Symantec™ Storage Foundation and High Availability Solutions 6.2.1 Release Notes - Linux

Maintenance Release

RHEL 6, 7, OL 6, 7, SLES 11

April 2015

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: 6.2.1

Document version: 6.2.1 Rev 0

Legal Notice

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

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 website 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

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

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 website.

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

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

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

About Symantec Storage Foundation and High Availability Solutions

This document includes the following topics:

Introduction

This document provides information about the products in Symantec Storage Foundation and High Availability Solutions 6.2.1 Maintenance Release (6.2.1 MR).

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

http://www.symantec.com/docs/TECH225259

The hardware compatibility list contains information about the supported hardware and is updated regularly. For the latest information on supported hardware visit:

http://www.symantec.com/docs/TECH211575

Before installing or upgrading Symantec Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

For instructions to install or upgrade the product, see the *Symantec Storage Foundation and High Availability Solutions 6.2.1 Installation Guide* on the Symantec website:

https://sort.symantec.com/documents

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

This is "Document version: 6.2.1 Rev 0" of the *Symantec Storage Foundation and High Availability Solutions 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

List of products

Apply the patches for the following Symantec Storage Foundation and High Availability Solutions products:

- Symantec Dynamic Multi-Pathing (DMP)
- Veritas Volume Manager (VxVM)
- Veritas File System (VxFS)
- Symantec Storage Foundation (SF)
- Symantec Cluster Server (VCS)
- Symantec Storage Foundation and High Availability (SFHA)
- Symantec Storage Foundation Cluster File System and High Availability (SFCFSHA)
- Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)
- Symantec ApplicationHA (ApplicationHA)
- Symantec Storage Foundation for Sybase ASE CE (SFSYBASECE)

Note: In 6.2.1, Symantec Storage Foundation for Sybase ASE CE is only supported on RHEL 6.

List of RPMs

The section lists the RPMs for Linux.

Note: You can also view the list using the `installmr` command: `./installmr -listpatches`

Table 1-1 lists the Red Hat Enterprise Linux 6 RPMs that are updated in this release.

Table 1-1 RPMs for Red Hat Enterprise Linux 6

Name	Version	Arch	Size in Bytes
VRTSamf	6.2.1.000	x86_64	3292688
VRTSaslapm	6.2.1.000	x86_64	6303200
VRTScavf	6.2.1.000	i686	200836
VRTScps	6.2.1.000	x86_64	12432432
VRTSdbed	6.2.1.000	x86_64	82721723
VRTSfsadv	6.2.1.000	x86_64	4470712
VRTSgab	6.2.1.000	x86_64	3600492
VRTSllt	6.2.1.000	x86_64	8978596
VRTSperl	5.16.1.27	x86_64	15835992
VRTSrhevm	6.2.1.000	x86_64	30604
VRTSsfcpi62	6.2.1.000	noarch	1445355
VRTSsfmh	6.1.0.400	x86_64	43668551
VRTSspt	6.2.1.000	noarch	26316201
VRTSvcs	6.2.1.000	i686	71450440
VRTSvcsag	6.2.1.000	i686	12590136
VRTSvcsea	6.2.1.000	i686	260264

Table 1-1 RPMs for Red Hat Enterprise Linux 6 *(continued)*

Name	Version	Arch	Size in Bytes
VRTSvcsvmw	6.2.1.000	i686	8905488
VRTSvxfen	6.2.1.000	x86_64	3821196
VRTSvxfs	6.2.1.000	x86_64	15254472
VRTSvxvm	6.2.1.000	x86_64	57202964

Table 1-2 lists the Red Hat Enterprise Linux 7 RPMs that are updated in this release.

Table 1-2 RPMs for Red Hat Enterprise Linux 7

Name	Version	Arch	Size in Bytes
VRTSamf	6.2.1.000	x86_64	2366140
VRTSaslapm	6.2.1.000	x86_64	843956
VRTScavf	6.2.1.000	i686	200808
VRTScps	6.2.1.000	i686	11634572
VRTSdbed	6.2.1.000	x86_64	82721723
VRTSfsadv	6.2.1.000	x86_64	3660148
VRTSgab	6.2.1.000	x86_64	2467204
VRTSglm	6.2.1.000	x86_64	126848
VRTSllt	6.2.1.000	x86_64	6113844
VRTSodm	6.2.1.000	x86_64	207200
VRTSperl	5.16.1.27	x86_64	15836048
VRTSsfcpi62	6.2.1.000	noarch	1445355
VRTSsfmh	6.1.0.400	x86_64	43668551
VRTSspt	6.2.1.000	noarch	26316202
VRTSvcs	6.2.1.000	i686	64038472
VRTSvcsag	6.2.1.000	i686	12374192
VRTSvcsea	6.2.1.000	i686	256344

Table 1-2 RPMs for Red Hat Enterprise Linux 7 *(continued)*

Name	Version	Arch	Size in Bytes
VRTSvcsvmw	6.2.1.000	i686	8491964
VRTSvxfen	6.2.1.000	x86_64	2680044
VRTSvxfs	6.2.1.000	x86_64	7118208
VRTSvxvm	6.2.1.000	x86_64	35645800

Table 1-3 lists the SUSE Linux Enterprise Server 11 RPMs that are updated in this release.

