Veritas™ Cluster Server Release Notes

AIX

6.0

November 2011

Symantec™

Veritas™ Cluster Server Release Notes

Product version: 6.0

Document version: 6.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's 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:

doc_feedback@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

Veritas Cluster Server Release Notes

This document includes the following topics:

About this document

This document provides important information about Veritas Cluster Server (VCS) version 6.0 for AIX. Review this entire document before you install or upgrade VCS.

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

This is Document version: 6.0.0 of the *Veritas Cluster Server Release Notes*. Before you start, make sure that you are using the latest version of this guide. The latest product documentation is available on the Symantec Web site at:

https://sort.symantec.com/documents

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 on the software media 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* (6.0)

About Veritas Cluster Server

Veritas™ Cluster Server (VCS) by Symantec provides High Availability (HA) and Disaster Recovery (DR) for mission critical applications running in physical and virtual environments. VCS ensures continuous application availability despite application, infrastructure or site failures.

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 the IBM XL C/C++ for AIX Compiler Version 8.0. Use the -brtl flag for runtime linking with the framework library.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

SORT can help you do the following:

Prepare for your next installation or upgrade	■ List product installation and upgrade requirements, including operating system versions, memory, disk space, and architecture. ■ Analyze systems to determine if they are ready to install or upgrade Symantec products. ■ Download the latest patches, documentation, and high availability agents from a central repository. ■ Access up-to-date compatibility lists for hardware, software, databases, and operating systems.

Manage risks	■ Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDLs), and high availability agents from a central repository. ■ Identify and mitigate system and environmental risks. ■ Display descriptions and solutions for hundreds of Symantec error codes.
Improve efficiency	■ Find and download patches based on product version and platform. ■ List installed Symantec products and license keys. ■ Tune and optimize your environment.

Note: Certain features of SORT are not available for all products. Access to SORT is available at no extra cost.

To access SORT, go to:

https://sort.symantec.com

Important release information

- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:
  http://www.symantec.com/docs/TECH164885
- For the latest patches available for this release, go to:
  http://sort.symantec.com/
- The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit the following URL:
  http://www.symantec.com/docs/TECH170013
  Before installing or upgrading Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

Changes introduced in 6.0

This section lists the changes in Veritas Cluster Server 6.0.

Changes related to installation and upgrades

The product installer includes the following changes in 6.0.

Support for product upgrades using the Network Installation Manager Alternate Disk Migration utility on AIX

You can now use the Network Installation Manager Alternate Disk Migration (nimadm) utility to upgrade the operating system and the product.

See the *Installation Guide* for more information.

Support for additional VCS installation and upgrade scenarios using native AIX operating system tools

This release supports additional installation and upgrade scenarios using native AIX operating system tools such as Network Installation Manager (NIM) and Alternate Disk Installation (ADI).

Table 1-1 Supported installation and upgrade scenarios

Native OS method	Install (Only product)	Install (Product + OS)	Upgrade (Only product)	Upgrade OS and Install product	Upgrade (Product + OS)
NIM	Supported	Supported	Not supported	Not supported	Not supported
Alternate Disk	Not supported	Not supported	Supported (TL and SP only)	Not supported	Supported (TL and SP only)
NIMADM	Not supported	Not supported	Not supported	Not supported	Supported

The installer can now detect duplicate VCS cluster IDs and can automatically generate cluster IDs

The installer can now detect duplicate VCS cluster IDs and prompt you to select an unused one. It can also generate an unused ID during installation.

The installer can check product versions and hotfixes

You can check the existing product versions using the installer command with the `-version` option before or after you install. After you have installed the current version of the product, you can use the `showversion` script in the /opt/VRTS/install directory to find version information.

You can discover the following information with these commands:

- The installed version of all released Strorage Foundation and High Availability Suite of products
- The missing required filesets or patches as applicable for platform
- The available updates (including patches or hotfixes) from SORT for the installed products

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

Using the installer's postcheck option

You can use the installer's postcheck option to diagnose installation-related problems and to provide troubleshooting information.

Rolling upgrade improvements

The rolling upgrade procedure has been streamlined and simplified.

Packaging updates

The following lists the package changes in this release.

- New `VRTSsfcpi60` fileset for product installer scripts

  The `VRTSsfcpi60` fileset is introduced in this release. The VRTSsfcpi60 fileset contains the installer scripts and libraries that the installer uses to install, configure and upgrade Veritas products.
- New `VRTSvbs` fileset

  The `VRTSvbs` fileset enables the VBS command line interface on a Veritas Operations Manager managed host in a Virtual Business Services configuration. For more information, see the *Virtual Business Service–Availability User's Guide*.
- `VRTSvcsag` fileset change

  The `/etc/VRTSvcs/conf/types.cf` and various sample configurations are packaged with the `VRTSvcsag` fileset instead if the `VRTSvcs` fileset. This is to ease hotfix installation for bundled agents that require attribute changes.

For more information, see the *Installation Guide*.

Online Migration of native LVM volumes to VxVM volumes

In this release, Veritas Volume Manager (VxVM) provides a feature to migrate volumes under native LVM control to VxVM volumes, with a limited application downtime.

This migrates source LVM volume data to target VxVM volumes on new storage, with the flexibility of different storage and layouts. Once the migration is set up, the application can be resumed, while data synchronization from source LVM to target VxVM volumes continues in the background.

The migration configuration is set up such that the application does not require immediate reconfiguration to the new VxVM device paths.

You can also choose the point of committing the migration, when data synchronization is complete for all required volumes. In case of errors, it provides a way to abort the migration and safely revert to the original LVM configuration.

This feature is also integrated with VCS to provide online migration in a VCS HA environment. During the migration process, VCS monitors and maintains high availability of the updated configuration.

A new CLI `vxmigadm` is provided, to administer online migration.

For more details, refer to *Veritas™ Storage Foundation and High Availability Solutions Solutions Guide*.

Changes to the VCS engine

Support multiple children in service group dependency

A service group can have dependency on multiple child service groups. All child dependencies must be satisfied for the parent service group to go online. The dependency types which are not supported in a multiple child configuration are "online local hard" and "offline local". The `-propagate` option cannot be used if the dependency tree contains global and/or remote dependency.

For more details, refer to the *Administrator's Guide*.

Single command line option to online or offline service groups in a service group dependency

If you have a parent service group in a service group dependency, you can online the entire dependency tree bottom-up with a single command, without having to online each group manually. For online operation, the command starts to online the service groups from the lowermost service group in dependency tree. Similarly, If you have a child service group in a service group dependency, you can offline the entire dependency tree top-down with a single command, without having to offline each group manually. For offline operation, the command offlines the service group from the top of the dependency tree.

You can use the following commands to online or(and) offline the service groups respectively:

- `hagrp -online -propagate <grp_name> -sys <sys_name>`
- `hagrp -offline -propagate <grp_name> -sys <sys_name>`

Note: The `-propagate` option cannot be used if the dependancy tree contains global and/or remote dependency.

Using the `-propagate` option with `hagrp -online`, all required child service groups are automatically brought online by VCS. Similarly using the `-propagate` option with `hagrp -offline`, all the required parent groups are automatically brought offline by VCS.

VCS support of CPU interrupt disablement on AIX

HAD process runs at a high priority on the system; however, interrupts are always run at the highest priority. In case lot of interrupts are generated on the system and the CPU where HAD process is running gets to service them, HAD does not get a chance to heartbeat with GAB and perform its task of making applications highly available.

To overcome this issue, VCS allows you to run HAD on a specific processor and mask off all interrupts on that processor. You can configure HAD to run on a specific processor by setting the CPUBinding attribute.

For more information on CPU binding of HAD, refer to *Veritas Cluster Server Administrator's Guide*.

Ability to send notifications to a wider audience

You can configure users, other than the owners of resources, resource types, service groups, systems, or clusters, as recipients of notifications about events related to a resource, resource type, service group, system, or cluster.

Use the following attributes to configure recipients of notifications:

- ResourceRecipients
- TypeRecipients
- GroupRecipients
- SystemRecipients
- ClusterRecipients

The registered recipients get notifications about the events that have a severity level that is equal to or greater than the level specified in the attribute. For more information, see *Veritas Cluster Server Administrator's Guide*.

Ability to specify a single user across all nodes of VCS cluster

You can add a user to the VCS configuration without specifying the host name, such as **admin** and assign administrator privileges. The admin user can log in using the host-specific credentials and perform any administrative operations.

Thus, you need not add the same user, 'admin', multiple times in the VCS configuration as admin@host1, admin@host2, and so on. Once added, the user can operate from any node of the cluster.

VCS now supports clusters with mixed operating system versions of AIX

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

Caution: While using mixed operating systems (OS) for an extended period of time, you may see issues with migrating OS-specific applications between major versions of the OS.

Changes related to IMF

This release includes the following changes to Intelligent Monitoring Framework (IMF):

IMF is enabled by default and has new agent support

The Intelligent Monitoring Framework (IMF) functionality is enabled by default for all agents that can leverage IMF.

The following agents are IMF-aware in VCS 6.0:

- WPAR
- DB2udb (provides only PRON IMF support)
- Sybase
- SybaseBk

Enable and disable IMF by automated script for agents

VCS provides the `/opt/VRTSvcs/bin/haimfconfig` script to enable and disable IMF for agents when VCS is either running or stopped. You can use this script to disable IMF for all IMF-aware agents, including bundled agents, enterprise agents, and custom agents. You must run the script once on each node of the cluster.

Note: The automated script restarts the agent, if it is running on the current node, to enable the IMF after confirming with the user.

Prevention of Concurrency Violation (PCV) using IMF

With the new IMF-based Proactive PCV feature, VCS can proactively prevent the same VCS failover service group from coming online on more than one node in the cluster. Typically, VCS detects such a concurrency violation after it has occurred. This feature is available only for application resources and is disabled by default.

For more information, refer to the *Administrator's Guide*.

Support plug-in for AMF support in custom agents

Script-based custom agents can now leverage IMF functionality by following the steps documented in the *Veritas Cluster Server Agent Developer's Guide*.

Enhanced amfstat utility

The `amfstat` utility is enhanced to display the new event types that AMF driver can support. For more details, refer to the `amfstat` man pages.

Changes related to VCS triggers

This release includes the following changes related to VCS triggers:

- VCS can execute trigger scripts specific to a service group and/or resource. Thus, trigger scripts for multiple objects need not be merged into single trigger script.
- You can enable the `nofailover`, `postonline` and `postoffline` triggers for each system by using the TriggersEnabled attribute.
- You can execute multiple scripts for a trigger. The trigger scripts must be installed inside the trigger directory using the `T<num>` nomenclature. VCS executes the trigger scripts in `T<num>` order.

  For example: If the preonline directory contains the scripts `T00preonline`, `T01preonline`, `T02preonline`, then the script `T00preonline` is executed first, then `T01preonline` and finally, `T02preonline` is executed.
- The agent restarts a faulted resource if the RestartLimit is set. Whenever the agent restarts a resource, VCS invokes the `resrestart` trigger if the TriggerResRestart attribute is set to 1 or if RESRESTART is specified in the

TriggersEnabled attribute. Otherwise, VCS invokes the `resstatechange` trigger. See the *Veritas Cluster Server Administrator's Guide* for more information.

Caution: Use of `resstatechange` to indicate restart is being deprecated. In later releases, you must use only the `resrestart` trigger to indicate restarting of resources.

New attributes

The following sections describe the attributes introduced in VCS 6.0, 5.1SP1, VCS 5.1, and VCS 5.0MP3.

Attributes introduced in VCS 6.0

Cluster-level attribute

- SystemRebootAction: Use this attribute to determine whether the frozen service groups are ignored on system reboot. If the value of SystemRebootAction is IgnoreFrozenGroup, VCS ignores the service groups that are frozen (TFrozen and Frozen) and takes the remaining service groups offline. If the Value of SystemRebootAction is "", VCS tries to take all service groups offline. See the *Veritas Cluster Server Administrator's Guide* for more information.
- EnableVMAutoDiscovery: Enables or disables auto discovery of virtual machines. By default, auto discovery of virtual machines is disabled.
- SystemRebootAction: Determines whether frozen service groups are ignored on system reboot.

Service group attributes

- OnlineClearParent: When this attribute is enabled for a service group and the service group comes online or is detected online, VCS clears the faults on all online type parent groups, such as online local, online global, and online remote.
- ProPCV: Indicates whether the service group is proactively prevented from concurrency violation for ProPCV-enabled resources.
- TriggerPath: Enables you to customize the trigger path.
- TriggerResRestart: Determines whether or not to invoke the restart trigger if resource restarts.
- TriggersEnabled: Determines if a specific trigger is enabled on a node or not.

Resource type attributes:

- AdvDbg: Enables activation of advanced debugging.

Sybase agent attributes:

- interfaces_File: Specifies the location of interfaces file for the Sybase instance. If this attribute is configured, [-I interfaces file] option is used when connecting to the isql session. If this attribute is not configured, the agent does not use the -I option.
- ShutdownWaitLimit: Specifies the maximum number of seconds for which the agent waits for the Sybase instance to stop after issuing the `shutdown with wait` command, and before attempting to issue the `kill -15 <data server-pid>` command, if required.
- DelayAfterOnline: Specifies the number of seconds that elapse after the Online entry point is complete and before the next monitor cycle is invoked.
- DelayAfterOffline: Specifies the number of seconds that elapse after the Offline entry point is complete and before the next monitor cycle is invoked.

SybaseBk agent attribute:

- interfaces_File: Specifies the location of the interfaces file for the Sybase instance. If this attribute is configured, [-I inerfaces file] option is used when connecting to the isql session. If this attribute is not configured, the agent does not use the -I option.

