the target systems.

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

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 Linux operating systems

This section lists the supported operating systems for this release of Veritas products.

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

<http://www.symantec.com/docs/TECH75506>

The Veritas Cluster Server 5.1 SP1 PR4 release supports only following operating systems and hardware:

- Red Hat Enterprise Linux 6 (RHEL 6) (2.6.32-71.el6.ppc64 kernel) on PPC64
- SUSE Linux Enterprise Server 11 (SLES 11) with SP1 (2.6.32.12-0.7-ppc64 kernel) on PPC64

If your system is running an older version of either Red Hat Enterprise Linux or SUSE Linux Enterprise Server, you must upgrade it before attempting to install the Symantec software. Consult the Red Hat or SUSE documentation for more information on upgrading or reinstalling your system.

Symantec supports only Red Hat and SUSE distributed kernel binaries.

Symantec products operate on subsequent kernel and patch releases provided the operating systems maintain kernel ABI (application binary interface) compatibility.

Information about the latest supported Red Hat errata and updates are available in the following TechNote:

<http://www.symantec.com/docs/TECH75506>

Read this TechNote before you install Symantec products.

Required Linux RPMs for VCS

Make sure you installed the following operating system-specific RPMs on the systems where you want to install or upgrade VCS. VCS will support any updates made to the following RPMs, provided the RPMs maintain the ABI compatibility.

[Required Linux RPMs for VCS](#) lists the RPMs that VCS requires for a given Linux operating system.

Table 1-1 Required RPMs

Operating system	Operating system
RHEL 6	glibc-2.12-1.7.el6.ppc glibc-2.12-1.7.el6.ppc64 ksh-20100621-2.el6.ppc64 libgcc-4.4.4-13.el6.ppc libstdc++-4.4.4-13.el6.ppc pam-1.1.1-4.el6.ppc
SLES11	glibc-2.11.1-0.17.4 glibc-32bit-2.11.1-0.17.4 ksh-93t-9.4 libgcc43-32bit-4.3.3_20081022-11.18 libstdc++43-32bit-4.3.3_20081022-11.18 pam-32bit-1.0.2-20.1

Supported software for VCS

VCS supports the following volume managers and file systems:

- ext2, ext3, ext4, NFS, and bind on LVM2, raw disks, and VxVM.
- VxVM 5.1 SP1 PR4 with VxFS 5.1 SP1 PR4
- ext4 and xfs on LVM2 and raw disks

Supported VCS agents

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
- Disk agent
- CampusCluster agent
- SANVolume agent
- VRTSWebApp
- Apache agent configuration wizard
- 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.

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.

Known issues in VCS 5.1SP1PR4

This section covers the known issues in 5.1SP1PR4 release.

Upgrades from previous versions of VCS not supported

This release does not support upgrades of previous versions of VCS running on RHEL 5, SLES 10, and SLES 11. You must uninstall VCS, upgrade the operating system, then reinstall VCS.

SELinux error during installation of VRTSvcsag package

Description: During the installation of VRTSvcsag package on RHEL 6 SELinux enabled machine, you may observe following SELinux error:

```
/usr/sbin/semodule: Failed on /opt/VRTSvcs/bin/selinux/vcsag.pp!
```

This error occurs due to improper installation of the SELinux package. As a result, SELinux commands may not function properly.

Workaround: Reinstall the SELinux package, if you observe this issue.

Trace messages from the gablogd daemon on the console for RHEL6 or later

On RHEL6 or later, the `gablogd` daemon prints informational and trace messages similar to the following [2139883]:

```
INFO: task gablogd:22812 blocked for more than 120 seconds.
"echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this
message.
gablogd D ffff81004100daa0 0 22812 1 23106 22809 (NOTLB)
ffff810faf539e38 0000000000000082 0000000000000084c 0000000000000001
ffff810faf539de8 0000000000000007 ffff810fc2a130c0 ffff810138ee8100
000019f130082599 0000000000018572 ffff810fc2a132a8 00000001f76c3d63
Call Trace:
[<ffffffffff88ee3690>] :gab:gab_linux_sv_wait+0x53/0x68
[<ffffffffff8008e68d>] default_wake_function+0x0/0xe
[<ffffffffff88ecd4c8>] :gab:gab_daemonlog+0xae1/0xc52
[<ffffffffff88ee326c>] :gab:gab_linux_ioctl1+0x10e/0x1a3
[<ffffffffff88ee331d>] :gab:gab_linux_compat_ioctl1+0x1c/0x20
```

```
[<ffffffff800f800f800f80>] compat_sys_ioctl+0xc5/0x2b2  
[<ffffffff8006249d>] sysenter_do_call+0x1e/0x76
```

Workaround: As the operating system message indicates, set the following:

```
echo 0 > /proc/sys/kernel/hung_task_timeout_secs
```

Error messages in syslog (2213651)

If you install or uninstall a product on a node, you may see the following warnings in syslog: /var/log/messages. These warnings are harmless and can be ignored.