Table 1-3 RPMs for SUSE Linux Enterprise Server 11

Name	Version	Arch	Size in Bytes
VRTSamf	6.2.1.000	x86_64	1634887
VRTSaslapm	6.2.1.000	x86_64	10410034
VRTScavf	6.2.1.000	i686	192061
VRTScps	6.2.1.000	i686	12342622
VRTSdbed	6.2.1.000	x86_64	56611623
VRTSfsadv	6.2.1.000	x86_64	3608862
VRTSgab	6.2.1.000	x86_64	1526238
VRTSllt	6.2.1.000	x86_64	3824380
VRTSperl	5.16.1.27	x86_64	15433706
VRTSsfcpi62	6.2.1.000	noarch	1445355
VRTSsfmh	6.1.0.400	x86_64	43668551
VRTSspt	6.2.1.000	noarch	26316206
VRTSvcs	6.2.1.000	i686	71724723
VRTSvcsag	6.2.1.000	i686	12736907
VRTSvcsea	6.2.1.000	i686	252019
VRTSvcsvmw	6.2.1.000	i686	8645861
VRTSvxfen	6.2.1.000	x86_64	1324945

Table 1-3 RPMs for SUSE Linux Enterprise Server 11 *(continued)*

Name	Version	Arch	Size in Bytes
VRTSvxfs	6.2.1.000	x86_64	8310191
VRTSvxvm	6.2.1.000	x86_64	87445165

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/TECH225259

- For the latest patches available for this release, go to:

  https://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/TECH211575

- The software compatibility list summarizes each Storage Foundation and High Availability (SFHA) Solutions product stack and the product features, operating system versions, and third-party products it supports. For the latest information on supported software, visit the following URL:

  http://www.symantec.com/docs/TECH225258

Note: Before you install or upgrade SFHA Solutions products, review the current compatibility lists to confirm the compatibility of your hardware and software.

Changes introduced in 6.2.1

This section lists the changes in Symantec Storage Foundation and High Availability Solutions 6.2.1.

Changes related to VCS

Symantec Cluster Server (VCS) includes the following changes in 6.2.1:

Btrfs support in Mount Agent

The Linux Mount agent is enhanced to support the Btrfs (B-tree file system) file system. With this enhancement, you now can use the VCS Mount Agent on the Linux platform to mount the btrfs file system.

Support for SAP ASE 16 in single instance mode

In this release, Symantec Cluster Server (VCS) is enhanced to support SAP ASE (previously Sybase) 16 in single instance mode.

Changes related to SF Sybase ASE CE

Symantec Storage Foundation for Sybase ASE CE (SFSYBASECE) includes the following changes in 6.2.1:

Support of SF Sybase ASE CE 15.7 on RHEL 6

SFHA Solutions 6.2.1 supports SF Sybase ASE CE 15.7 on RHEL 6.

Changes related to Veritas Volume Manager

Veritas Volume Manager (VxVM) includes the following changes in 6.2.1:

Remote Caching

Generally, SSDs are not put into every server in cluster, but you may like to use pool of available SSDs across all servers for caching purpose.

In this release, Remote Caching allows you to use SSDs from another node(s) for caching purpose. Flexible Storage Sharing (FSS) feature enables cluster-wide sharing of local storage through the use of a network interconnect among the nodes of the cluster. Integration of SmartIO and FSS feature allows you to utilize the SmartIO feature on node(s) in cluster, which doesn’t have locally attached SSDs.

RHEL 7.1 Support

In this release, SFHA Solutions 6.2.1 supports RHEL 7.1.

SUSE 12 Support

In this release, SFHA Solutions 6.2.1 supports SUSE 12.

GUI interface integration with the RHEV console

This Feature provides SF support to Red Hat Enterprise Virtualization as the storage backend.

RHEV GUI is a simple yet effective enhancement. It creates a tab in the RHEVM Web UI which further does the same set of operations provided by vxrhevadm, but it uses the single sign-on authentication to make REST API calls to SF objects with virtual machine. Operations supported are:

1. Attach
2. Detach
3. List

There is no need to configure host after the host-reboot. The permissions on the devices would be set automatically.

It supports boot device as SF device.