Oracle agent attributes

- DBName: Specifies the database name. This attribute is required only for a policy-managed database. The value of this attribute must be set to the database name.
- ManagedBy: Specifies whether the database is administrator-managed or policy-managed. The default value of this attribute is ADMIN. You need not explicitly set its value. In a policy managed RAC database, this attribute must be set to **POLICY**.

DiskGroupSnap agent attributes:

- FDType: Specifies the configuration to be used for the firedrill. The possible values of this attribute are Bronze and Gold (default).

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. See the *Bundled Agents Reference Guide* for more information.
  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.

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 “metric 2” then “metric 2” option is set on the interface while bringing IPMultiNICB resource online.

LVMVG agent attribute

- ModePermSyncFlag: This attribute is added to get the mode and permissions without activating the volume group. The default value of ModePermSyncFlag is 1. To skip the activation of the volume group before before preserving mode and permissions, set the value of ModePermSyncFlag attribute to 0 (zero).

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.

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.

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.

WPAR agent attributes

- ResourceSet: A resource set is used to define a subset of processors in the system. If a resource set is specified for a workload partition, it can use the processors within the specified resource set only. The value of the ResourceSet attribute is the name of the resource set created using the `mkrset` command. If set, the agent configures the WPAR to use only the resource set specified by this attribute.
- WorkLoad: Allows modification of resource control attributes of WPAR - shares_CPU and shares_memory. This attribute has two keys, CPU and MEM. The key CPU is used to specify the number of processor shares that are available to the workload partition. The key MEM is used to specify the number of memory shares that are available to the workload partition.

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 VCS bundled agents

This section describes changes to the bundled agents for VCS.

See the *Veritas Cluster Server Administrator's Guide* and *Veritas Cluster Server Bundled Agents Reference Guide* for more information.

Support for Windows DNS server

The DNS agent now supports Windowcs DNS server in its configuration. A new attribute UseGSSAPI is added to DNS agent configuration for this functionality.

See the *Veritas Cluster Server Bundled Agents Reference Guide* for more information on using this attribute and additional requirements for configuring DNS agent with Windows DNS server.

DNS agent supports DNS scavenging for Windows DNS servers

DNS agent can now be configured to send periodic refresh request to configured Windows DNS servers to avoid aging and scavenging of resource records.

Added support for DR of AIX WPAR

The WPAR agent is enhanced to accept cluster (subnet) specific network parameters that are applied when the agent starts the WPAR. These are mainly the DNS settings for the WPAR.

RVGPrimary agent starts replication from new primary post role change to the other secondaries in the RDS

After a successful migration or takeover of a Secondary RVG, the RVGPrimary agent ensures to automatically start the replication from the new Primary to the additional Secondary(s) that exists in the RDS, if any.

Refer to the *SF Replication Administrator's Guide* for information about how the RVGPrimary agent works in a multiple secondary setup.

LVMVG agent on AIX supports synchronization of ODM entries

LVMVG agent on AIX now supports synchronization of the ODM entries of all the nodes in a cluster, if the disk configuration of the volume group is changed on a node.

If physical volumes are added, deleted or replaced in a volume group, some or all of the ODM entries on other nodes become stale. This may cause the volume group resource online failure on those nodes. The updated disk information can now be propagated to all nodes in the cluster using “updatepv” action entry point. See the *Bundled Agent Reference Guide* for more information about the updatepv action entry point.

Improved LVMVG agent performance on AIX

The LVMVG monitor is now C++ based and uses LVM API. Therefore, the CPU utilization is low even with large number of LVMVG resources.

Campus Cluster firedrill made easy

Campus Cluster firedrill configuration has been made easier by introducing a new attribute FDType. You can control the firedrill flavor by setting just this attribute instead of specifying specific values for other attributes.

You need to install the Global Cluster Option (GCO) license to run firedrill in a Campus Cluster configuration.

Change in behavior of DiskGroup agent

The following changes have been affected to the DiskGroup agents:

- The type of the attribute PanicSystemOnDGLoss is changed from boolean to integer. Attribute PanicSystemOnDGLoss now accepts the following values:
  0: Do not halt the system
  1: Halt the system if either disk groups go into disabled state or the disk group resource faults due to monitor timeout.
  2: Halt the system if disk group goes into disabled state.
  3: Halt the system if disk group resource faults due to monitor timeout.
- The monitor agent function takes the service group containing the DiskGroup resource offline if the MonitorReservation attribute is set to 0, the value of the cluster wide attribute UseFence is set to SCSI3, and if the disk group is found imported without SCSI reservation.

Application agent enhancements

Application agent has undergone the following enhancements:

- Enhanced agent to support shared disk for StartProgram, StopProgram, MonitorProgram, and CleanProgram.
- Enhanced agent to understand Unix style for return codes for MonitorProgram, 0 (ONLINE) and 1 (OFFLINE).

Apache agent enhancements

The following are the enhancements to the Apache agent

- The httpDir attribute is enhanced such that you can specify the full path of the binary (including the binary name). If you specify only the directory name, the agent assumes the default binary name httpd.
- If the Apache Benchmarking binary in the httpDir directory does not use the default name, then the agent recognizes the alternative binary name ab2, and performs detail monitoring.
- Enhanced Apache agent version parsing to accommodate IBM HTTP server 7.0.

Enable IMF for WPAR Agent

The WPAR agent now leverages the IMF functionality for instantaneous detection of resource state change. This also reduces the CPU footprint of the agent by significantly reducing the periodic monitoring for resource states.

For more information refer to the *Administrator's Guide*.

First failure data capture for VCS agent entry point times out

To debug entry point timeout, a new attribute AdvDbg is introduced. The attribute helps VCS are some information like process stack, process tree and core on entry point timeout. This is helpful in troubleshooting entry point timeout scenarios.

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

MultiNICA resource with IPv6 goes to UNKNOWN state if the protocol is not set to IPv6

In versions before VCS 6.0 , if you used MultiNICA resource with IPv6 addresses and if you did not set the Protocol attribute to IPv6, the Protocol attribute took the default value of IPv4, which was not a desired condition. In VCS 6.0, this behavior is corrected such that if the Protocol attribute is not set to IPv6, the MultiNICA resource goes to the UNKNOWN state.

Changes in network agents

The NetMask attribute is a required attribute for the following agents:

- IP
- IPMultiNIC
- IPMultiNICA
- IPMultiNICB

Changes to database agents

Changes to DB2 agent

- The VCS agent for DB2 now supports intelligent resource monitoring for online Db2 processes in PRON mode for non-MPP and MPP configuration mode.
- Prior to VCS 6.0 release, in case of partition mobility from source node to the target node having high speed inter-connect/switch configuration, the switch name entry would not get updated in the db2nodes.cfg configuration file. In VCS 6.0 release, the DB2 agent ensures that the switch name gets updated correctly in the configuration file.
- Added IMF support for DB2 agent: The DB2 agents now leverages the IMF functionality for instantaneous detection of resource state change. This also reduces the CPU footprint of the agent by significantly reducing the periodic monitoring for resource states.
  See the *Administrator's Guide* for more information.

Changes to the Oracle agent

- The VCS agent for Oracle has two new attributes: DBName and ManagedBy.
- The VCS agent for Oracle has additional options to the StartUpOpt and ShutDownOpt attributes:
  - The StartUpOpt attribute introduces SRVCTLSTART_RO as additional startup options.
  - The ShutDownOpt attribute introduces SRVCTLSTOP_TRANSACT, SRVCTLSTOP_ABORT, and SRVCTLSTOP_IMMEDIATE as additional shut down options.
- The VCS agent for Oracle introduces support for policy managed database.
- The VCS agent for Oracle ASM instance introduces the following additional Startup options:

- STARTUP_MOUNT
- STARTUP_OPEN
- SRVCTLSTART_MOUNT
- SRVCTLSTART_OPEN

- The VCS agent for Oracle ASM instance introduces the following additional Shutdown option:
  - SRVCTLSTOP
- With Oracle version 11.2.0.2, the Oracle agent for VCS supports Startup and Shutdown options that use `srvctl` utility for Oracle restart configuration.

Changes to the Sybase agent

The Veritas Cluster Server agent for Sybase includes the following new or enhanced features:

- The VCS agents for Sybase and SybaseBk now support intelligent resource monitoring.
- Intelligent monitoring framework (IMF) is enabled by default in VCS 6.0 release. The `haimfconfig` script can be used to enable/disable IMF for Sybase and SybaseBk agents. The Sybase agent now leverages the IMF functionality for instantaneous detection of resource state change. This also reduces the CPU footprint of the agent by significantly reducing the periodic monitoring for resource states.
  See the *Administrator's Guide* and *Agent for Sybase Installation and Configuration Guide* for more information.
- The Sybase agent introduces the following new attributes:
  - interfaces_File
  - ShutdownWaitLimit (default value 60)
  - DelayAfterOnline (default value 10)
  - DelayAfterOffline (default value 2)
- The SybaseBk agent introduces the following new attribute:
  - interfaces_File
- The default value of ToleranceLimit attribute is set to 1 (one) for Sybase agent.
- The DetailMonitor attribute is deprecated in VCS 6.0. Instead, LevelTwoMonitorFreq attribute of Sybase agent may be used. The default value of LevelTwoMonitorFreq attribute is 0 (zero).

- The long pathname limitation for $SYBASE is resolved.
- With VCS 6.0 release using VCS Cluster Manager (Java Console), Sybase and SybaseBk agents encrypt the password by default. Sybase and SybaseBk agents supports both plain text and encrypted password. If required, the plain text value can be specified for agent attributes using the command line or by editing the configuration file.
- Sybase agent uses new timeout option during shutdown of Sybase dataserver used instead of "shutdown with nowait". For Sybase ASE Enterprise edition the timeout option for shutdown command is supported for versions 12.5.4 and 15.0.2 onwards.

Changes to VCS clusters in secure mode

In this release, the installation and configuration experience of secure cluster is considerably simplified. You can easily convert the cluster into secure cluster with this simplified secure cluster configuration model.

The new architecture is based on embedded VxAT, where the security components are installed as a part of the VCS package. The root broker is no longer a single-point-of-failure in the new architecture. There is no dependency on a separate VRTSat package. Non-root users who are already logged on VCS hosts are now not prompted for password. Additionally, a cluster-level user feature is introduced to simplify user administration in secure clusters.

See the *Installation Guide* and *Administrator's Guide* for more information.

Changes to LLT

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

- LLT now supports VLAN tagging (IEEE 802.1Q).
- The `lltconfig` command includes the following new options:
  - -N
    You can use this option to list all the used cluster IDs.
  - -M
    You can use this option to display the currently loaded LLT module version information.

  See the `lltconfig` manual page for more information.
- Link utilization statistics are enhanced that help in the root cause analysis of performance related issues.
- Periodic flushing of ARP cache is disabled.

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

Changes to GAB

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

Better GAB and I/O fencing integration to ensure application availability

In the event of a split-brain situation before VxFEN module implements the decision, sometimes GAB proceeds with attempting to resolve the join after the split-brain. GAB removes all but one joining subcluster. This behavior can cause the entire cluster to shut down. To avoid this scenario, GAB now gives priority to the fencing module.

With the GAB and I/O fencing integration in this release, if the I/O fencing module's decision is still pending before GAB initiates a join of the subcluster, GAB delays the iofence message. GAB wait depends on the value of the VxFEN tunable parameter *panic_timeout_offst* based on which VxFEN computes the delay value and passes to GAB.

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

GAB can now recognize clients with names in addition to ports

When kernel clients initialize GAB API, they can now define a client name string. GAB now adds a client name which enables GAB to track the client even before GAB port is registered. GAB also passes the client name information to LLT when registering the LLT port. The `lltstat -p` command also displays the GAB client names when providing the status details of the ports in use.

This feature is applicable only to GAB kernel clients, and not applicable for user-land GAB clients such as HAD.

The gabconfig command has new -C option

The -C option of the `gabconfig` command lists the names of the GAB clients that have registered with GAB. The `-C` option when used with `-a` option lists the client names along with the port membership details.

Changes to I/O fencing

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

Installer support to migrate between fencing configurations in an online cluster

You can now use the installer to migrate between disk-based and server-based fencing configurations. You can also replace the coordination points for any I/O fencing configuration in an online cluster using the same installer option. The installer uses the `vxfenswap` script internally.

You can also use response files to perform these I/O fencing reconfiguration operations.

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

Support for racer node re-election during I/O fencing race

At the time of a network partition, the VxFEN module elects the lowest node in each sub-cluster as the racer node to race for the coordination points on behalf of the sub-cluster. The other spectator nodes wait on the racer node to do the fencing.

In the previous releases, the I/O fencing race was entirely dependent on the single racer node as follows:

- If the racer node is not able to reach a majority of coordination points, then the VxFEN module on the racer node sends a LOST_RACE message and all nodes in the subcluster also panic when they receive the LOST_RACE message.
- If the racer node panics during the arbitration, then the spectator nodes in the sub-cluster assume that the racer node lost the race and the spectator nodes also panic.

With the new racer node re-election feature, the VxFEN module re-elects the node with the next lowest node id in the sub-cluster as the racer node. This feature optimizes the chances for the sub-cluster to continue with the race for coordination points.

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

Support for multiple virtual IP addresses in CP servers

You can now configure multiple network paths (virtual IP addresses) to access a CP server. CP server listens on multiple virtual IP addresses. If a network path fails, CP server does not require a restart and continues to listen on one of the other available virtual IP addresses.

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

Support for Quorum agent in CP servers

With the support for multiple virtual IP addresses, you can now use the Quorum agent to configure CP server service group failover policies. You can specify the minimum number of IP resources that must be online for the Quorum resource to remain online.

