Veritas™ Cluster Server Release Notes

Solaris

6.0 Platform Release 1

April 2012

Veritas™ Cluster Server Release Notes

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

Product version: 6.0 PR1

Document version: 6.0PR1.1

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 PR1 for Solaris. 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: 6.0PR1.1 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 `docs` directory on the software media that contains the product guides to the `/opt/VRTS` directory on your system.

This release includes the following component product release notes:

- *Veritas Storage Foundation Release Notes* (6.0 PR1)

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 Oracle Solaris Studio. The following is the layout of libvcsagfw.so in usr/lib:

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

If you use custom agents compiled on older compilers, the agents may not work with VCS 6.0 PR1. If your custom agents use scripts, continue linking to ScriptAgent. Use Script50Agent for agents written for VCS 5.0 and above.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a 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 PR1

This section lists the changes in Veritas Cluster Server 6.0 PR1.

Support for Solaris 11

VCS 6.0 PR1 supports Solaris 11 and also supports VCS/SFHA/SF/SFCFS/SVS product install packages in Image Packaging System (IPS) format.

Changes related to installation

The product installer includes the following changes in VCS 6.0 PR1.

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 packages 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.

Packaging updates

The following lists the package changes in this release.

- New `VRTSsfcpi60` package for product installer scripts

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

  The `VRTSvbs` package 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` package change

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

For more information, see the *Installation 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.

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.

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 PR1:

- Zone

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.

Attributes introduced in VCS 6.0PR1

Following are the list of attributes introduced in VCS 6.0 PR1:

Cluster-level attribute

- 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.

Zpool agent attributes

- DeviceDir: Specifies the directories that the `zpool import` command must search for devices or files.
- FailMode: Controls the system behavior in the event of a catastrophic pool failure. The value of this attribute is used as the failmode option while

importing the ZFS storage pool. The possible values are **wait**, **continue**, or **panic**.

- ForceOpt: Invokes the following commands again with the -f option if this attribute is enabled (if the value is set to 1) and if the following commands fail:
  - `zpool export` in the offline entry point
  - `zpool export` in the clean entry point
  - `zpool import` in the online entry point
- ForceRecoverOpt: Invokes the `zpool import` command again with -F option when this attribute is enabled (if its value is set to 1) and if the `zpool import` command fails.

LDom agent attributes

- Memory: Specifies the amount of memory to be assigned to an LDom.

  See the *Bundled Agents Reference Guide* for more information on the new attributes.
- RemoveLDomConfigForMigration: If enabled, agent removes the LDom configuration from the system during offline and clean operations provided CfgFile attribute is configured. You must enable this attribute if domain migration is planned for the logical domain. This is because, domain migration cannot be performed if logical domain configuration is present on target node for migration.
- IPAddress: The IP address to be assigned to an exclusive IP zone at this site after a cross-site failover. The agent writes the IP address inside the Zone Root in the `/etc/hostname.Device` file, where Device is the value of Device key.
- Netmask: The netmask to be used in an exclusive IP zone at this site after a cross-site failover. The agent writes the netmask inside the Zone Root in the file`/etc/netmasks`.
- Gateway (Default Router): The default gateway used by this Zone at this site.
- DNS: The domain name to use within the Zone at this site.
- ConfigureNetwork: Specifies if the LDom agent configures the network-bootarguments PROM variable of the guest domain.

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).

Zone agent attribute:

- DeleteVCSZoneUser: If enabled on a non-secure cluster, Zone agent deletes the VCS Zone user created for password-less communication between local-zone and global zone during offline and clean entry points. DeleteVCSZoneUser is disabled by default.
- DROpts: The value of this attribute consists of the following keys that define disaster recovery options for the Zone agent:
  - DNSDomain
  - DNSSearchPath
  - DNSServers
  - Gateway
  - Device
  - IPAddress
  - Netmask
  - Hostname

  In a DR configuration, if one or more of these keys are set, the resource is considered to be DR-enabled. If all the keys stay at their default value (""), then the resource is not DR-enabled even if it is in a disaster recovery configuration.

MultiNICB agent attribute

- IPMPDevice: Stores the IPMP interface name. To configure MultiNICB resource in IPMP mode on Solaris 11, set the value of this attribute to the valid name of IPMP interface created for interfaces under MultiNICB control. At the same time, make sure that UseMpathd attribute of MultiNICB is set to 1.