When installing, the log may display:

```
Dec  3 17:21:26 cdc-d2950130 kernel: type=1400 audit(1291368086.666:20): avc:  
denied { write } for pid=16553 comm="semanage"  
path="/var/tmp/installer-201012031718JNC/install.VRTSvxvm.cdc-d2950130"  
dev=sdok1  
ino=1443459 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

```
Dec  3 17:21:32 cdc-d2950130 kernel: type=1400 audit(1291368092.123:22): avc:  
denied { write } for pid=16556 comm="semanage"  
path="/var/tmp/installer-201012031718JNC/install.VRTSvxvm.cdc-d2950130"  
dev=sdok1  
ino=1443459 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

```
Dec  3 17:21:55 cdc-d2950130 kernel: type=1400 audit(1291368115.245:24): avc:  
denied { write } for pid=16950 comm="semodule"  
path="/var/tmp/installer-201012031718JNC/install.VRTSvxfs.cdc-d2950130"  
dev=sdok1  
ino=1443463 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

```
Dec  3 17:21:55 cdc-d2950130 kernel: type=1400 audit(1291368115.312:25): avc:  
denied { write } for pid=16950 comm="semodule"  
path="/var/tmp/installer-201012031718JNC/install.VRTSvxfs.cdc-d2950130"  
dev=sdok1  
ino=1443463 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

When uninstalling, the log may display:

```
Dec  3 17:29:00 cdc-d2950130 kernel: type=1400 audit(1291368540.794:27): avc:  
denied { write } for pid=19151 comm="semodule"
```

```
path="/var/tmp/uninstallsfcfsrac-201012031725oCf/uninstall.VRTSvxfs.cdc-  
d2950130"  
dev=sdok1 ino=1186738 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

```
Dec 3 17:29:00 cdc-d2950130 kernel: type=1400 audit(1291368540.866:28): avc:  
denied { write } for pid=19151 comm="semodule"  
path="/var/tmp/uninstallsfcfsrac-201012031725oCf/uninstall.VRTSvxfs.cdc-  
d2950130"  
dev=sdok1 ino=1186738 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

```
Dec 3 17:29:45 cdc-d2950130 kernel: type=1400 audit(1291368585.473:30): avc:  
denied { write } for pid=19683 comm="semanage"  
path="/var/tmp/uninstallsfcfsrac-201012031725oCf/uninstall.VRTSvxvm.cdc-  
d2950130"  
dev=sdok1 ino=1186621 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

```
Dec 3 17:29:50 cdc-d2950130 kernel: type=1400 audit(1291368589.975:32): avc:  
denied { write } for pid=19687 comm="semanage"  
path="/var/tmp/uninstallsfcfsrac-201012031725oCf/uninstall.VRTSvxvm.cdc-  
d2950130"  
dev=sdok1 ino=1186621 scontext=unconfined_u:system_r:semanage_t:s0-s0:c0.c1023  
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file
```

The syslog gets flooded with SELinux messages

The SELinux audit feature logs lot of SELinux messages in the syslog. [2220265]

The following is an example of the SELinux messages:

```
Dec 13 22:29:12 cdc-d2950133 setroubleshoot: SELinux is preventing  
/sbin/rpc.statd access to a leaked /var/VRTSvcs/log/NFSRestart_A.log file  
descriptor. For complete SELinux messages, run  
sealert -l 8cdfb88d-7ab2-4815-b5e5-ea6696bfa89e
```

This does not affect the VCS functionality. This is a SELinux behavior. Such messages occur when SELinux dontaudit rules are enabled for policies, as dontaudit feature of SELinux does an access check of the applications.

Workaround: Run the following command to disable the SELinux messages.