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

With fencing enabled, GAB can now automatically seed the cluster when some cluster nodes are unavailable

In the earlier releases, if some of the nodes are not up and running in a cluster, then GAB port does not come up to avoid any risks of preexisting split-brain. In such cases, you can manually seed GAB using the command `gabconfig -x` to bring the GAB port up. However, if you have enabled I/O fencing in the cluster, then I/O fencing can handle any preexisting split-brain in the cluster.

In this release, I/O fencing has extended this functionality to be able to automatically seed GAB as follows:

- If a number of nodes in a cluster are not up, GAB port (port a) still comes up in all the member-nodes in the cluster.
- If the coordination points do not have keys from any non-member nodes, I/O fencing (GAB port b) also comes up.

This new functionality is disabled by default. You must manually enable this automatic seeding feature of GAB in clusters where I/O fencing is configured in enabled mode.

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

You can still use the `gabconfig -x` command to manually seed the cluster.

Graceful shutdown of a node no longer triggers I/O fencing race condition on peer nodes

In the earlier releases, a gracefully leaving node clears its I/O fencing keys from coordination points. But the remaining sub-cluster races against the gracefully leaving node to remove its registrations from the data disks. During this operation, if the sub-cluster loses access to the coordination points, the entire cluster may panic if the racer loses the race for coordination points.

In this release, this behavior has changed. When a node leaves gracefully, the CVM or other clients on that node are stopped before the VxFEN module is unconfigured. Hence, data disks are already clear of its keys. The remaining

sub-cluster tries to clear the gracefully leaving node's keys from the coordination points but does not panic if it is not able to clear the keys.

Changes related to virtualization support

This section lists virtualization changes for this release.

New LPAR agent on AIX

The LPAR agent monitors the logical partitions running on the same physical host and brings them online and offline. LPAR agent communicates with HMC to perform its operations.

You can use this agent to make the LPARs highly available and to monitor them. This agent is added as a part of virtualization support.

Licensing changes in the SFHA Solutions 6.0 release

Storage Foundation and High Availability Solutions 6.0 introduces the following licensing changes:

- The Cluster File System license is deprecated. CFS customers are entitled to the Storage Foundation Cluster File System High Availability (SFCFS HA) functionality.
- The VVR Option is renamed as Veritas Replicator Option. This option includes VVR (volume-based replication) and the new file-based replication solution.
- The VVR Enterprise license is deprecated; you can use Storage Foundation Enterprise and add Veritas Replicator Option to get this functionality. VVR Enterprise customers are entitled to Storage Foundation Enterprise with Replicator Option.
- The VCS license enables full cluster functionality as well as the limited start/stop functionality.
- Storage Foundation Enterprise CFS for Oracle RAC (Linux/x64) customers are entitled to Storage Foundation Enterprise for Oracle RAC (Linux/x64.)

The following functionality is included in the Standard and Enterprise licenses:

- The Compression feature is available with the Standard license.
- The SmartTier feature is now available with the Standard license.
- The Deduplication feature is available with the Enterprise license.

The following products are included in this release:

- Dynamic Multi-Pathing

- VirtualStore
- Storage Foundation Basic
- Storage Foundation Standard
- Storage Foundation Enterprise
- Veritas Cluster Server
- Veritas Cluster Server HA/DR
- Storage Foundation Standard HA: Storage Foundation Standard plus Veritas Cluster Server
- Storage Foundation Enterprise HA: Storage Foundation Enterprise plus Veritas Cluster Server
- Storage Foundation Enterprise HA/DR
- Storage Foundation Enterprise Cluster File System HA
- Storage Foundation Enterprise Cluster File System HA/DR
- Storage Foundation Enterprise for Oracle RAC
- Storage Foundation Enterprise HA/DR for Oracle RAC
- Storage Foundation Enterprise for Sybase ASE CE
- Storage Foundation Enterprise HA/DR for Sybase CE

HA: High Availability

HA/DR: High Availability and Disaster Recovery

Veritas Replicator Option can be added to all Storage Foundation and High Availability products, except Dynamic Multi-Pathing and Veritas Cluster Server.

Note that products, features, and options may differ by operating system and platform. Please see the product documentation for information on supported platforms.

Enhancements to collecting a VxExplorer troubleshooting archive

The Symantec Operations Readiness Tools (SORT) data collector contains functionality to collect and submit a VxExplorer archive. You can send this archive to Symantec Technical Support for problem diagnosis and troubleshooting. VxExplorer does not collect customer data.

The legacy `VxExplorer` script now works differently. When you run the script, it launches the SORT data collector on the specified local host with the `-vxexplorer` option.

To learn more about using the data collector to collect a VxExplorer archive, see:

www.symantec.com/docs/HOWTO32575

Changes related to product documentation

The Storage Foundation and High Availability Solutions 6.0 release includes the following changes to the product documentation.

Table 1-2 lists the documents introduced in this release.

Table 1-2 New documents

New documents	Notes
Veritas Storage Foundation Installation Guide	Installation and upgrade information for Storage Veritas Foundation.
Veritas Storage Foundation Administrator's Guide	Administration information for Veritas Storage Foundation.
Veritas Storage Foundation and High Availability Release Notes	Release-specific information for Veritas Storage Foundation and High Availability users.
Veritas Storage Foundation and High Availability Solutions Solutions Guide	Solutions and use cases for Veritas Storage Foundation and High Availability Solutions.
Veritas Storage Foundation and High Availability Solutions Troubleshooting Guide	Troubleshooting information for Veritas Storage Foundation and High Availability Solutions.

Table 1-3 lists the documents that are deprecated in this release.

Table 1-3 Deprecated documents

Deprecated documents	Notes
Veritas File System Administrator's Guide	Content now appears in the *Veritas Storage Foundation Administrator's Guide* and in the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.
Veritas Volume Manager Administrator's Guide	Content now appears in the *Veritas Storage Foundation Administrator's Guide* and in the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

Table 1-3 Deprecated documents *(continued)*

Deprecated documents	Notes
Veritas Storage Foundation Advanced Features Administrator's Guide	Content now appears in the *Veritas Storage Foundation and High Availability Solutions Solutions Guide.*
Veritas Volume Manager Troubleshooting Guide	Content now appears in the *Veritas Storage Foundation and High Availability Solutions Troubleshooting Guide.*
Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide	Content now appears in the *Veritas Cluster Server Bundled Agents Reference Guide.*
Veritas Volume Replicator Planning and Tuning Guide	Content now appears in the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide.*
Veritas Volume Replicator Advisor User's Guide	Content now appears in the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide.*

Table 1-4 lists documents that are no longer bundled with the binaries. These documents are now available online.

Table 1-4 Online documents

Document
Veritas Cluster Server Agent Developer's Guide
Veritas File System Programmer's Reference Guide

Changes introduced in VCS 5.1SP1PR1

This section introduces the changes introduced in VCS 5.1SP1PR1.

Support for AIX 7.1

VCS 5.1SP1PR1 supports AIX 7.1.

Attributes supported in VCS 5.1SP1PR1

The following attributes are supported in addition to those introduced in VCS 5.1SP1.

WPAR agent attributes:

- ResourceSet: A resource set is used to define a subset of processors in the system. If a resource set is specified for a workload partition, it can use the processors within the specified resource set only. The value of the ResourceSet attribute is the name of the resource set created using the `mkrset` command. If set, the agent configures the WPAR to use only the resource set specified by this attribute.
- WorkLoad: : Allows modification of resource control attributes of WPAR - shares_CPU and shares_memory. This attribute has two keys, CPU and MEM. The key CPU is used to specify the number of processor shares that are available to the workload partition. The key MEM is used to specify the number of memory shares that are available to the workload partition.

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 supports an environment where a few nodes in the cluster are hosted on LPARs with storage and network connectivity presented to the OS using VIOS. The remaining nodes in the cluster are hosted on physical systems with storage and network connectivity presented to the OS directly. However SCSI3 I/O fencing is not supported in this environment.

VCS requires that all nodes in the cluster use the same processor architecture and 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 37.

See "Supported AIX operating systems " on page 38.

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/TECH170013

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

Supported AIX operating systems

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

Table 1-5 shows the supported operating systems for this release.

Table 1-5 Supported operating systems

Operating systems	Levels	Chipsets
AIX 7.1	TL0 or later	Any chipset that the operating system supports
AIX 6.1	TL5 or later	Power 7, Power 6, or earlier

AIX 7.1 support for virtual processors

Veritas Cluster Server supports up to 1024 virtual processors on AIX 7.1.

Supported software for VCS

VCS supports the following volume managers and file systems:

- Logical Volume Manager (LVM)
- Journaled File System (JFS) and Enhanced Journaled File System (JFS2) on LVM
- Veritas Storage Foundation (SF): Veritas Volume Manager (VxVM) with Veritas File System (VxFS)

  VCS 6.0 supports the following versions of SF:

  - SF 6.0
    - VxVM 6.0 with VxFS 6.0
  - SF5.1SP1
    - VxVM 5.1SP1 with VxFS 5.1SP1

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

Supported VCS agents

Table 1-6 lists the agents for enterprise applications and the software that the agents support.

Table 1-6 Supported software for the VCS agents for enterprise applications

Agent	Application	Application version	AIX version
DB2	DB2 Enterprise Server Edition	9.1, 9.5, 9.7	AIX 6.1, AIX 7.1
Oracle	Oracle	10gR2, 11gR1, 11gR2	AIX 6.1, AIX 7.1
Sybase	Sybase Adaptive Server Enterprise	12.5.x, 15.x	AIX 6.1, AIX 7.1

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.

No longer supported

The following features are not supported in this release of VCS products:

- Several documents are deprecated in this release.
  See "Changes related to product documentation" on page 35.

No longer supported agents and components

VCS no longer supports the following:

- Configuration wizards
- ServiceGroupHB agent.
  This release does not support disk heartbeats. Symantec recommends using I/O fencing.
- VRTSWebApp
- Oracle 8.0.x, Oracle 8.1.x, and Oracle 9i - not supported by the 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.

- The *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide* is deprecated and its content is accommodated in the *Veritas Storage Foundation and HIgh Availability Solutions Replication Administrator's Guide* and *Veritas Cluster Server Bundled Agents Reference Guide*.
- hahbsetup tool. This tool is removed as no supported feature requires this tool.
- VRTScutil fileset. This fileset is no longer supported.

Deprecated attributes

Deprecated Oracle agent attributes:

- AgentDebug
- DetailMonitor

Deprecated LVMVG agent attribute:

- ModePermSyncFlag

Deprecated Mount agent attributes:

- SecondLevelMonitor
- SecondLevelTimeout

Deprecated Host Monitor attribute:

- CPUUsageMonitoring: The attribute can no longer be used to disable CPU usage monitoring by Host Monitor agent.

Sybase agent attribute:

- DetailMonitor

Fixed issues

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

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

See "Documentation" on page 92.

LLT, GAB, and I/O fencing fixed issues

Table 1-7 lists the fixed issues for LLT, GAB, and I/O fencing.

Table 1-7 LLT, GAB, and I/O fencing fixed issues

Incident	Description
2563177	[Fencing] Uninstallation of VRTSvxfen package shows error message when the GAB port b does not show up even when VxFEN is being used in case GAB is waiting for seeding.
2515932	[GAB] gabconfig ioctl behaviour changed to return EALREADY if GAB is already configured.
2509400	[GAB] System crashed when uninstalling the GAB package.
2495020	[Fencing] vxfend does not terminate if you run the `vxfenswap` command to change the fencing mode from 'scsi3' to 'customized', and chooses to rollback when vxfenswap prompts for confirmation.
2481098	[LLT] Improve LLT over UDP performance.
2442402	[LLT] Reduce lltd CPU consumption by reducing the wakeup calls.
2437022	[Fencing] Fails to run the `vxfenswap` command to the same diskgroup when the disk policy changed.
2426664	[Fencing] vxfend does not terminate when you run the `vxfenswap` command to migrate from the customized mode to the scsi3 mode.
2411652	[GAB] Add a check in GAB for MAX message size of 64KB before enqueuing the message.
2386325	[Fencing] Fencing configuration fails and vxfenadm prints same serial number for all LUNs which have more than 96 bytes of SCSI Inquiry data in page 0x83.
2369742	[Fencing] Once vxfenconfig -c with a particular mode (say customized) has returned EFAULT ("1036 Unable to configure..."), all subsequent runs of vxfenconfig -c with a different mode (say scsi3) fail with error EBADMSG ("1050 Mismatched modes...").
2351011	[Fencing] The vxfenswap utility fails to accurately check for the exit status of the vxfenconfig commands run on the other nodes in the background. This may lead to the vxfenswap utility appearing indefinitely hung if the vxfenconfig process does not succeed for any reason.
2337916	[Fencing] Fencing shutdown script does not retry stopping the fencing module if fencing fails to unconfigure because of clients being registered.
2311361	[Fencing] Fencing details are printed in the engine logs every five minutes if fencing is running and the CoordPoint resource is configured.

Table 1-7 LLT, GAB, and I/O fencing fixed issues *(continued)*

Incident	Description
2254947	[Fencing] VxFEN tunable resets when node comes up after panic.
2253321	[Fencing] Fencing fails to start if any of the coordination points is unavailable at the startup time.
2252470	[Fencing] Provide options to force the fencing library to obtain serial numbers using standard inquiry or extended inquiry using a variety of ID types.
2242747	[LLT] Disable the fastpath in LLT and make it optional.
2218448	[VxCPS] The cpsadm command fails if LLT is not installed or configured on a single-node cluster which hosts the CP server.
2209664	[VxCPS] Configuring fencing is successful with three disks even when single_cp=1 and the formatting of warning messages aer required in vxfend_A.log.
2203070	[Fencing] Failed to configure fencing on a 64-node cluster, fencing comes up only on first 33 nodes.
2176097	[Fencing] Fencing panics in fp_close() after a considerable time after storage is unavailable.
2161816	[Fencing] 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.
2112742	[VxCPS] Server-based I/O fencing fails to start after configuration on nodes with different locale settings.
2100896	[Fencing] There is failure message even the migration from server-based to disk-based using vxfenswap succeeded.
2085941	[VxCPS] 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.