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 solaris10 brand zones

Oracle Solaris has added support for solaris10 brand zone on Solaris 11 system. Zone agent is updated to support solaris10 brand zone on Solaris 11 system.

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.

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).
- Application agent no longer uses the StopProgram during clean operation if CleanProgram is not specified.
- The character limitation for processes length in MonitorProcesses attribute is removed. Now you can use `/usr/ucb/ps -ww <pid>` command to get the full COMMAND for process and configure it in MonitorProcesses attribute.
- For applications running in Solaris 10 zones, you must set PidFile attribute to the path as seen from the non-global zone.
- Application Agent requires pkg:/compatibility/ucb package to run in Solaris 11.

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.

Zone agent enables milestone while making the zone online

When boot-state is specified in the Zone agent, the Zone agent must run `svcadm enable -r <boot-state>` to enable the specified boot-state. If Zone is on shared disk and you disable the bootstate, the Zone faults on the other node and since the boot state is disabled, it faults on that node as well. Therefore, Zone agent must run `svcadm enable -r <boot-state>`.

Zone agent enables milestone while making the zone online, if not already enabled. The following option enables all the dependent services:

```
zlogin <zone-name>; svcadm enable -r <boot-state>
```

Enhanced preonline_ipc trigger

The `preonline_ipc` trigger functionality of VCS, that performs certain checks before bringing a group online, did not work for resources other than IP resources.

The `preonline_ipc` trigger is enhanced to support the following types of resources on a system:

- IP
- IPMultiNIC
- IPMultiNICB

Enhancing Zpool agent for better support with Solaris 10

Enahnced Zpool agent with the following attributes to handle various `zpool` issues:

- DeviceDir
- FailMode
- ForceOpt
- ForceRecoverOpt

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.

Enabled IMF for Zone agent

The Zone agent now leverages 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*.

Change in behavior of Zpool agent

Before VCS 6.0, if the storage pool was brought online ouside VCS and altrootpath setting of the zpool was not set, then the Zpool agent returned ONLINE state. The Zpool agent is modified such that it returns UNKNOWN. You must export the zpool and online the resource to set the altrootpath.

For more information, refer to *Veritas Cluster Server Bundled Agents Reference Guide*.

Changes in network agents

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

- IP
- IPMultiNIC
- MultiNICA
- IPMultiNICB

Changes to Share agent

VCS 6.0 PR1 requires at least one shared directory on a node in order to configure Share agent.

Use the following command to share a directory across reboots:

```
#share /xyz
```

Changes in Apache agent requirements

On Solaris 11 platform, VCS Apache agent requires the following package as prerequisite:

```
pkg:/compatibility/ucb
```

In absence of the above package the following error is displayed:

```
Can't exec "/usr/ucb/ps": No such file or
directory at /opt/VRTSvcs/bin/Apache/Proc.pm line 699.
Use of uninitialized value $sErrorString in scalar chomp
at /opt/VRTSvcs/bin/Apache/Proc.pm line 720.
```

Change to NFS agent

Setting UseSMF attribute of NFS resource to 0 is not supported.

IPMultiNICB and MultiNICB must be configured in IPMP mode

Since IPMP mode is the only supported mode to configure MultiNICB agent in VCS 6.0 PR1, IPMultiNICB and MultiNICB resources on Solaris 11 system must be configured in the following order:

1. Create IPMP interface manually for the interfaces under MultiNICB control. Refer to *Oracle Solaris Administration: Network interfaces and Network Virtualization Guide* for more details.
2. Specify the IPMP interface name in IPMPDevice attribute of MultiNICB resource.
3. Set UseMpathd and ConfigCheck attributes of MultiNICB resource to 1 and 0 respectively.
4. Make sure that the IPMP interface and corresponding base interfaces are configured correctly and are up before enabling MultiNICB resource.

Changes to database agents

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 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:

- Faster detection of LLT link failures

  LLT now has the capability to detect the LLT link failures immediately using the operating system's link-down notification feature.
- LLT now supports VLAN tagging (IEEE 802.1Q).