```
semodule -D -B
```

Veritas Cluster Server agents for Veritas Volume Replicator known issues in 5.1 SP1 PR4

The following are new additional Veritas Cluster Server agents for Veritas Volume Replicator known issues in 5.1 SP1 PR4 release.

RVGPrimary online script does not function correctly (1949293)

The RVGPrimary online script does not function correctly.

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.

Stale NFS file handle on the client across failover of a VCS service group containing LVMLogicalVolume resource

A VCS service group for a LVM volume group will be online automatically after a failover. However, the client applications may fail or be interrupted by stale NFS file handle error.

Workaround: To avoid the stale NFS file handle on the client across service group failover, specify "fsid=" in the Options attribute for Share resources.

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.

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 (").

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.

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.

LVM SG transition fails in all paths disabled status

If you have disabled all the paths to the disks, the `LVM2 vg` commands stop responding and wait until at least one path to the disks is restored. As `LVMVolumeGroup` agent uses `LVM2` commands, this behavior causes online and offline entry points of `LVMVolumeGroup` agent to time out and `clean EP` stops responding for an indefinite time. Because of this, the service group cannot fail over to another node.

Workaround: You need to restore at least one path.

SG goes into Partial state if Native LVM VG is imported and activated outside VCS control

If you import and activate LVM volume group before starting VCS, the `LVMVolumeGroup` remains offline though the `LVMLogicalVolume` resource comes online. This causes the service group to be in a partial state.

Workaround: You must bring the VCS `LVMVolumeGroup` resource online manually, or deactivate it and export the volume group before starting VCS.

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

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`:

```
# hagrps -modify ClusterService SystemList -add newnode n
# hagrps -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`:

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

Issues related to the bundled agents

LVM Logical Volume will be auto activated during I/O path failure

LVM Logical Volume gets auto activated during the I/O path failure. This causes the VCS agent to report "Concurrency Violation" errors, and make the resource groups offline/online temporarily. This is due to the behavior of Native LVM. [2140342]

Workaround: Enable the LVM Tagging option to avoid this issue.

Issues related to the agent framework

Agent may fail to heartbeat under heavy load (2073018)

Description: An agent may fail to heartbeat with the VCS engine under heavy load.

This may happen when agent does not get enough CPU to perform its tasks and when the agent heartbeat exceeds the time set in the AgentReplyTimeout attribute. The VCS engine therefore stops the agent and restarts it. The VCS engine generates the following log when it stops and restarts the agent:

Resolution: If you are aware that the system load is likely to be high, then:

- The value of AgentReplyTimeout attribute can be set to a high value
- The scheduling class and scheduling priority of agent can be increased to avoid CPU starvation for the agent, using the AgentClass and AgentPriority attributes.

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.

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 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.

Issues related to GAB

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

Trace messages from the `gablogd` daemon on the console for RHEL5 Update 5 or later

On RHEL5 Update 5 or later, the `gablogd` daemon prints informational and trace messages similar to the following [2139883]:

```
INFO: task gablogd:22812 blocked for more than 120 seconds.
"echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
gablogd      D ffff81004100daa0      0 22812      1      23106 22809 (NOTLB)
 ffff810faf539e38 0000000000000082 000000000000084c 0000000000000001
 ffff810faf539de8 0000000000000007 ffff810fc2a130c0 ffff810138ee8100
 000019f130082599 00000000000018572 ffff810fc2a132a8 00000001f76c3d63
Call Trace:
 [<ffffffff88ee3690>] :gab:gab_linux_sv_wait+0x53/0x68
 [<ffffffff8008e68d>] default_wake_function+0x0/0xe
 [<ffffffff88ecd4c8>] :gab:gab_daemonlog+0xae1/0xc52
 [<ffffffff88ee326c>] :gab:gab_linux_ioctl1+0x10e/0x1a3
 [<ffffffff88ee331d>] :gab:gab_linux_compat_ioctl1+0x1c/0x20
 [<ffffffff800fbe53>] compat_sys_ioctl1+0xc5/0x2b2
 [<ffffffff8006249d>] sysenter_do_call+0x1e/0x76
```

Workaround: As the operating system message indicates, set the following:

```
echo 0 > /proc/sys/kernel/hung_task_timeout_secs
```

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]

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.