Table 1-7 LLT, GAB, and I/O fencing fixed issues *(continued)*

Incident	Description
2076240	[VxCPS] 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.
1973713	[Fencing] The agent XML files are missing for CP server agent.
1863916	[Fencing] Cannot change the VxFEN tunable parameters due to a software limitation.

Bundled agents fixed issues

Table 1-8 lists the fixed issues for bundled agents.

Table 1-8 Bundled agents fixed issues

Incident	Description
1923877	Agents which use `hanotify` should have corresponding entries in vcs.mib and vcs_trapd files.
2198632	When we try to offline service groups configured with WPAR, sometimes it does not go to OFFLINE state and remains in UNABLE TO OFFLINE state.
2220640	Application agent clean script fails to work when using PidFiles due to bad use of array
2246528	Error messages from hawparsetup.pl should go to stderr and not stdout
2380925	Two IPMultiNICB resources are online which are configured over the same MutiNICB resource. During the offline of one of the IPMultiNICB resource, the default route is deleted.
2476899	In an AIX WPAR environment, if you configure a resource for physical-to-virtual (P2V) failover on a VCS node, the configured resource may fail to come online. The affected agents include: Application, IP, IPMultiNICB, Mount.
2518610	The WPAR entry points (online, offline, and clean) do not log any message on failure of the commands.

Table 1-8 Bundled agents fixed issues *(continued)*

Incident	Description
2553550	Offline monitoring for Process Agent on a node where Enabled =2 should show Global under Container tab.
2282170	LVMVG agent does not sync correctly even with SyncODM option.
2212600	While using phantom resource in NFS configuration, Phantom resource arbitrarily goes into FAULTED state.
1539927	Dependent resources ArgListValues are not populated correctly when Target resource is deleted and then re-added.
2255688	DNS agent should not send update request if Resource Record is already present in DNS server.
2255772	DNS resource should come online on AutoStart node after a cluster restart.
2593176	The Online entry point of DiskGroup agent should look for correct return code from vxdg import command in case of serial split brain.
2371672	Setting the IMF mode to 2 for DB2 agent since only PRON monitoring is supported. Currently, the mode is set to 3.
2379649	Apache agent to support non default binary name (httpd2) as well as "httpd" binary.
2489758	Apache agent is not able to online the resource if user shell is csh and env file attribute is configured.
2514438	Add support in Apache agent for the benchmarking tool "ab2" as well as "ab".
2416960	For VCS 5.1SP1 or later, if you do not set the value of the CleanProgram attribute, then the Application agent uses the StopProgram attribute to clean a resource during a clean entry point. This behavior may invalidate your agent configuration.
2258553	Manually imported disk groups which are unfenced remain online in VCS without any action or message even if the cluster is configured with "UseFence = SCSI3".
2423977	Application Agent is not working properly when a nonexistent user is configured.

Table 1-8 Bundled agents fixed issues *(continued)*

Incident	Description
2415454	Monitor entry point of Application agent should report OFFLINE when MonitorProgram is not present, but it should report UNKNOWN if it is present but not executable.
2436656	When the Netmask configured on the interface of IP agent is changed outside VCS control, VCS should show a warning message.
2324342	In GCO environment, failover of DNS resource causes duplicate Resource Records in DNS server.
2393939	Correct Apache agent version parsing to accommodate IBM HTTP server 7.0.
2406655	The propcv action entry shows error messages in engine log if Application resource monitoring type is PID files/MonitorProgram.

VCS engine fixed issues

Table 1-9 lists the fixed issues for VCS engine.

Table 1-9 VCS engine fixed issues

Incident	Description
1948444	If cluster address attribute is modified to NULL, then an invalid IP address message is displayed.
2085292	SFSYBASECE: Provide resstatechange script for ase and vxfend dependency issue.
2173455	hares -wait command for IState does not work.
2182462	VCS_GAB_TIMEOUT is restricted to take values between 30,000 ms to 300,000 ms.
2194478	HAD dumps core while overriding the ExternalStateChange attribute at resource level.
2195609	The Simulator core dumps when the systems are switching to running state for simulator.

Table 1-9 VCS engine fixed issues *(continued)*

Incident	Description
2210718	If a non-critical resource faults while group is going online, the state of the VCS service group remains in STARTING|PARTIAL.
2244182	hacf -verify command shows a syntax error when main.cf file is empty.
2252099	For VCS, Parallel "non-local" parent groups are not getting autostarted.
2276242	If an online command for a parallel SG is executed using -any flag in some scenarios then the command fails.
2285716	Service groups fail to restart if they have a mix of persistent and non-persistent resources in the FAULTED state.
2296173	Failover Policy does not take into consideration AutoFailover = 2 and SystemZones when the nodes within a SystemZone are brought down or rebooted.
2330981	No notifications about resources should be sent to agents running on nodes already existing in SystemList of service group, when a node is added or deleted to SystemList.
2345879	VCS should not add 1 to computed value of fencing weight.
2371786	ContainerInfo attribute should be allowed to be updated even when Group is not completely offline
2398808	The soft limit for file descriptors is not specified in vcsenv file.
2400234	The resource state remains "OFFLINE|UNABLE TO OFFLINE" for the panicked node as seen from other node in the cluster.
2406743	Persistent resource is reported OFFLINE (not FAULTED) when system is added to group using hagrp -modify command.
2411865	If a non-responsive NFS mount is present on the system, the entry point of the agent may get timed out.
2416761	HAD consumes over 99% CPU time. Multiple ha commands are hung in pollsys().
2477302	Service group did not fail over on node panic.

Table 1-9 VCS engine fixed issues *(continued)*

Incident	Description
2479006	If the engine receives the second offline message for already offline resources while VCS is bringing the resources offline in path of the faulted resource (when PathCount of the group is still positive) engine core dumps.
2482035	HAD stops before VxFEN startup.
2488867	HAD fails to send the acknowledgement message for the resource state change when a service group or a resource is taken offline or failed over to another cluster by VCS.
2519988	No cluster can be started from Simulator Launch Pad using 'start cluster'.
2077414	Mismatch in display of the values of ContainerInfo attribute at group level & resource level .
2198335	Issue with displaying the value of ResourceInfo attribute using the hares -display command.
2204343	Parent service group does not failover in case of "online local firm" dependent child service group having OnOnly resources.
2216914	In concurrency violation when service group is offlined on one node and is flushed, the IntentOnline attribute is incorrectly set to zero.
2220677	RemoteGroup agent crashes when VCSAPI_LOG_LEVEL is set to non zero value.
2341239	Users with group level administrator privileges are not able to execute the operations on the service groups.
2354935	`hacli -cmd` command triggers HAD coredump.
2388052	For whyonlining parameter of PreOnline script, MANUAL corresponds to Manual online whereas FAULT corresponds to both failover and manual switch. However when service group is manually switched, whyonlining parameter of PreOnline script is shown as MANUAL.
2197899	Child service group which is locally dependent should always have all the systems in the systemlist as that of the parent service group.

Table 1-9 VCS engine fixed issues *(continued)*

Incident	Description
2202616	Sometimes when a node reboots the IntentOnline attribute of the service group is set to 2 even if the service group is online elsewhere. This later causes the service group to consider the AutoStartList attribute.
2486414	GAB errors are logged while running a single node or standalone VCS cluster when GAB is disabled.
2521535	`hares -modify -delete` command for invalid key returns with code zero.
2558997	When a system faults, the CurrentLimits attribute does not get correctly updated on the systems in the cluster.
2292481	VRTSvcs pre-uninstall script detects the wrong HAD process.
2434953	Remove dependency of VRTSvcs package on VRTSgab package.
2527123	Remove static linking of liblltdb Library.
2399895	`hagrp -switch` command fails for child service group if two or more parent service groups are online on alternate systems in the cluster.
2205747	The default name of theVCS service was changed from vcs to vcs-app.
2329486	The whyonlining paramater of preonline trigger needs to be set to SYSFAULT.

Installation related fixed issues

Table 1-10 Installation related fixed issues

Incident	Description
2494592	The /opt/VRTSvcs/bin/vcsenv file is overwritten when installing VRTSvcs package.
2563177	While uninstalling VRTSvxfen package, some failure messages appear.
2168712	Uninstallation of VRTSvcs fails, if CmdServer is running.

Table 1-10 Installation related fixed issues *(continued)*

Incident	Description
2556797	VCS Simulator does not get listed under Program File even after successful installation.

Enterprise agents fixed issues

Table 1-11 lists the fixed issues for enterprise agents.

Table 1-11 Enterprise agents fixed issues

Incident	Description
2124793	Provide additional options for StartUpOpt attribute of ASMInst resource.
2202513	Add support for Timeout option during shutdown of Sybase dataserver.
2203201	VCS Cluster Manager (Java Console) does not encrypt Sybase and SybaseBK agent passwords.
2234530	After bringing the DB2 service group online, the DB2 agent fails to register db2sysc process for PRON monitoring with IMF.
2271885	MonitorMethod attribute of Netlsnr resource does not reflect IMF value without setting Listener attribute.
2336496	DB2 Agent updates the switch-name in db2nodes.cfg for a specific partition which is not correct. The switch-name should be updated for a host.
2343816	Add support for Policy Managed database environment of Oracle 11gR2.
2348684	Add PRON support for DB2 with IMF in MPP and NON-MPP mode.
2392688	Provide SRVCTL READ ONLY option to start database in read only mode for Oracle agent.
2403770	Sybase agent scripts are setting incorrect path for cat command.
2407334	clean script of Sybase agent selects incorrect IPC object types for removal.
2480890	After enabling the WaitForRecovery attribute of the Sybase agent, the recovery state is incorrectly shown as unknown.

Table 1-11 Enterprise agents fixed issues *(continued)*

Incident	Description
2533320	Oracle resource configured inside the container should go in offline state when the container is in DOWN state.
2554938	Setting the IMF mode to 2 for DB2 Agent since only PRON monitoring is supported. Currently the mode is set to 3.
2530402	IMF offline registration is not proper when oracle and listener resources are configured inside container when container is offline.

Agent framework fixed issues

Table 1-12 lists the fixed issues for agent framework.

Table 1-12 Agent framework fixed issues

Incident	Description
1846015	If you configure a resource that has more than 425 values in its ArgListValues, the agent managing that resource logs a warning message.

Fixed issues related to AMF driver

Table 1-13 AMF kernel fixed issues

Incident	Description
2507061	In amfstat output, the value of argv0 flag gets corrupted while getting copied out from the AMF driver.
2392390	If we unconfigure AMF outside VCS control, continuous error messages are displayed in the log: "Failed to open [/dev/amf]: No such device"
2386280	AMF: Updated Module version from 1.0 to 2.0
2331206	IMF not registering db2 process inside WPAR.
2328381	amfext relies on a system environment variable ODMDIR to be defined.
2323310	The process based agents are sometimes allowed to register online process for offline monitoring with AMF.
2322014	After a forceful unload of AMF module, the VXFS file system fails to get unloaded.

Table 1-13 AMF kernel fixed issues *(continued)*

Incident	Description
2301725	In a rare case, when a system call enters into AMF driver at the same time when the AMF driver is getting unconfigured, the node panicks.
2255535	If Mount Agent uses IMF to monitor mounts of type VxFS, then you cannot unload AMF driver as long as Mount Agent is running.
2238441	imf_register entry point (PRON) incorrectly detects "db2sysc" process.
2213447	The `amfregister` command returns unwanted message while unregistering Reaper in special case.
2165304	In imf_register entry point, the values read from amfregister.xml should be flushed after each registration.
2145014	If the user unregisters an event from AMF outside VCS control, VCS will not get any state change notifications from AMFfor that event.
2478322	The man pages are displayed after you generate the catman pages using the `nroff` command. The AMF packaging scripts did not generate thecatman pages.

Veritas Cluster Server: Issues fixed in 5.1 SP1 RP1

This section describes the incidents that are fixed in Veritas Cluster Server in 5.1SP1RP1 release.

Table 1-14 Veritas Cluster Server 5.1 SP1 RP1 fixed issues

Fixed Issues	Description
1999058	RVGSnapshot: DR Fire Drills support Oracle RAC environments using VVR.
2011536	Db2 IMF Integration for NON MPP PRON).
2179652	The monitor script of Db2udb do not handle the case when a parameter is undefined, which make an empty value being passed to next level.
2180721	IPMultiNICB: haipswitch does not support AIX version 6.
2180759	Add WorkLoad attribute to WPAR.xml.
2184205	Parent service group does not failover in case of online local firm dependency with child service group.
2185494	Panic issue related to fp_close().