- The `lltconfig` command includes the following new options:
  - -Q
    You can use this option to configure a link as "hidden". LLT needs this type of link when you enable faster detection of link failure.
  - -j
    You can use this option to set the LLT link failure detection level.
  - The command also includes a new timer parameter `linkstable`. This parameter specifies the amount of time to wait before LLT processes the link-down event for any link of the local node when you have enabled faster link failure detection. This `linkstable` prevents a flaky link from causing unnecessary membership changes.
  - -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.

  The llttab file includes the following changes:
  - hidden
    The new keyword hidden indicates that the link is a hidden link which LLT uses when you enable faster detection of link failure.
  - set-linkfaildetectlevel
    You can use this new command option in the `/etc/llttab` file to set the LLT link failure detection level.
- 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.

Support for Non-SCSI3 fencing

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

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

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.

HAD and Fencing wait sufficiently to start after Volume Manager has performed recovery after node reboot

The high availability daemon (HAD) and fencing module (VxFen) failed to start if the Volume Manager (VxVM) was performing a recovery after node reboot. The fencing module was unable to access the coordinator disk group until the Volume Manager had completed the recovery. The `init` script of the fencing module and HAD process is modified to accommodate the time taken by Volume Manager to complete the recovery process before configuring the fencing module. This configurable period can be defined by setting the VXFEN_VXVMRECOVER_TIMEOUT_SOL variable in `/etc/default/vxfen` file. The default value of this variable is 300 seconds. The `init` script of HAD waits an additional 30 seconds more than the configured time for the fencing module to complete its configuration before starting the HAD process.

Changes related to virtualization support

This section lists virtualization changes for this release.

Enhanced LDom agent to support dynamic memory reconfiguration

The Oracle VM server for SPARC support dynamic reconfiguration of memory assigned to logical domain. Symantec added a new attribute memory to support this feature with LDOM agent.

Virtualization support on Solaris

The following new virtualization features are introduced on Solaris:

- Support for LDom domain migration: LDom agent now detects the LDom migration (warm/live) and changes the state of the LDom resource accordingly.
- Support for Zone agent to allow single VCS user to manage multiple zones: You can use single VCS user to manage multiple zones in VCS environment. You no longer require a separate VCS user to manage each zone in single VCS

cluster. The hazonesetup command is enhanced to support this. See hazonesetup command usage for more information.

- VCS supports zone root on ZFS filesystem only. Oracle Solaris 11 supports zone root creation on ZFS file systems only.

Domain migration support for Oracle VM server (OVM) for SPARC

Added support for logical domain migration (live migration on OVM 2.1) in Oracle VM Server for SPARC environment. LDom agent detects the logical domains being migrated and changes the state of VCS resource accordingly.

See the *Veritas Storage Foundation and High Availability Virtualization Guide* for more information on supported configurations for domain migration.

Parallel option is added to hazonesetup command to configure parallel service groups

The hazonesetup command does not set localized zone name attribute in case of parallel zone. Parallel option is added to hazonesetup command to configure parallel service group.

Updated hazonesetup command syntax to accommodate new arguments

Updated hazonesetup syntax to accommodate the following:

- Support to accept the user name for Zone from hazonesetup command.
- Support to update the password for the VCS Zone user whenever needed.
- If the username is not passed to hazonesetup, it creates a user with the default username.
- Support to configure parallel Zone service group.

The new syntax for hazonesetup command is:

```
# /opt/VRTS/bin/hazonesetup [-t] -g <sg_name>
-r <res_name> -z <zone_name> [-u <user_name>] -p <password>
[-a] [-l] -s <systems>
```

Where:

-t	Update the password for VCS zone user
-g sg_name	Name of the zone service group to be created in VCS configuration

-r res_name	Name of the zone resource to be created in VCS configuration
-z zone_name	Name of the zone configured on the system
-u user_name	Name of the VCS user used for password less communication between local zone and global zone. If no user name is specified default user name is assumed
-p password	Password for the VCS user used for password less communication
-a	Populate AutoStartList for the group
-l	Configure parallel service group. If -l is not specified a failover service group is created by default.
-s systems	Comma (,) separated list of systems on which the zone service group need to be configured. (Ex., sys1,sys2,...).

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 1-1 lists the documents introduced in this release.