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
```

HAD dumps core when hagr -clear is executed on a group in OFFLINE|FAULTED state and a resource in the fault path is waiting to go online (2536404)

This issue occurs if you have a resource dependency, such as r1 -> r2 -> r3. While resources r2 and r3 are online and you initiate bringing resource r1 online, before

the OnlineTimeout occurs, resources r2 and r3 suffer a fault. Resource r2 faults first, and then r3 faults. After the fault of both resources is detected, the group is becomes in an OFFLINE|FAULTED state and resource r1 is stuck waiting to become online. If you execute the `hagrps -clear` command to clear the fault, then HAD dumps core on all nodes due to assertion failure.

Workaround: Flush the pending online operation using the `hagrps -clear` command before clearing the fault.

Software limitations

Software limitation of 5.1 SP1 PR4 release

This section covers the software limitations of the 5.1 SP1 PR4 release.

Limitations related to IMF

- IMF registration on Linux for “bind” file system type is not supported.
- 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.

Limitation related to LLT

LLT may not start on the node which does not have 'BOOTPROTO=none' in the interface configuration file `ifcfg-ethX`. [2191023]

Software limitations of VCS 5.1SP1 release

This section covers the software limitations of VCS 5.1SP1 release.

Limitations related to installing and upgrading VCS

Limitation when you use the installer from a remote system

If you use the installer from a remote system, then the remote system must have the same operating system and architecture as that of the target systems where you want to install VCS. [589334]

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 VCSmg 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.

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.

Mount agent

The Mount agent mounts a block device at only one mount point on a system. After a block device is mounted, the agent cannot mount another device at the same mount point.

Share agent

To ensure proper monitoring by the Share agent, verify that the `/var/lib/nfs/etab` file is clear upon system reboot. Clients in the Share agent must be specified as fully qualified host names to ensure seamless failover.

Driver requirements for DiskReservation agent

The DiskReservation agent has a reserver module in the kernel mode that reserves disks persistently. Any driver that works correctly with the `scsiutil` utility shipped with the `VRTSvcsdr` package is supported. Refer to the manual page for `scsiutil` functionality.

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 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.

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 `hagrps -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.

Using the KDE desktop

Some menus and dialog boxes on Cluster Manager (Java Console) may appear misaligned or incorrectly sized on a KDE desktop. To ensure the proper appearance and functionality of the console on a KDE desktop, use the Sawfish window manager. You must explicitly select the Sawfish window manager even if it is supposed to appear as the default window manager on a KDE desktop.

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”.

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: 5.1SP1PR4.0 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 48.

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

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 1-2](#) lists the documents for Veritas Cluster Server.

Table 1-2 Veritas Cluster Server documentation

Title	File name
<i>Veritas Cluster Server Installation Guide</i>	vcs_install_51sp1pr4_lin.pdf
<i>Veritas Cluster Server Release Notes</i>	vcs_notes_51sp1pr4_lin.pdf
<i>Veritas Cluster Server Administrator's Guide</i>	vcs_admin_51sp1pr4_lin.pdf
<i>Veritas Cluster Server Bundled Agents Reference Guide</i>	vcs_bundled_agents_51sp1pr4_lin.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_51sp1pr4_lin.pdf
<i>Veritas Cluster Server Agent for DB2 Installation and Configuration Guide</i>	vcs_db2_agent_51sp1pr4_lin.pdf
<i>Veritas Cluster Server Agent for Oracle Installation and Configuration Guide</i>	vcs_oracle_agent_51sp1pr4_lin.pdf
<i>Veritas Cluster Server Agent for Sybase Installation and Configuration Guide</i>	vcs_sybase_agent_51sp1pr4_lin.pdf

[Table 1-3](#) lists the documentation for Veritas Volume Replicator.

Table 1-3 Veritas Volume Replicator documentation

Document title	File name
<i>Veritas Volume Replicator Administrator's Guide</i>	vvr_admin_51sp1pr4_lin.pdf

Table 1-3 Veritas Volume Replicator documentation (*continued*)

Document title	File name
<i>Veritas Volume Replicator Planning and Tuning Guide</i>	vvr_planning_51sp1pr4_lin.pdf
<i>Veritas Volume Replicator Advisor User's Guide</i>	vvr_advisor_users_51sp1pr4_lin.pdf

[Table 1-4](#) lists the documentation for Symantec Product Authentication Service (AT).

Table 1-4 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.

Manual pages are divided into sections 1, 1M, 3N, 4, and 4M. Edit the `man(1)` configuration file `/etc/man.config` to view these pages.

To edit the man(1) configuration file

- 1 If you use the man command to access manual pages, set `LC_ALL` to “C” in your shell to ensure that the pages are displayed correctly.

```
export LC_ALL=C
```

See incident 82099 on the Red Hat Linux support website for more information.

- 2 Add the following line to `/etc/man.config`:

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

where other man paths are specified in the configuration file.

- 3 Add new section numbers. Change the line:

```
MANSECT          1:8:2:3:4:5:6:7:9:tcl:n:l:p:o
```

to

```
MANSECT          1:8:2:3:4:5:6:7:9:tcl:n:l:p:o:3n:1m
```