Table 1-14 Veritas Cluster Server 5.1 SP1 RP1 fixed issues *(continued)*

Fixed Issues	Description
2194473	HAD dumping core while overriding the static attribute to resource level.
2205556	DNS Agent: The offline EP does not remove all A/AAAA records if OffDelRR=1 for Multi-home records
2205563	DNS Agent: Clean EP does not remove any resource records for OffDelRR=1.
2205567	DNS Agent: master.vfd fails to query dns server
2209337	RemoteGroup agent crashes if VCSAPI log level is set to non zero value.
2210489	cfs.noise.n1 test hit the assert "xtpw_inactive_free:1c xtpw_free is empty!"
2214539	When node reboots sometimes the intentonline of group is set to 2 even if group is online elsewhere. This later causes group to consider autostartlist and not doing failover.
2218556	cpsadm should not fail if llt is not installed/configured on a single node cluster.
2218565	MonitorTimeStats incorrectly showing 303 secs Intermittently.
2219955	Split-brain occurs even when using VCS Steward.
2220317	Application agent clean script fails to work when using PidFiles due to bad use of array.
2221618	Fixed an issue where Cluster Manager (Java Console) was not encrypting the "DBAPword" attribute of Oracle Agent.
2223135	nfs_sg fail when execute hastop -all.
2238968	LLT: disable the fastpath in LLT and make it optional.
2241419	halogin does not work in secure environment where Root broker is not VCS node.
2244148	Fixed an issue with Netlsnr agent where not specifying the container name would result into core dump if debug logs were enabled.

Veritas Cluster Server: Issues fixed in 5.1 SP1 RP2

Table 1-15 describes the incidents that are fixed in Veritas Cluster Server in 5.1 SP1 RP2.

Table 1-15 Veritas Cluster Server 5.1 SP1 RP2 fixed issues

Fixed Issues	Description
2518609	Clean EP of WPAR does not stop the WPAR
2516926	Changes to Application agent to support physical to virtual failover.
2516856	Changes to Mount agent to support physical to virtual failover.
2512840	Changes to Oracle, Netlsnr and ASMInst agents to support physical to virtual failover.
2511385	Sybase online script should honor RECOVERY state of the database.
2508637	system got crashed when uninstall GAB package.
2483044	Changes to VCS engine to skip state update requests when resource is already in that state
2481086	LLT: Improve LLT-over-UDP performance
2477372	LLT: reduce "lltd" CPU consumption by reducing the wakeup calls
2477305	Changes to WPAR agent to support physical to virtual failover
2477296	Application service group did not fail over on node panic
2477280	Application resource is not failover when system reboot after Concurrency Violation
2476901	Changes to IP agent to support physical to virtual failover.
2439895	LLT: lltconfig reports its own cluster node as part of duplicate cluster
2439772	WAC resource offline failed after network interruption
2438261	Failed to perform online migration from scsi raw to scsi dmp policy.
2435596	NFS resource failed to come online with NFSv4 on AIX, because of local domain not set on machine.
2434782	ContainerInfo should be allowed to be set for group that is already online.
2426663	On OCPR from customized mode to scsi3 mode, vxfend does not terminate
2426572	Changes to VCS engine to reports a persistent resource as FAULTED when a system is added to group using hagrp -modify command.
2423990	Changes to Application agent to handle non-existent user

Table 1-15 Veritas Cluster Server 5.1 SP1 RP2 fixed issues *(continued)*

Fixed Issues	Description
2416842	Changes to VCS engine to gracefully handle the case when the file descriptor limit is exhausted.
2411860	Agent entry points time out due to non-responsive NFS mount
2411653	GAB: Add check for MAX message size in GAB
2407755	Changes to the agent framework to avoid memory allocation between fork and exec system calls.
2406748	Changes to AMF module to prevent registration of already online process for offline monitor with AMF.
2405391	LLT: The arp ack packet should include the nodename of the node
2403851	AMF status is showing Module loaded but not configured.
2403782	Sybase agent should use perl file I/O for password file specified in SApswd attribute with "VCSSY:" key.
2403633	ContainerInfo attribute should be allowed to be updated even when Group is not completely offline
2400485	Once vxfenconfig -c with mode A has returned EFAULT ("1036 Unable to configure..."), all subsequent runs of vxfenconfig -c with mode B fail with error EBADMSG ("1050 Mismatched modes...")
2400330	whyonlining does not behave as advertised in VCS 5.1SP1
2399898	hagrp -switch of child group fails if 2 or more parent groups online on alternate node
2399658	System panicked while executing the installrp to update RP1.
2398807	VCS should set a soft limit for file descriptors in /opt/VRTSvcs/bin/vcsenv
2394176	vxfenswap process hangs, "ps -ef" shows "vxfenconfig -o modify" on one node but not on other. "vxfenswap -a cancel" kills the stuck operation.
2386326	cannot configure fencing, vxfenadm prints same Serial Number for all LUNs which have more than 96 bytes of SCSI Inquiry data in page 0x83
2382583	CP Agent doesn't show coordination point information in engine log when CP server is not accessible.
2382582	Vxfen tunable resetting when node comes up after panic.

Table 1-15 Veritas Cluster Server 5.1 SP1 RP2 fixed issues *(continued)*

Fixed Issues	Description
2382575	Cannot modify VxFEN tunable parameters
2382559	Online Migration fails with the message I/O fencing does not appear to be configured on node.
2382493	Parent service group does not failover in case of online local firm dependency with child service group.
2382460	Configuring fencing is successful with 3 disks even when single_cp=1 and formatting of warning messages required in vxfend_A.logo
2382452	Syntax errors while unconfiguring CP server using configure_cps.pl scripto.
2382335	vxfentsthdw fails to choose the same fencing disk on two nodes.
2380922	The default route gets deleted when two IPMultiNICB resources are configured for a given network and one resource is brought offline.
2377788	IPMultiNICB agent dumps core when configured for IPv6
2367721	The owner.vfd virtual fire drill check of Oracle agent should only match the uid and gid from the id command output.
2366201	Allow Fencing to start when a majority of the coordination points are available.
2354932	hacli -cmd' triggers had coredump
2330980	When a node is added or deleted from the Group's SystemList, notifications about resources should be sent to agents running only on the added or deleted systems.
2330045	RemoteGroup resource does not go offline when network fails
2330041	VCS group dependencies do not online parallel parent group after upgrading SF 5.0MP3 RP2 to SF5.1SP1.
2318334	Oracle agent should set $Oracle_home/lib library to be first in LD_LIBRARY_PATH
2301731	Panic in amf_lock() due to bad mutex during system shutdown.
2296172	Failover Policy does not take into consideration AutoFailover = 2 and SystemZones when the nodes within a SystemZone are brought down or rebooted.

Table 1-15 Veritas Cluster Server 5.1 SP1 RP2 fixed issues *(continued)*

Fixed Issues	Description
2276622	Cannot configure SCSI-3 fencing using RamSan DMP devices.
2271882	MonitorMethod attribute does not reflect IMF value without setting Listener attribute on Netlsnr Resource
2253349	When netmask changed outside VCS, VCS should show a warning message
2393939	Enhanced Apache agent version parsing to accommodate IBM HTTP server 7.0.

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 92.

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.

Recovery and rollback to original configuration may not succeed if the system reboots while the online migration setup is in partial state (2611423)

During online migration from LVM to VxVM volumes, if there is a system reboot when the migration setup is in partial state, that is, the start operation has not completed successfully, then the recover and abort operations might not be able to recover and rollback the configuration.

Workaround: This needs manual intervention for cleanup, depending on the state, to restore the original configuration.

Issues related to installation

This section describes the known issues during installation and upgrade.

Stopping the installer during an upgrade and then resuming the upgrade might freeze the service groups (2591399)

The service groups freeze due to upgrading using the product installer if you stopped the installer after the installer already stopped some of the processes and then resumed the upgrade.

Workaround: You must unfreeze the service groups manually after the upgrade completes.

To unfreeze the service groups manually

1 List all the frozen service groups

```
# hagrp -list Frozen=1
```

2 Unfreeze all the frozen service groups:

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

Manual upgrade of VRTSvlic fileset loses keyless product levels [2115662]

If you upgrade the `VRTSvlic` fileset 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 fileset.

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 fileset.

   ```
   # installp -u VRTSvlic
   ```

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

   ```
   # installp -acgX -d pathname VRTSvlic
   ```

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 higher versions of VCS, 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 are using keyless licenses before upgrading to 5.1SP1 or higher versions of VCS. 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]
```

Secure WAC communication needs to be disabled explicitly [2392568]

If you have WACs communicating securely where VCS is configured in secure mode and if you disable the VCS security, the WAC where VCS security is disabled

continues attempting to communicate securely without success. Therefore, you need to explicitly disable WAC security when you disable VCS security.

Workaround: No workaround. Secure WAC communication needs to be disabled explicitly.

Web installer has no option to remove node from a cluster

Web Installer does not provide the option to remove node from a cluster.

Workaround: Manually remove nodes from a cluster. There is no option to remove nodes available from Web Installer or CPI.

Web installer does not ask for authentication for the same URL after the first session if the browser is still open [2509330]

If you have closed the web installer window after either installing or configuring VCS and you have other windows of the same browser open, the web installer does not ask for authentication in the subsequent sessions. Since there is no option to gracefully log out of the web installer, its session remains open as long as the browser is used by the web installer is open on the system.

However, This issue is URL-specific and is observed only when you use the same URL to perform the subsequent operations. Therefore, if you use different URLs for your purpose, the browser prompts for authentication each time you access the web installer.

Workaround: You can use different URL to access the web installer.

Perl messages seen in engine log during rolling upgrade [2627360]

While performing a rolling upgrade from VCS 5.2SP1 to 6.0 with MultiNICA resource configured, if VRTSperl fileset is upgraded but VRTSvcsag fileset is not yet upgraded on the system, Perl code related messages may be seen. The messages seen are similar to the following:

```
Using a hash as a reference is deprecated at MultiNICA.pm line 108.
```

Workaround: No workaround.

sfmh discovery issue when you upgrade your Veritas product to 6.0 (2622987)

If a host is not reporting to VOM but sfmh discovery is running before you upgrade to 6.0, sfmh-discovery may fail to start after the upgrade.

Workaround:

If the host is not reporting to VOM, stop sfmh-discovery manually before upgrade to 6.0.

Incorrect server names sometimes display if there is a clock synchronization issue (2627076)

When you install a cluster with the Web-based installer, you choose to to synchronize your systems with an NTP server due to a clock synchronization issue, you may see the NTP server name in messages instead of your server names.

Workaround:

Ignore the messages. The product is still installed on the correct servers.

Operational issues for VCS

Connecting to the database outside VCS control using sqlplus takes too long to respond

Connecting to start the database outside VCS control, using sqlplus takes more than 10 minutes to respond after pulling the public network cable. [704069]

Some VCS components do not work on the systems where a firewall is configured to block TCP traffic

The following issues may occur if you install and configure VCS on systems where a firewall is installed:

- If you set up Disaster Recovery using the Global Cluster Option (GCO), the status of the remote cluster (cluster at the secondary site) shows as "initing".
- If you configure fencing to use CP server, fencing client fails to register with the CP server.
- Setting up trust relationships between servers fails.

Workaround:

- Ensure that the required ports and services are not blocked by the firewall. Refer to the *Veritas Cluster Server Installation Guide* for the list of ports and services used by VCS.
- Configure the firewall policy such that the TCP ports required by VCS are not blocked. Refer to your respective firewall or OS vendor documents for the required configuration.

Issues related to the VCS engine

Extremely high CPU utilization may cause HAD to fail to heartbeat to GAB

When CPU utilization is very close to 100%, HAD may fail to heartbeat to GAB. [1818687]

The hacf -cmdtocf command generates a broken main.cf file

The `hacf -cmdtocf` command used with the `-dest` option removes the include statements from the types files. [1728738]

Workaround: Add include statements in the main.cf files that are generated using the `hacf -cmdtocf` command.

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.

VCS fails to validate processor ID while performing CPU Binding [2441022]

If you specify an invalid processor number when you try to bind HAD to a processor on a remote system, HAD does not bind to any CPU. However, the command displays no error to indicate that the specified CPU does not exist. The error is logged on the node where the binding has failed and the values are reverted to default.

Workaround: Symantec recommends that you modify CPUBinding from the local system.

Trigger does not get executed when there is more than one leading or trailing slash in the triggerpath [2368061]

The path specified in TriggerPath attribute must not contain more than one leading or trailing '\' character.

Workaround: Remove the extra leading or trailing '\' characters from the path.

Service group is not auto started on the node having incorrect value of EngineRestarted [2397532]

When HAD is restarted by `hashadow` process, the value of EngineRestarted attribute is temporarily set to 1 till all service groups are probed. Once all service groups are probed, the value is reset. If HAD on another node is started at roughly the same time, then it is possible that it does not reset the value of EngineRestarted attribute. Therefore, service group is not auto started on the new node due to mismatch in the value of EngineRestarted attribute.

Workaround: Restart VCS on the node where EngineRestarted is set to 1.

Group is not brought online if top level resource is disabled [2486476]

If the top level resource which does not have any dependancy is disabled then the other resources do not come online and the following message is displayed:

```
VCS NOTICE V-16-1-50036 There are no enabled
 resources in the group cvm to online
```

Workaround: Online the child resources of the topmost resource which is disabled.

NFS resource goes offline unexpectedly and reports errors when restarted [2490404]

VCS does not perform resource operations, such that if an agent process is restarted multiple times by HAD, only one of the agent process is valid and the remaining processes get aborted, without exiting or being stopped externally. Even though the agent process is running, HAD does not recognize it and hence does not perform any resource operations.

Workaround: Forcefully stop the agent process.

Parent group does not come online on a node where child group is online [2489053]

This happens if the AutostartList of parent group does not contain the node entry where the child group is online.

Workaround: Bring the parent group online by specifying the name of the system then use the `hargp -online [parent group] -any` command to bring the parent group online.

Cannot modify temp attribute when VCS is in LEAVING state [2407850]

An `ha` command to modify a temp attribute is rejected if the local node is in a LEAVING state.

Workaround: Execute the command from another node or make the configuration read-write enabled.

If secure and non-secure WAC are connected the engine_A.log receives logs every 5 seconds [1539646]

Two WACs in GCO must always be started either in secure or non-secure mode. The secure and non-secure WAC connections cause log messages to be sent to engine_A.log file.

Workaround: Make sure that WAC is running in either secure mode or non-secure mode on both the clusters in GCO.

Oracle group fails to come online if Fire Drill group is online on secondary cluster [2556835]

If a parallel global service group faults on the local cluster and does not find a failover target in the local cluster, it tries to failover the service group to the remote cluster. However, if the firedrill for the service group is online on a remote cluster, offline local dependency is violated and the global service group is not able to failover to the remote cluster.

Workaround: Offline the Firedrill service group and online the service group on a remote cluster.

POSTONLINE and POSTOFFLINE triggers are not enabled by default [2567387]

Before VCS 6.0, POSTONLINE and POSTOFFLINE triggers were enabled by default, so the triggers got executed whenever a service group came online. In VCS 6.0, you must explicitly enable the POSTONLINE and POSTOFFLINE triggers whenever you upgrade to VCS 6.0.

Alternatively, if you want the triggers to execute after the upgrade:

1. Before upgrade, set vcs_start = 0 in /etc/default/vcs

   so that HAD does not start after the upgrade.
2. Upgrade the existing VCS to VCS 6.0.
3. Set vcs_start = 1 in /etc/default/vcs

4 Start VCS on each node using `hastart`.

5 Set TriggersEnabled in main.cf for required groups as ollows:

```
TriggersEnabled @<systemname>={POSTONLINE, POSTOFFLINE}
```

Example of trigger behavior:

```
group scriptfileonoff (
        SystemList = { vcssx235 = 0, vcssx236 = 1 }
        AutoStartList = { vcssx235, vcssx236 }
        TriggersEnabled @vcssx235 = { POSTONLINE }
        )
        MyFileOnOff MFileOnOff (
                PathName = "/tmp/mf1"
                )
        MyFileOnOff MFileOnOff1 (
                PathName = "/tmp/mf2"
```

Two CmdServer instances seen running on a node [2399292]

You may see two instances of CmdServer running on a node. One of these using IPv4 and the other IPv6.

This does not impact functionality in any way.

Workaround: No workaround.

Service group may fail to come online after a flush and a force flush operation [2616779]

A service group may fail to come online after flush and force flush operations are executed on a service group where offline operation was not successful.

Workaround: If the offline operation is not successful then use the force flush commands instead of the normal flush operation. If a normal flush operation is already executed then to start the service group use `-any` option.

Issues related to the bundled agents

VCS resources may time out if NFS server is down [2129617]

The VCS resources may time out if the server NFS mounted file system and the NFS server is down or inaccessible. This behavior is exclusive to AIX platform.

Workaround: You must unmount the NFS mounted file system to restore the cluster to sane condition.

MultiNICB resource may show unexpected behavior with IPv6 protocol [2535952]

When using IPv6 protocol, set the LinkTestRatio attribute to 0. If you set the attribute to another value, the MultiNICB resource may show unexpected behavior.

Workaround: Set the LinkTestRatio attribute to 0.

Application agent cannot handle a case with user as root, envfile set and shell as csh [2584285]

Application agent does not handle a case when the user is root, envfile is set, and shell is csh. The application agent uses the `system` command to execute the `Start`/`Stop`/`Monitor`/`Clean` Programs for the root user. This executes `Start`/`Stop`/`Monitor`/`Clean` Programs in `sh` shell, due to which there is an error when root user has csh shell and EnvFile is written accordingly.

Workaround: Do not set `csh` as shell for root user. Use `sh` as shell for root instead.

IMF registration fails for Mount resource if the configured MountPoint path contains spaces [2442598]

If the configured MountPoint of a Mount resource contains spaces in its path, then the Mount agent can online the resource correctly, but the IMF registration for ONLINE monitoring fails. This is due to the fact that the AMF driver does not support spaces in the path. Leading and trailing spaces are handled by the Agent and IMF monitoring can be done for such resources.

Workaround: Symantec recommends to turn off the IMF monitoring for a resource having spaces in its path. For information on disabling the IMF monitoring for a resource, refer to Veritas Cluster Server Administrator's Guide.

Bringing the LPAR resource offline may fail [2418615]

Bringing the LPAR resource offline may fail with the following message in the engine_A.log file.

```
<Date Time> VCS WARNING V-16-10011-22003 <system_name>
LPAR:<system_name>:offline:Command failed to run on MC
<hmc_name> with error HSCL0DB4 An Operating System
Shutdown can not be performed because the operating system image
running does not support remote execution of this task from the HMC.
```

```
This may be due to problem in communication with
MC <hmc_name>
```

This is due to RMC failure between HMC and management LPAR. Since the LPAR could not be shutdown gracefully in offline, the LPAR is shutdown forcefully in the clean call, hence it shows as Faulted.

Workaround: In order to recycle the RSCT deamon for LPAR and HMC, refer the *Veritas Storage Foundation™ and High Availability Solutions Virtualization Guide*.

LPAR agent may not show the correct state of LPARs [2418615, 2425990]

When the Virtual I/O server (VIOS) gets restarted, LPAR agent may not get the correct state of the resource. In this case, the LPAR agent may not show the correct state of the LPAR.

Workaround: Restart the management LPAR and all the managed LPARs that depend on the VIOS.

RemoteGroup agent does not failover in case of network cable pull [2588807]

A RemoteGroup resource with ControlMode set to OnOff may not fail over to another node in the cluster in case of network cable pull. The state of the RemoteGroup resource becomes UNKNOWN if it is unable to connect to a remote cluster.

Workaround:

- Connect to the remote cluster and try taking offline the RemoteGroup resource.
- If connection to the remote cluster is not possible and you want to bring down the local service group, change the ControlMode option of the RemoteGroup resource to MonitorOnly. Then try taking offline the RemoteGroup resource. Once the resource is offline, change the ControlMode option of the resource to OnOff.

Concurrency violation in the service group [2555306]

Concurrency violation and data corruption of a Volume resource may occur, if storage connectivity is lost or all paths under VxDMP are disabled and PanicSystemOnDGLoss is set to 0

This happens when:

- In a cluster environment/configuration, if cluster wide UseFence attribute is set to SCSI3 and service group contains Volume resource and DiskGroup resource with the PanicSystemOnDGLoss attribute set to 0 (zero).
- If storage connectivity is lost or all paths under VxDMP are disabled, VCS fails over the service group. If storage connectivity is restored on the node on which the service group was faulted and DG is not deported manually, then volume may get started if disk group is not deported during the service group failover. So volume resource shows state as online on both the nodes and thus cause concurrency violation. This may lead to data corruption.

Workaround: Ensure that the disk group is deported soon after storage connectivity is restored.

You are recommended to always configure Volume resource whenever Disk group resources is configured and set the attribute PanicSystemOnDGLoss to 1 or 2 as per requirement.

Coordpoint agent remains in faulted state [2555191]

The Coordpoint agent remains in faulted state because it detects `rfsm` to be in replaying state.

Workaround: Clear the fault and reconfigure fencing.

Prevention of Concurrency Violation (PCV) is not supported for applications running in a container [2536037]

For an application running in a container, VCS uses a similar functionality if that resource is not registered to IMF. Hence, there is no IMF control to take a resource offline. When the same resource goes online on multiple nodes, agent detects and reports to engine. Engine uses the offline monitor to take the resource offline. Hence, even though there is a time lag before the detection of the same resource coming online on multiple nodes at the same time, VCS takes the resource offline.

PCV does not function for an application running inside a WPAR on AIX.

Workaround: No workaround.

No IPv6 support for NFS [2022174]

IPv6 is not supported for NFS.

Workaround: No workaround.

MemCPUAllocator agent fails to come online if DLPAR name and hostname do not match [2407671]

If hostname of the DLPAR and name of DLPAR as seen from HMC are different, the MemCPUAllocator agent is unable to provide CPU or memory to the DLPAR.

Workaround: Change the name of DLPAR from HMC to match the hostname.

VCS does not monitor applications inside an already existing WPAR [2494532]

If a WPAR is already present on the system at the time of VCS installation, and this WPAR or an application running inside this WPAR needs to be monitored using VCS, then VCS does not monitor the application running in that WPAR. This is because the VCS packages/files are not visible inside that WPAR.

Workaround: Run `syncwpar` command for that WPAR. This makes the VCS packages/files visible inside the WPAR and VCS can then monitor the applications running inside the WPAR.

HA commands inside WPAR agent get stuck due to the login/password prompt [2431884]

After upgrade of secure clusters from VCS versions lower than VCS 6.0, the HA commands that run from within the WPAR display login/password prompts. Hence, agents trying to run HA commands inside WPAR get stuck because of the prompt, as the WPAR credentials are not upgraded because of change of architecture of VxAT in VCS 6.0.

Wrorkaround: Run `hawaparsetup.pl` again for each WPAR resource. This will create new credentials for the WPAR which can be used by HA commands in VCS 6.0.

The hawparsetup.pl script does not check the service group status [2523171]

If the service group in which WPAR resource needs to be added already exists and is not in OFFLINE state, `hawparsetup.pl` script does not modify the ContainerInfo attribute for the system on which it is not completely OFFLINE.The hawparsetup.pl scrip, therefore it does not check whether the service group passed to it is completely OFFLINE or not if it already exists.

Workaround: The `hawparsetup.pl` script does not check whether the service group passed to it is completely OFFLINE or not if it already exists.

The hawparsetup.pl script does not check the key value in ContainerInfo [2523171]

If ContainerInfo attribute is already set for a service group and the key "Enabled" is set to some value other than 1, running h`hawparsetup.pl` overwrites the value for key "Enabled" to 1. Thus, `hawparsetup.pl` does not check whether the key "Enabled" in attribute "ContainerInfo" has been set or not.

Workaround: Manually set the value of key "Enabled" in attribute "ContainerInfo" to the desired value after running `hawparsetup.pl`.

NFS client reports I/O error because of network split brain [2564517]

When network split brain occurs, the failing node may take some time to panic. Thus, the service group on the failover node may fail to come online, as some of the resources (like IP resource) are still online on the failing node or disk group on the failing node may get disabled but IP resource on the same node continues to be online.

Workaround: Configure the preonline trigger for the service group containing DiskGroup resouce on each system in the service group:

1 Copy the preonline_ipc trigger from `/opt/VRTSvcs/bin/sample_triggers/VRTSvcs` to `/opt/VRTSvcs/bin/triggers/preonline/` as T0preonline_ipc.

```
# cp /opt/VRTSvcs/bin/sample_triggers/VRTSvcs/preonline_ipc
 /opt/VRTSvcs/bin/triggers/preonline/T0preonline_ipc
```

2 Enable PREONLINE trigger for the service group.

```
# hagrp –modify <group_name> TriggersEnabled PREONLINE
 –sys <node_name>
```

Some agents may fail to come online after full upgrade to VCS 6.0 if they were online before the upgrade [2618482]

Resources of type NFSRestart and DNS do not come online automatically after a full upgrade to VCS 6.0 if they were previously online

Workaround: Online the resources manually after the upgrade, if they were online previously.

Coexistence of Live Partition Mobility (LPM) and VCS failover of managed LPAR

Coexistence of LPM and VCS failover of manged LPAR may cause an issue. If you plan to do LPM on a managed LPAR, make sure you see the *Live partition mobility of managed LPARs* section in *Veritas Storage Foundation and High Availability Solutions Virtualization Guide* for AIX for the correct information.

Error messages for wrong HMC user and HMC name do not communicate the correct problem

The wrong HMC user and wrong HMC name errorsd are not reflective of the correct problem. If you see the following errors in engine_A.log for LPAR resource, it means wrong HMC user:

```
Permission denied, please try again
Permission denied, please try again
```

If you see the following errors in engine_A.log for LPAR resource, it means wrong HMC name:

```
ssh: abc: Hostname and service name
not provided or found.
```

You must see the applicationha_utils.log file to confirm the same.

Issues related to the VCS database agents

Health check monitoring does not work with VCS agent for Oracle [2101570, 1985055]

The health check monitoring in Oracle agent for VCS does not work due to incompatibility of the health check APIs provided by Oracle.

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

Intentional Offline does not work for VCS agent for Oracle [1805719]

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

Make sure that the ohasd has an entry in the init scripts [1985093]

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.

Workaround: Respawn off the `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.

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.

NOFAILOVER action specified for certain Oracle errors

The Veritas High Availability agent for Oracle provides enhanced handling of Oracle errors encountered during detailed monitoring. The agent uses the reference file oraerror.dat, which consists of a list of Oracle errors and the actions to be taken.

See the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide* for a description of the actions.

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

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

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

ASM instance does not unmount VxVM volumes after ASMDG resource is offline

In configurations where ASMInstance resource is part of a separate parallel service group, the ASM instance does not unmount the volumes even after the ASMDG resource is taken offline. Therefore, the Volume resource cannot be taken offline. This issue occurs when you use VxVM volumes as ASM disk groups. [918022]

Workaround: Configure the ASMInstance resource as part of the failover service group where ASMDG resource is configured.

IMF registration fails if sybase server name is given at the end of the configuration file [2365173]

AMF driver supports a maximum of 80 characters of arguments. In order for AMF to detect the start of the Sybase process, the Sybase server name must occur in the first 80 characters of the arguments.

Workaround: Must have the server name, -sSYBASE_SERVER, as the first line in the configuration file: `ASE-15_0/install/RUN_SYBASE_SERVER`.

Issues related to the agent framework

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 [1511211]

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.

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.

IMF related error messages while bringing a resource online and offline [2553917]

For a resource registered with AMF, if you run `hagrp -offline` or `hagrp -online` explicitly or through a collective process to offline or online the resource respectively, the IMF displays error messages in either case.

The errors displayed is an expected behavior and it does not affect the IMF functionality in any manner.

Workaround: No workaround.

Issues related to global clusters

The engine log file receives too many log messages on the secure site in global cluster environments [1539646]

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.

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 (2107386)

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.

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 may fail to make connections with LLT on peer nodes in virtual environment (2343451/2376822)

After you upgrade from 5.0 MP3 or earlier releases to version 6.0, LLT may fail to make connections with LLT on the peer nodes in AIX virtual environment.

This is a known IBM VIOS issue. Install APAR IV00776 on your VIOS server. Without this fix, VIOS fails to handle new LLT packet header and drops packets.

Workaround: Disable the largesend attribute of the SEA adapter. Check the properties of the SEA adapter (on which the virtual links are configured under LLT maps) on each VIOS using the following command:

```
#lsattr -El SEA
```

If the largesend is set to 1, then set it to 0 using the following command:

```
#chdev -l SEA -a largesend=0
```

LLT port stats sometimes shows recvcnt larger than recvbytes (1788315)

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.

This does not impact the LLT functionality.

LLT may incorrectly declare port-level connection for nodes in large cluster configurations (1809827)

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.

Issues related to GAB

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

While deinitializing GAB client, "gabdebug -R GabTestDriver" command logs refcount value 2 (2536373)

After you unregister the gtx port with `-nodeinit` option, the `gabconfig -C` command shows refcount as 1. But when forceful `deinit` option (`gabdebug -R GabTestDriver`) is run to deinitialize GAB client, then a message similar to the following is logged.