Table 1-1 New documents

New documents	Notes
Veritas Storage Foundation Installation Guide	Installation and upgrade information for Storage Veritas Foundation.

Table 1-1 New documents *(continued)*

New documents	Notes
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.
Symantec VirtualStore Release Notes	Release-specific information Symantec VirtualStore.
Virtual Business Services–Availability User's Guide	Information about Virtual Business Services. This document is available online.

Table 1-2 lists the documents that are deprecated in this release.

Table 1-2 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*.
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*.

Table 1-2 Deprecated documents *(continued)*

Deprecated documents	Notes
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 1-3 lists documents that are no longer bundled with the binaries. These documents are now available online.

Table 1-3 Online documents

Document
Veritas Cluster Server Agent Developer's Guide
Veritas Cluster Server Application Note: Dynamic Reconfiguration of Oracle Sun Servers
Veritas File System Programmer's Reference Guide

VCS system requirements

This section describes system requirements for VCS.

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

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

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

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 33.

See “Supported Solaris operating systems ” on page 33.

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 Solaris operating systems

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

Table 1-4 shows the supported operating systems for this release.

Table 1-4 Supported operating systems

Operating systems	Levels	Chipsets
Oracle Solaris 11	GA	SPARC
Oracle Solaris 11	GA	x64

Supported software for VCS

VCS supports the following volume managers and file systems:

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

  VCS 6.0 PR1 supports the following versions of SF:

  - SF 6.0PR1
    - VxVM 6.0PR1 with VxFS 6.0PR1

Supported VCS agents

Table 1-5 lists the agents for enterprise applications and the software that the agents support.

Table 1-5 Supported software for the VCS agents for enterprise applications

Agent	Application	Application version	Solaris version
Oracle	Oracle	11gR2 (11.2.0.3.0)	SPARC: Oracle Solaris 11 x64: Oracle Solaris 11

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 30.

No longer supported agents and components

VCS no longer supports the following:

- Configuration wizards
- CampusCluster agent
- NFSLock agent.
  Use the NFSRestart agent to provide high availability to NFS lock records.
- nfs_restart trigger.
  Use the NFSRestart agent to provide high availability to NFS lock records.
- ServiceGroupHB agent.
  This release does not support disk heartbeats. Symantec recommends using I/O fencing.
- SANVolume agent
- VRTSWebApp
- 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.
- VRTSutil package. This package is no longer supported.
- The push install features is not supported for Solaris 11 VRTSvbs package through VOM 4.1CS
- VCS does not support CFS, UFS and VxFS mounts for the zone root in this release as Oracle Solaris.
- Sybase and DB2udb agents are not supported in VCS 6.0 PR1.
- The following agents are not supported in VCS 6.0 PR1 on Solaris 11 platform:
  - AlternateIO
  - IPMultiNIC
  - MultiNICA
- The following features are not supported for the respective agent in VCS 6.0 PR1:
  - Zone: Disaster Recovery for Zone.
  - LDom: Disaster Recovery for LDom.

Deprecated attributes

Deprecated Oracle agent attributes:

- AgentDebug
- DetailMonitor

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.

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 69.

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.

Locale message displayed on Solaris 11 system for solaris10 brand zones

When you run the `zlogin` command on a Solaris 11 system, the system logs the following error message:

```
Could not set locale correctly.
```

The default locale for Solaris 11 is en_US.UTF-8 and that of Solaris 10 is C. With Solaris 10 branded zone, en_US.UTF-8 is not installed inside the zone by default. Therefore, the error message is logged.

Workaround: This message can be safely ignored as there is no functionality issue. To avoid this message, install en_US.UTF-8 locale on solaris10 brand zone.

Issues related to installation

This section describes the known issues during installation and upgrade.

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.

Installing VRTSvlic package on Solaris system with local zones displays error messages [2555312]

If you try to install VRTSvlic package on a Solaris system with local zones in installed state, the system displays the following error messages:

```
cp: cannot create /a/sbin/vxlicinst: Read-only file system
cp: cannot create /a/sbin/vxlicrep: Read-only file system
cp: cannot create /a/sbin/vxlictest: Read-only file system
```

Workaround: On the Solaris system, make sure that all non-global zones are started and in the running state before you install the VRTSvlic package.

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

Due to a clock synchronization issue, when you install a cluster using installer and if you synchronize your systems with an NTP server, 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.

VCS installation with CPI fails when a non-global zone is in installed state and zone root is not mounted on the node (2731178)

CPI tries to boot a zone in installed state during installation/ or uninstallation. The boot fails if the underlying storage for zone root is not imported and mounted onto the node, causing the installation or uninstallation to fail.

Workaround: Make sure that the non-global zones are in running or configured state when CPI is invoked for installation or uninstallation.

Operational issues for VCS

Issues with configuration of resource values [1848959]

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

```
VCS WARNING V-16-2-13806 Thread(1437547408) ArgListValues overflow;

Cannot append values more than upper limit of (425).
```

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

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.

Missing characters in system messages [2334245]

You may see missing characters, especially in long system messages in response to certain commands.

Workaround: No workaround.

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]

Missing host names in engine_A.log file

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

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.

Character corruption observed when executing the uuidconfig.pl -clus -display -use_llthost command [2350517]

If password-less ssh/rsh is not set, the use of `uuidconfig.pl` command in non-English locale may print garbled characters instead of a non-English string representing the Password prompt.

Workaround: No workaround.

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.

Oracle service group faults on secondary site during failover in a disaster recovery scenario [2558903]

Oracle service group fails to go online in the DR site when disaster strikes the primary site. This happens if the AutoFailover attribute on the Service Group is set to 1 and when the corresponding service group's FireDrill is online in the DR site. Firedrill Service group may remain ONLINE on the DR site.

Workaround: If the service group containing the Oracle (or any database) resource faults after attempting automatic DR failover while FireDrill is online in the DR site, manually offline the FireDrill Service Group. Subsequently, attempt the online of the Oracle Service Group in the DR site.

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.

CmdServer process is unable to stop if VCS is stopped (2721526)

The CmdServer is only able to receive credentials if VCS is running. Therefore, CmdServer cannot stop if VCS is stopped before stopping CmdServer.

Workaround: Manually kill the CmdServer process using `pkill CmdServer` before stopping VCS.

VCS service does not start when security is disabled on a cluster in security enabled mode (2724844)

When you change a VCS cluster state from security enabled to security disabled using script based installer, SMF service for VCS goes into a maintenance state.

Workaround: Perform the following steps:

1 Clear the SMF service state for VCS.

```
# svcadm clear system/vcs
```

2 Enable the SMF service.

```
# svcadm enable system/vcs
```

Startup trust failure messages in system logs (2721520)

If you configure a cluster with security enabled, there might be some messages logged in system message logs related to Symantec authentication. These messages can be ignored and have no effect on functionality.

Workaround: No workaround.

Issues related to the bundled agents

Entry points that run inside a zone are not cancelled cleanly [1179695]

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

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

Solaris mount agent fails to mount Linux NFS exported directory

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

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

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

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

Example

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

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

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

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

Zone remains stuck in down state if tried to halt with file system mounted from global zone [2291200]

This issue is seen in filesystems chich are mounted with lock inside non-global zone. For filesystem which are mounted directly inside non-global zone do not set the VxFSMountLock attribute for Mount resource.

Workaround: To resolve this issue perform the following steps:

1 Unmount the file system manually from global zone and then halt the zone. For VxFS, use following commands to unmount the file system from global zone.

```
# unmount -o mntunock=VCS<zone root path>/<Mount Point>
```

2 If the above command fails forcefully unmount the filesystem.

```
# unmount -f -o mntunlock=VCS<zone root path>/<Mount Point>
```

3 To halt the zone, use following command:

```
# zoneadm -z<zone_name> halt
```

4 Set the VxFSMountLock attribute to 0 for Mount resource.

```
# hares -modify <mnt_res> VxFSMountLock 0
```

Process and ProcessOnOnly agent rejects attribute values with white spaces [2303513]

Process and ProcessOnOnly agent does not accept Arguments attribute values that are separated by multiple whitespaces. The Arguments attribute specifies the set of arguments for a process. If a script controls the process, the script is passed as an argument. You must separate multiple arguments by using a single whitespace. A string cannot accommodate more than one space between arguments, or allow leading or trailing whitespace characters. This attribute must not exceed 80 characters.