```
GAB INFO V-15-1-20239
Client GabTestDriver with refcount 2 forcibly deinited on user request
```

The `refcount` value is incremented by 1 internally. However, the refcount value is shown as 2 which conflicts with the `gabconfig -C` command output.

Cluster panics during reconfiguration (2590413)

While a cluster is reconfiguring, GAB broadcast protocol encounters a race condition in the sequence request path. This condition occurs in an extremely narrow window which eventually causes the GAB master to panic.

Issues related to I/O fencing

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

CP server repetitively logs unavailable IP addresses (2530864)

If coordination point server (CP server) fails to listen on any of the IP addresses that are mentioned in the `vxcps.conf` file or that are dynamically added using the command line, then CP server logs an error at regular intervals to indicate the failure. The logging continues until the IP address is bound to successfully.

```
CPS ERROR V-97-51-103 Could not create socket for host
10.209.79.60 on port 14250
CPS ERROR V-97-1400-791 Coordination point server could not
open listening port = [10.209.79.60]:14250
Check if port is already in use.
```

Workaround: Remove the offending IP address from the listening IP addresses list using the `rm_port` action of the `cpsadm` command.

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

Fencing port b is visible for few seconds even if cluster nodes have not registered with CP server (2415619)

Even if the cluster nodes have no registration on the CP server and if you provide coordination point server (CP server) information in the `vxfenmode` file of the cluster nodes, and then start fencing, the fencing port b is visible for a few seconds and then disappears.

Workaround: Manually add the cluster nodes' and users' information to the CP server to resolve this issue. Alternatively, you can use installer as the installer adds cluster nodes' and users' information to the CP server during configuration.

The cpsadm command fails if LLT is not configured on the application cluster (2583685)

The cpsadm command fails to communicate with the coordination point server (CP server) if LLT is not configured on the application cluster node where you run the cpsadm command. You may see errors similar to the following:

```
# cpsadm -s 10.209.125.200 -a ping_cps
CPS ERROR V-97-1400-729 Please ensure a valid nodeid using
environment variable
CPS_NODEID
CPS ERROR V-97-1400-777 Client unable to communicate with CPS.
```

However, if you run the cpsadm command on the CP server, this issue does not arise even if LLT is not configured on the node that hosts CP server. The cpsadm command on the CP server node always assumes the LLT node ID as 0 if LLT is not configured.

According to the protocol between the CP server and the application cluster, when you run the cpsadm on an application cluster node, cpsadm needs to send the LLT node ID of the local node to the CP server. But if LLT is unconfigured temporarily, or if the node is a single-node VCS configuration where LLT is not configured, then the cpsadm command cannot retrieve the LLT node ID. In such situations, the cpsadm command fails.

Workaround: Set the value of the CPS_NODEID environment variable to 255. The cpsadm command reads the CPS_NODEID variable and proceeds if the command is unable to get LLT node ID from LLT.

In absence of cluster details in CP server, VxFEN fails with pre-existing split-brain message (2433060)

When you start server-based I/O fencing, the node may not join the cluster and prints error messages in logs similar to the following:

In the /var/VRTSvcs/log/vxfen/vxfen.log file:

```
VXFEN vxfenconfig ERROR V-11-2-1043
Detected a preexisting split brain. Unable to join cluster.
```

In the /var/VRTSvcs/log/vxfen/vxfen.log file:

```
operation failed.
CPS ERROR V-97-1400-446 Un-authorized user cpsclient@galaxy,
domaintype vx; not allowing action
```

The vxfend daemon on the application cluster queries the coordination point server (CP server) to check if the cluster members as seen in the GAB membership are registered with the CP server. If the application cluster fails to contact the CP server due to some reason, then fencing cannot determine the registrations on the CP server and conservatively assumes a pre-existing split-brain.

Workaround: Before you attempt to start VxFEN on the application, ensure that the cluster details such as cluster name, UUID, nodes, and privileges are added to the CP server.

The vxfenswap utility does not detect failure of coordination points validation due to an RSH limitation (2531561)

The `vxfenswap` utility runs the `vxfenconfig -o modify` command over RSH or SSH on each cluster node for validation of coordination points. If you run the `vxfenswap` command using RSH (with the `-n` option), then RSH does not detect the failure of validation of coordination points on a node. From this point, `vxfenswap` proceeds as if the validation was successful on all the nodes. But, it fails at a later stage when it tries to commit the new coordination points to the VxFEN driver. After the failure, it rolls back the entire operation, and exits cleanly with a non-zero error code. If you run `vxfenswap` using SSH (without the `-n` option), then SSH detects the failure of validation of coordination of points correctly and rolls back the entire operation immediately.

Workaround: Use the `vxfenswap` utility with SSH (without the `-n` option).

Fencing does not come up on one of the nodes after a reboot (2573599)

If VxFEN unconfiguration has not finished its processing in the kernel and in the meantime if you attempt to start VxFEN, you may see the following error in the `/var/VRTSvcs/log/vxfen/vxfen.log` file:

```
VXFEN vxfenconfig ERROR V-11-2-1007 Vxfen already configured
```

However, the output of the `gabconfig -a` command does not list port b. The `vxfenadm -d` command displays the following error:

```
VXFEN vxfenadm ERROR V-11-2-1115 Local node is not a member of cluster!
```

Workaround: Start VxFEN again after some time.

The cpsadm command fails after upgrading CP server to 6.0 in secure mode (2478502)

The `cpsadm` command may fail after you upgrade coordination point server (CP server) to 6.0 in secure mode. If the old VRTSat fileset is not removed from the system, the `cpsadm` command loads the old security libraries present on the system. As the installer runs the `cpsadm` command on the CP server to add or upgrade the VCS cluster (application cluster), the installer also fails.

Workaround : Perform the following steps on all the nodes of the CP server:

- Rename cpsadm to cpsadmbin.

  ```
  # mv /opt/VRTScps/bin/cpsadm /opt/VRTScps/bin/cpsadmbin
  ```

- Create a file `/opt/VRTScps/bin/cpsadm` with the following content:

  ```
  #!/bin/sh
  EAT_USE_LIBPATH="/opt/VRTScps/lib"
  export EAT_USE_LIBPATH
  /opt/VRTScps/bin/cpsadmbin "$@"
  ```

- Provide the following permissions to the new file:

  ```
  # chmod 755 /opt/VRTScps/bin/cpsadm
  ```

Server-based fencing comes up incorrectly if default port is not mentioned (2403453)

When you configure fencing in customized mode and do no provide default port, fencing comes up. However, the `vxfenconfig -l` command output does not list the port numbers.

Workaround: Retain the "port=<port_value>" setting in the `/etc/vxfenmode` file, when using customized fencing with atleast one CP server. The default port value is 14250.

Secure CP server does not connect from localhost using 127.0.0.1 as the IP address (2554981)

The `cpsadm` command does not connect to the secure CP server on the localhost using 127.0.0.1 as the IP address

Workaround: Connect the secure CP server using any of the virtual IPs that is configured with the CP server and is plumbed on the local node.

Unable to customize the 30-second duration (2551621)

When the vxcpserv process is not able to bind to an IP address during startup, it attempts to bind to that IP address at an interval of 30 seconds. This interval is not configurable.

Workaround: No workaround.

NIC resource gets created with incorrect name while configuring CPSSG with the configure_cps.pl script (2585229)

The name of the NIC resource created by the `configure_cps.pl` script does not come out correct when, for example, m^{th} VIP is mapped to n^{th} NIC and every m is not equal to n. In this case, although CPSSG continues to function without any problem, when you unconfigure CPSSG using `configure_cps.pl`, it fails.

Workaround: To unconfigure CPSSG, you must remove the CPSSG configuration from the VCS configuration.

Issues related to Intelligent Monitoring Framework (IMF)

Registration error while creating a Firedrill setup [2564350]

While creating the Firedrill setup using the `Firedrill setup` utility, VCS encounters the following error:

```
AMF amfregister ERROR V-292-2-167
Cannot register mount offline event
```

During Firedrill operations, VCS may log error messages related to IMF registration failure in the engine log. This happens because in the firedrill service group, there is a second CFSMount resource monitoring the same MountPoint through IMF. Both the resources try to register for online/offline events on the same MountPoint and as a result, registration of one fails.

Workaround: No workaround.

Pearl errors seen while using haimfconfig command

Pearl errors seen while using `haimfconfig` command:

```
Pearl errors seen while using haimfconfig command
```

This error is due to the absolute path specified in main.cf for type-specific configuration files. Currently, `haimfconfig` does not support absolute path for type-specific configuration file in main.cf.

Wrokaround: Replace the actual path with the actual file name and copy the file from its absolute location to `/etc/VRTSvcs/conf/config` directory.

For example, if OracleTypes.cf is included in main.cf as:

```
include "/etc/VRTSagents/ha/conf/Oracle/OracleTypes.cf"
```

It should be replaced as follows in main.cf:

```
include "OracleTypes.cf"
```

Issues related to the Cluster Manager (Java Console)

This section covers the issues related to the Cluster Manager (Java Console).

Some Cluster Manager features fail to work in a firewall setup [1392406]

In certain environments with firewall configurations between the Cluster Manager and the VCS cluster, the Cluster Manager fails with the following error message:

```
V-16-10-13 Could not create CmdClient. Command Server
may not be running on this system.
```

Workaround: You must open port 14150 on all the cluster nodes.

VCS Cluster Manager (Java Console) does not encrypt Sybase and SybaseBk agent passwords [2379510]

If `isvcsagencrypt` flag is set to True in Sybase.xml and SybaseBk.xml files, the attribute values get encrypted. However, the password attributes of Sybase and SybaseBk agents do not have the `isvcsagentcrypt` flag set to True in Sybase.xml and SybaseBk.xml files.

Workaround: Sybase and SybaseBk agents are modified to encrypt the password by default. As a result, you need not encrypt passwords if you use the VCS Cluster Manager (Java Console) to configure attributes.

Issues related to Virtual Business Services (VBS)

Fault propagation for Virtual Business Services with shared service groups and different controllers [2407832]

Fault propagation may not work for certain configurations having shared service groups and distinct controllers.

Workaround: No workaround.

Virtual Business Services fail to start if a participating service group has multiple children with the LOCAL FIRM dependency type [2490098]

Virtual Business Services fail to start if a participating service group has multiple children with the LOCAL FIRM dependency type. This occurs because Vertias Cluster Server (VCS) does not support propagating dependencies.

Workaround: Pull the dependent VCS groups into the Virtual Business Services without any dependencies. The Virtual Business Services will recognize the VCS dependencies and treat them as soft Virtual Business Services dependencies.

Software limitations

This section covers the software limitations of this release.

See the corresponding Release Notes for a complete list of software limitations related to that component or product.

See "Documentation" on page 92.

Limitations related to installing and upgrading VCS

Upgrades on alternate disk supported only from version 5.1

VCS supports upgrade on an alternate disk only from version 5.1 to version 6.0. If you are running earlier versions of VCS, perform a full or phased upgrade to version 5.1 and then upgrade to version 6.0 using an alternate disk.

Upgrade of secure clusters not supported using native operating system tools

This release does not support the upgrade of secure clusters using native operating system tools such as Alternate Disk Installation (ADI) and Network Install Manager Alternate Disk Migration (NIMADM).

Limitation on upgrading to 6.0 on a Veritas Storage Foundation and High Availability cluster

Veritas Storage Foundation (SF) 6.0 requires the AIX operating system to be at 6.1 TL5 or above. To upgrade SF to 6.0 from a release prior to 5.0 MP3 RP1, you must first upgrade SF to the 5.0 MP3 RP1 release. If upgrading to 5.0 MP3 RP1

requires an intermediate operating system upgrade, the operating system level cannot exceed 6.1 TL1. After upgrading to 5.0 MP3 RP1, you must upgrade the operating system to AIX 6.1 TL5, which is the minimum requirement for the 6.0 release. You must upgrade SF to 5.0 MP3 RP1 to avoid a system panic or crash that can occur when a node running AIX 6.1 TL2 or above with a release prior to 5.0 MP3 RP1 is removed from the Veritas Storage Foundation and High Availability cluster. Removing the node causes file system threads to exit. The panic is caused by a check introduced from AIX 6.1 TL2 that validates the lockcount values when a kernel-thread-call exits.

For more information, see the following TechNote:

http://www.symantec.com/docs/TECH67985

Limitations related to 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 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/netsvc.conf

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 when the disk group is imported, irrespective of the value of the StartVolumes attribute in VCS. This behavior is observed if the value of the system-level attribute `autostartvolumes` in Veritas Volume Manager is set to On.

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.

WPAR agent registered to IMF for Directory Online event

The Directory Online event monitors the Zone root directory. If the parent directory of the Zone root directory is deleted or moved to another location, AMF does not provide notification to the Zone agent. In the next cycle of the zone monitor, it detects the change and reports the state of the resource as offline.

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.

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.

Limitations with DiskGroupSnap agent

The DiskGroupSnap agent has the following limitations:

- The DiskGroupSnap agent does not support layered volumes. [1368385]

- 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.

Virtualizing shared storage using VIO servers and client partitions

In an Advanced POWER™ Virtualization (APV) environment, AIX uses the VIO Server to monitor and manage the I/O paths for the virtualized client partitions. At a very high level, the VIO server provides a partition's access to storage that is external to the physical computer. The VIO server encapsulates the physical hardware into virtual adapters called virtual SCSI adapters (server adapter). On the client side, you can create virtual adapters (client adapters) that map to the server adapter and enable a partition to connect to external storage.

The VIO server provides similar mechanisms to share limited networking resources across partitions. Refer to the manual that came with your system to help set up partitions, and to configure and use the various components such as VIO server and HMC, which are integral parts of IBM's APV environment.

The minimum patch level for using VIO servers with VCS is: version 2.1.3.10-FP-23 and later.

Supported storage

Refer to the IBM data sheet:

http://www14.software.ibm.com/webapp/set2/sas/f/vios/home.html

Disk Restrictions

When using VCS in combination with VIO servers and their client partitions, you need to ensure that no reservations are placed on the shared storage. This enables client partitions on different systems to access and use the same shared storage.

- If the shared storage is under MPIO control, set the reserve_policy attribute of the disk to no_reserve.
- If the shared storage is not under MPIO control, look up the array documentation to locate a similar attribute to set on the disk.

Internal testing on EMC disks shows that this field maps as the reserve_lock attribute for EMC disks. In this case, setting it to no achieves the same result.

Accessing the same LUNs from Client Partitions on different Central Electronics Complex (CEC) modules

This section briefly outlines how to set shared storage so that it is visible from client partitions on different CEC modules.

With the VIO server and client partitions set up and ready, make sure that you have installed the right level of operating system on the client partitions, and that you have mapped the physical adapters to the client partitions to provide access to the external shared storage.

To create a shareable diskgroup, you need to ensure that the different partitions use the same set of disks. A good way to make sure that the disks (that are seen from multiple partitions) are the same is to use the disks serial numbers, which are unique.

Run the following commands on the VIO server (in non-root mode), unless otherwise noted.

Get the serial number of the disk of interest:

```
$ lsdev -dev hdisk20 -vpd
 hdisk20
 U787A.001.DNZ06TT-P1-C6-T1-W500507630308037C-
 L401 0401A00000000  IBM FC 2107

 Manufacturer.............IBM
 Machine Type and Model......2107900
 Serial Number..............7548111101A
 EC Level.....................131
 Device Specific.(Z0).........10
 Device Specific.(Z1).........0100
 …
```

Make sure the other VIO server returns the same serial number. This ensures that you are viewing the same actual physical disk.

List the virtual SCSI adapters.

```
$ lsdev -virtual | grep vhost
 vhost0  Available  Virtual SCSI Server Adapter
 vhost1  Available  Virtual SCSI Server Adapter
```

Note: Usually vhost0 is the adapter for the internal disks. vhost1 in the example above maps the SCSI adapter to the external shared storage.

Prior to mapping hdisk20 (in the example) to a SCSI adapter, change the reservation policy on the disk.

```
$ chdev -dev hdisk20 -attr reserve_policy=no_reserve
hdisk20 changed
```

For hdisk20 (in the example) to be available to client partitions, map it to a suitable virtual SCSI adapter.

If you now print the reserve policy on hdisk20 the output resembles:

```
$ lsdev -dev hdisk20 attr reserve_policy
 value
 no_reserve
```

Next create a virtual device to map hdisk20 to vhost1.

```
$ mkvdev -vdev hdisk20 -vadapter vhost1 -dev mp1_hdisk5
 mp1_hdisk5 Available
```

Finally on the client partition run the cfgmgr command to make this disk visible via the client SCSI adapter.

You can use this disk (hdisk20 physical, and known as mp1_hdisk5 on the client partitions) to create a diskgroup, a shared volume, and eventually a shared file system.

Perform regular VCS operations on the clients vis-a-vis service groups, resources, resource attributes, etc.

Cluster Manager (Java console) limitations

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

Cluster Manager (Java Console) version 5.1 and lower cannot manage VCS 6.0 secure clusters

Cluster Manager (Java Console) from versions lower than VCS 5.1 cannot be used to manage VCS 6.0 secure clusters. Symantec recommends using the latest version of Cluster Manager.

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

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”.

Limited support from Cluster Manager (Java console)

Features introduced in VCS 6.0 may not work as expected with Java console. However, CLI option of the simulator supports all the VCS 6.0 features. You are recommended to use Veritas Operations Manager (VOM) since all new features are already supported in VOM. However, Java console may continue to work as expected with features of releases prior to VCS 6.0.

Port change required to connect to secure cluster [2615068]

In order to connect to secure cluster, the default port must be changed from 2821 to 14149. You must choose **Advanced settings** in the **Login** dialog box and change **IP**: **2821** to **IP**: **14149** for secure cluster login.

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]

A service group that runs inside of a WPAR may not fail over when its network connection is lost

For a WPAR configuration when the WPAR root is on NFS, the WPAR service group may not fail over if the NFS connection is lost. This issue is due to an AIX operating system limitation. [1637430]

Limitations related to LLT

This section covers LLT-related software limitations.

LLT over IPv6 UDP cannot detect other nodes while VCS tries to form a cluster (1533308)

LLT over IPv6 requires link-local scope multicast to discover other nodes when VCS tries to form a cluster. If multicast networking is undesirable, or unavailable in your environment, use the address of the peer nodes to eliminate the need for the multicast traffic.

Workaround: Add the set-addr entry for each local link into the /etc/llttab file. You add the entry to specify the address of the peer nodes that are available on the corresponding peer links. For example, you add the following lines into the llttab file to specify the set-addr entry for a node. In this example, the node's IPv6 address is fe80::21a:64ff:fe92:1d70.

```
set-addr 1 link1 fe80::21a:64ff:fe92:1d70
set-arp 0
```

LLT does not start automatically after system reboot (2058752)

After you reboot the systems, if you had not completed the terminal setting procedure, LLT does not start automatically and does not log any error messages. You can manually start LLT using the `/etc/init.d/llt.rc` command.

If you reinstall a system, when the system reboots a message appears on the system console to set the terminal setting if you have not already done so. LLT does not start until you complete the terminal setting procedure.

Workaround: To resolve the LLT startup issue

1. After you reboot the systems, open the system console using any available method, for example, from HMC.
2. On the console, go to the terminal setting menu, and set the terminal of your choice.
3. Select the **Task Completed** menu option.

Limitations related to I/O fencing

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

Preferred fencing limitation when VxFEN activates RACER node re-election

The preferred fencing feature gives preference to more weighted or larger subclusters by delaying the smaller subcluster. This smaller subcluster delay is effective only if the initial RACER node in the larger subcluster is able to complete the race. If due to some reason the initial RACER node is not able to complete the race and the VxFEN driver activates the racer re-election algorithm, then the smaller subcluster delay is offset by the time taken for the racer re-election and the less weighted or smaller subcluster could win the race. This limitation though not desirable can be tolerated.

Limitation with RDAC driver and FAStT array for coordinator disks that use raw disks

For multipathing to connected storage, AIX uses the RDAC driver for FAStT arrays. Since it is an active/passive array, only the current active path is exposed to clients. The I/O fencing driver, vxfen, can use only a single active path and has no foreknowledge of the passive paths to the coordinator disks on an array. If the single active path fails, all nodes in the cluster lose access to the coordinator disks.

The loss of the path to the coordinator disks can potentially go unnoticed until a reboot, split brain, or any other reason that leads to a cluster membership change occurs. In any of these conditions, the cluster cannot form, and all nodes panic to prevent data corruption. No data loss occurs.

Workaround: Use DMP and specify paths to coordinator disks as DMP paths rather than raw disks to avoid this limitation.

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.

In a cluster using SCSI-3 based fencing, I/O fencing implements data protection by placing the SCSI-3 PR keys on both the data disks and coordinator disks. In a cluster using CP server-based fencing, I/O fencing implements data protection by placing the SCSI-3 PR keys on data disks and similar registrations on CP server. 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 coordination 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 coordination 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.

Uninstalling VRTSvxvm causes issues when VxFEN is configured in SCSI3 mode with dmp disk policy (2522069)

When VxFEN is configured in SCSI3 mode with dmp disk policy, the DMP nodes for the coordinator disks can be accessed during system shutdown or fencing arbitration. After uninstalling VRTSvxvm fileset, the DMP module will no longer be loaded in memory. On a system where VRTSvxvm fileset is uninstalled, if VxFEN attempts to access DMP devices during shutdown or fencing arbitration, the system panics.

Documentation errata

The following sections cover additions or corrections for Document version: 6.0.0 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 92.

See "About Symantec Operations Readiness Tools" on page 9.

Veritas Cluster Server Bundled Agents Reference Guide

Topic: MultiNICA agent > Attributes

The Device attribute description also needs to mention the following:

Device attribute must be localized per system and must have different base IP addresses (as explained in *Sample Configuration: IPMultiNIC and MultiNICA* of *IPMultiNIC agent*).

Veritas Cluster Server Installation Guide

The note in the *Supported software for VCS* section must read as VCS supports the previous and the next versions of SF to facilitate product upgrades.

Documentation

Product guides are available in the PDF format on the software media in the `/product_name/docs` directory. Additional documentation is available online.

Symantec recommends copying pertinent information, such as installation guides and release notes to your system's `/opt/VRTS/docs` directory for reference.

Make sure that you are using the current version of documentation. The document version appears on page 2 of each guide. The publication date appears on the title page of each document. The latest product documentation is available on the Symantec website.

http://sort.symantec.com/documents

Documentation set

Table 1-16 lists the documents for Veritas Cluster Server.

Table 1-16 Veritas Cluster Server documentation

Title	File name
Veritas Cluster Server Installation Guide	vcs_install_60_aix.pdf
Veritas Cluster Server Release Notes	vcs_notes_60_aix.pdf
Veritas Cluster Server Administrator's Guide	vcs_admin_60_aix.pdf
Veritas Cluster Server Bundled Agents Reference Guide	vcs_bundled_agents_60_aix.pdf
Veritas Cluster Server Agent Developer's Guide	vcs_agent_dev_60_unix.pdf
Veritas Cluster Server Agent for DB2 Installation and Configuration Guide	vcs_db2_agent_60_aix.pdf
Veritas Cluster Server Agent for Oracle Installation and Configuration Guide	vcs_oracle_agent_60_aix.pdf
Veritas Cluster Server Agent for Sybase Installation and Configuration Guide	vcs_sybase_agent_60_aix.pdf

Table 1-17 lists the documentation for Veritas Storage Foundation and High Availability Solutions products.

Table 1-17 Veritas Storage Foundation and High Availability Solutions products documentation

Document title	File name
Veritas Storage Foundation and High Availability Solutions Solutions Guide	sfha_solutions_60_aix.pdf
Veritas Storage Foundation and High Availability Solutions Virtualization Guide	sfha_virtualization_60_aix.pdf

If you use Veritas Operations Manager (VOM) to manage Veritas Storage Foundation and High Availability products, refer to the VOM product documentation at:

http://sort.symantec.com/documents

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.

New features related to Virtual Business Services (VBS)

Virtual Business Services (VBS) feature extends the VOM Business Entity (BE) functionality available since VOM 3.x release. VOM BE support Application Entity type which is hence forth referred to as Virtual Business Services (VBS) in VOM

4.1 and SFHA 6.1 releases. Virtual Business Services allow users to define and manage heterogeneous, inter-cluster, multi-tier applications. Each tier is represented by a Service Group which may be configured on separate VCS Clusters or ApplicationHA nodes. VBS builds on top of VCS HA/DR and ApplicationHA to provide business service availability across physical and virtual environments. The application tiers (Service Group) can optionally be linked with configurable dependency types and fault actions.

Ordered Start/Stop operations on a VBS

VBS allows ordered start/stop of the entire business service via a single click or through a single command-line interface. If applications are hosted on VMWare virtual machines, you can configure the virtual machines to be automatically started or stopped when you start or stop the Virtual Business Service.

Ability to perform VBS operations via CLI

You can work on Virtual Business Services using CLI from any node of any participating tier clusters. Thus VOM CS is optional after you have configured VBS.

DR support for VBS

VBS provides a comprehensive DR solution that builds on top of VCS DR. The DR support is based on having one or more GCO Service Groups in the VBS.

VBS support for robust fault management

VBS provides robust fault management with configurable actions like stopping, starting, restarting a Service Group (application tier) when the child Service Group faults or recovers. Three dependency types (viz. Soft, Firm, Restart) are supported between Service Groups configured within a VBS.

Secure access control for Virtual Business Services

Operations on a VBS via CLI are permitted only for root users in the participating tiers. Operations through VOM support role based access control (RBAC).

Audit trail of operations performed on a VBS

All user actions performed on a VBS are easily traceable via audit trail and logs.