Workaround: You should use only single whitespace to separate the argument attribute values. Make sure you avoid multiple whitespaces between the argument attribute values or trailing whitespace characters.

The zpool commands hang and remain in memory till reboot if storage connectivity is lost [2433609]

If the FailMode attribute of `zpool` is set to continue or wait and the underlying storage is not available, the `zpool` commands hang and remain in memory until the next reboot.

This happens when storage connectivity to the disk is lost, the `zpool` commands hang and they cannot be stopped or killed. The zpool commands run by the monitor entry point remains in the memory.

Workaround: There is no recommended workaround for this issue.

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.

Offline of zone resource may fail if zoneadm is invoked simultaneously [2353542]

Offline of zone EP uses zoneadm command to offline a zone. Therefore, if zoneadm is invoked simultaneously for multiple zones, the command may fail. This is due to Oracle bug 6757506 that causes a race condition between multiple instances of zoneadm command and displays the following message:

```
zoneadm: failed to get zone name: Invalid argument
```

Workaround: No workaround.

Password changed while using hazonesetup script does not apply to all zones [2332349]

If you use the same user name for multiple zones, updating password for one zone does not updated the password of other zones.

Workaround: While updating password for VCS user which is used for multiple zones, update password for all the zones.

NIC agent may report incorrect interface state due to less traffic [2512592]

When PingOptimize is set to 1 and no NetworkHosts is specified, NIC agent depends on packet count to report the health of the interface. If the traffic on the interface is not sufficient enough, NIC agent may report incorrect state of the interface.

Workaround: Any of the following workaround must resolve the issue:

- Setting PingOptimize = 0. This makes NIC agent ping the broadcast address whenever there is no traffic on the interface.
- Setting valid NetworkHosts value. This makes NIC agent to ping NetworkHosts to check health of status.

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 local Zone on Solaris

Workaround: No workaround.

No IPv6 support for NFS [2022174]

IPv6 is not supported for NFS.

Workaround: No workaround.

Share resource goes offline unexpectedly causing service group failover [1939398]

Share resource goes offline unexpectedly and causes a failover when NFSRestart resource goes offline and UseSMF attribute is set to 1 (one).

When NFSRestart resource goes offline, NFS daemons are stopped. When UseSMF attribute is set to 1, the exported file systems become unavailable, hence Share resource unexpectedly goes offline.

Workaround: Set the value of ToleranceLimit of Share resource to a value more than 1.

Mount agent does not support all scenarios of loopback mounts [2604471]

For a mount point under VCS control, you can create loop back mounts for the mount point. For example, mount point /mntpt is mounted on /a as loop back mount and /a is mounted on /b as loop back mount, then offline and online of the mount resource fails.

Workaround: Mount the mount point /mntpt on /b as loop back mount.

State of the Application resource is resported OFFLINE if MonitorProgram does not have executable permissions [2612140]

Application agent reports state of resource as OFFLINE instead of UNKNOWN if the MonitorProgram command is present but does not have executable permissions.

Workaround: Make sure that the MonitorProgram command has executable permissions.

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>
```

Monitor falsely reports NIC resource as offline when zone is shutting down (2683680)

If a NIC resource is configured for an Exclusive IP zone, the NIC resource is monitored inside the zone when the zone is functional. If the NIC monitor program is invoked when the zone is shutting down, the monitor program may falsely report the NIC resource as offline. This may happen if some of the networking services are offline but the zone is not completely shut down. Such reports can be avoided if you override and set the ToleranceLimit value to a non-zero value.

Workaround: When a NIC resource is configured for an Exclusive IP zone, you are recommended to set the ToleranceLimit attribute to a non-zero value.

Calculate the ToleranceLimit value as follows:

Time taken by a zone to completely shut down must be less than or equal to NIC resource's MonitorInterval value + (MonitorInterval value x ToleranceLimit value).

For example, if a zone take 90 seconds to shut down and the MonitorInterval for NIC agent is set to 60 seconds (default value), set the ToleranceLimit value to 1.

Apache resource does not come online if the directory containing Apache pid file gests deleted when a node or zone restarts (2680661)

The directory in which Apache http server creates PidFile may get deleted when a node or zone restarts. Typically the PidFile is located at `/var/run/apache2/httpd.pid`. When the zone reboots, the `/var/run/apache2` directory may get removed and hence the http server startup may fail.

Workaround: Make sure that Apache http server writes the PidFile to an accessible location. You can update the PidFile location in the Apache http configuration file (For example: `/etc/apache2/httpd.conf`).

Zone root configured on ZFS with `-F` option causes boot failure (2695418)

On Solaris 11 system, attaching zone with `-F` option may result in zone boot failure if zone root is configured on ZFS.

Workaround: Change the ForceAttach attribute of Zone resource from 1 to 0. With this configuration, you are recommended to keep the default value of DetachZonePath as 1.

Error message is seen for Apache resource when zone is in transient state (2703626)

If the Apache resource is probed when the zone is getting started, the following error message is logged:

```
Argument "VCS ERROR V-16-1-10600 Cannot connect to VCS engine\n"
isn't numeric in numeric ge (>=) at /opt/VRTSvcs/bin/Apache/Apache.pm
line 452.
VCS ERROR V-16-1-10600 Cannot connect to VCS engine
LogInt(halog call failed):TAG:E:20314 <Apache::ArgsValid> SecondLevel
MonitorTimeOut must be less than MonitorTimeOut.
```

Workaround: You can ignore this message. When the zone is started completely, the `halog` command does not fail and Apache agent monitor runs successfully.

IP resource does not go online inside a shared IP zone on Oracle Solaris 11 (2730451)

On an Oracle Solaris 11 system, when you configure IP resource in a shared IP zone of type solaris brand, the IP resource does not go online.

Workaround: No workaround.

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.

Issues related to the agent framework

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

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

Resolution: No resolution.

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

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

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

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

GAB SMF service sometimes fails to start after reboot (2724565)

In SFRAC environments, sometimes GAB might fail to start because of the race between GAB and LMX in calling add_drv.

Workaround: Start the GAB SMF service and all other dependent services manually using:

```
# svcadm enable gab
# svcadm enable vxfen
# svcadm enable vcs
```

Issues related to I/O fencing

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

Delay in rebooting Solaris 10 nodes due to vxfen service timeout issues (1897449)

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

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

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

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

To avoid the vxfen stop service timeout error

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

```
# hastop -all
```

2 Reboot the systems:

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

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.

When I/O fencing is not up, the svcs command shows VxFEN as online (2492874)

Solaris 10 SMF marks the service status based on the exit code of the start method for that service. The VxFEN start method executes the vxfen-startup script in the background and exits with code 0. Hence, if the vxfen-startup script subsequently exits with failure then this change is not propagated to SMF. This behavior causes the `svcs` command to show incorrect status for VxFEN.

Workaround: Use the `vxfenadm` command to verify that I/O fencing is running.

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 package 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, mth VIP is mapped to nth 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.

CP server configuration fails while setting up secure credentials for CP server hosted on an SFHA cluster (2621029)

When you configure CP server using the `configure_cps.pl` utility, the configuration fails while setting up secure credentials for CP server that is hosted on an SFHA cluster. You may see the following error:

```
Creating softlink to credential directory /etc/VRTScps/db/CPSERVER
on node nodename.
Unable to connect to node nodename using /usr/bin/ssh.
Please configure ssh communication and retry. Exiting.
```

Workaround: You can use any of the following options:

- Before running the `configure_cps.pl` utility, change the default shell for root user to either KSH or bash.
- Perform the following steps after running the `configure_cps.pl` utility on each node of the cluster:
  - Manually remove the old credential directory or softlink. For example:

    ```
    # rm -rf /var/VRTSvcs/vcsauth/data/CPSERVER
    ```

  - Create a new soft-link to the shared location of the credential directory:

    ```
    # ln -s path_of_CP_server_credential_directory \
     /var/VRTSvcs/vcsauth/data/CPSERVER
    ```

- Start the CPSSG service group:

  ```
  # hagrp -online CPSSG -any
  ```

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.

IMF does not fault zones if zones are in ready or down state [2290883]

IMF does not fault zones if zones are in ready or down state.

IMF does not detect if zones are in ready or down state. In Ready state, there are no services running inside the running zones.

Workaround: Offline the zones and then restart.

IMF does not detect the zone state when the zone goes into a maintenance state [2534980]

IMF does not detect the change in state. However, the change in state is detected by Zone monitor in the next cycle.

Workaround: No workaround.

Engine log gets flooded with messages proportionate to the number of mount offline registration with AMF [2619778]

In a certain error condition, all mount offline events registered with AMF are notified simultaneously. This causes the following message to get printed in the engine log for each registered mount offline event:

```
<Date> <Time> VCS INFO V-16-2-13717
(vcsnode001) Output of the completed operation
(imf_getnotification)
==============================================
Cannot continue monitoring event
Got notification for group: cfsmount221

==============================================
```

This is an expected behavior for this error condition. Apart from the messages there will be no impact on the functionality of the VCS solution.

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.

Unable to log on to secure VCS clusters on Solaris 11 using Java GUI (2718955)

Connecting to secure clusters deployed on Solaris 11 systems using VCS Java GUI is not supported in VCS 6.0PR1. The system displays the following error when you attempt to use the Java GUI:

```
Incorrect username/password
```

Workaround: No workaround.

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 69.

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/nsswitch.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.

Online for LDom resource fails [2517350]

Online of LDom resource fails when the boot disk configured in the guest domain that is a part of the virtual disk multi-pathing group (mpgroup) and also the primary path to the virtual disk is not available.

This is due to the limitations in Oracle VM Server that do not allow retrying of other device paths that exist for the virtual disks, which are part of a virtual disk multi-pathing group, when booting a guest domain.

Workaround: None.

Zone 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.

LDom resource calls clean entry point when primary domain is gracefully shut down

LDom agent sets failure policy of the guest domain to stop when primary domain stops. Thus when primary domain is shut down, guest domain is stopped. Moreover, when primary domain is shutdown, ldmd daemon is stopped abruptly and LDom configuration cannot be read. These operations are not under VCS control and VCS may call clean entry point.

Workaround: No workaround.

Share agent limitation (2717636)

If the Share resource is configured with VCS to share a system directory (for example, /usr) or Oracle Solaris 11 which gets mounted at boot time, the VCS share resource detects it online once VCS starts on the node after a panic or halt. This can lead to a concurrency violation if the share resource is a part of a failover service group, and the group has failed over to another node in the cluster. VCS brings down the Share resource subsequently. This is due to the share command behavior or Oracle Solaris 11, where a directory shared with share command remains persistently on the system across reboots.

Limitations related to the VCS database agents

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.

- Configuring Veritas Volume Replicator for Zone Disaster Recovery is not supported for zone root replication. Oracle Solaris 11 supports zone root only on ZFS file system.

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.

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.

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.

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 package, the DMP module will no longer be loaded in memory. On a system where VRTSvxvm package is uninstalled, if VxFEN attempts to access DMP devices during shutdown or fencing arbitration, the system panics.

Documentation

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

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 1-6 lists the documents for Veritas Cluster Server.

Table 1-6 Veritas Cluster Server documentation

Title	File name
Veritas Cluster Server Installation Guide	vcs_install_60pr1_sol.pdf
Veritas Cluster Server Release Notes	vcs_notes_60pr1_sol.pdf
Veritas Cluster Server Administrator's Guide	vcs_admin_60pr1_sol.pdf
Veritas Cluster Server Bundled Agents Reference Guide	vcs_bundled_agents_60pr1_sol.pdf
Veritas Cluster Server Agent Developer's Guide	vcs_agent_dev_60_unix.pdf
Veritas Cluster Server Application Note: Dynamic Reconfiguration for Oracle Servers	vcs_dynamic_reconfig_60pr1_sol.pdf
Veritas Cluster Server Agent for Oracle Installation and Configuration Guide	vcs_oracle_agent_60pr1_sol.pdf

Table 1-7 lists the documentation for Veritas Storage Foundation and High Availability Solutions products.

Table 1-7 Veritas Storage Foundation and High Availability Solutions products documentation

Document title	File name
Veritas Storage Foundation and High Availability Solutions Solutions Guide	sfha_solutions_60pr1_sol.pdf
Veritas Storage Foundation and High Availability Solutions Virtualization Guide	sfha_virtualization_60pr1_sol.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.