Changes related to Dynamic Multi-Pathing

Dynamic Multi-Pathing (DMP) includes the following changes in 6.2.1:

DMP support for NetApp Data On TAP 8.x cluster

In this release, DMP is enhanced to optimally support multi-controller (> 2 controllers) NetApp Data On TAP 8.x cluster mode configurations. This release addresses DMP limitations with supporting NetApp Data On TAP 8.x cluster mode configurations.

System requirements

Supported Linux operating systems

For current updates, visit the Symantec Operations Readiness Tools Installation and Upgrade page: https://sort.symantec.com/land/install_and_upgrade.

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

Table 1-4 Supported operating systems

Operating systems	Kernel version
Red Hat Enterprise Linux 6	Update 4 (2.6.32-358.el6) Update 5 (2.6.32-431.el6) Update 6 (2.6.32-504.el6)

Table 1-4 Supported operating systems *(continued)*

Operating systems	Kernel version
Oracle Linux 6 Unbreakable Enterprise Kernel 2 (UEK2)	2.6.39-400.17.1.el6uek **Note:** UEK 2 is supported only with Oracle Linux 6, Updates 4, 5, and 6.
Red Hat Enterprise Linux 7	3.10.0-123.el7
Red Hat Enterprise Linux 7.1	3.10.0-229.el7
SUSE Linux Enterprise 11	SP2 (3.0.13-0.27.1) SP3 (3.0.76-0.11.1)
Oracle Linux 7 (RHEL compatible mode)	3.10.0-123.el7
Oracle Linux 6 (RHEL Compatible mode)	Update 4 (2.6.32-358.el6) Update 5 (2.6.32-431.el6) Update 6 (2.6.32-504.el6)

Note: Oracle Linux 6 Unbreakable Enterprise Kernel v2 is supported with VCS only.

Note: SF Oracle RAC has not yet announced support for Oracle Linux 7. You may find information pertaining to OL 7 in the installation and administrator guides. Note that this information will become relevant only after SF Oracle RAC announces support when due certification efforts are complete. Refer to the following TechNote for the latest information on the supported operating systems and Oracle RAC database versions. http://www.symantec.com/docs/DOC4848

Note: Configuring LLT over RDMA is not supported with Oracle Linux Unbreakable Enterprise Kernel 2 (2.6.39-400.17.1.el6uek).

Note: All subsequent kernel versions and patch releases on the supported operating system levels are supported, but you should check the Symantec Operations Readiness Tools (SORT) website for additional information that applies to the exact kernel version for which you plan to deploy.

Note: Only 64-bit operating systems are supported on the AMD Opteron or the Intel Xeon EM64T (x86_64) Processor line.

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

Symantec supports only Oracle, Red Hat, and SUSE distributed kernel binaries.

For Storage Foundation for Oracle RAC, all nodes in the cluster need to have the same operating system version and update level.

Required Linux RPMs for SFHA Solutions

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

Note: Some required RHEL RPMs have different version numbers between RHEL update versions.

Table 1-5 lists the RPMs that SFHA Solutions products require for a given Linux operating system.

Table 1-5 Required RPMs

Operating system	Required RPMs
RHEL 7 **Note:** Symantec recommends that you install RHEL 7 as the operating system of Server GUI.	bc -1.06.95-13.el7.x86_64 coreutils-8.22-11.el7.x86_64 ed-1.9-4.el7.x86_64 findutils-4.5.11-3.el7.x86_64 gcc-c++-4.8.2-16.el7.x86_64 gcc-4.8.2-16.el7.x86_64 glibc-2.17-55.el7.i686 glibc-2.17-55.el7.x86_64 glibc-headers-2.17-55.el7.x86_64 glib-networking-2.36.2-3.el7.x86_64 glibmm24-2.36.2-4.el7.x86_64 glibc-common-2.17-55.el7.x86_64 glibc-devel-2.17-55.el7.x86_64 glibc-devel-2.17-55.el7.i686 glib2-2.36.3-5.el7.x86_64 glibc-utils-2.17-55.el7.x86_64 kmod-14-9.el7.x86_64 ksh-20120801-19.el7.x86_64

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
RHEL 7 (continued)	libacl-2.2.51-12.el7.i686 libacl-2.2.51-12.el7.x86_64 libaio-devel-0.3.109-12.el7.x86_64 libaio-devel-0.3.109-12.el7.i686 libaio-0.3.109-12.el7.i686 libaio-0.3.109-12.el7.x86_64 libgcc-4.8.2-16.el7.i686 libgcc-4.8.2-16.el7.x86_64 libstdc++-4.8.2-16.el7.i686 libstdc++-4.8.2-16.el7.x86_64 lsof-4.87-4.el7.x86_64 ncompress-4.2.4.4-3.el7.x86_64 ncurses-libs-5.9-13.20130511.el7.x86_64 nss-softokn-freebl-3.15.4-2.el7.i686 pam-1.1.8-9.el7.i686 parted-3.1-17.el7.x86_64 pcre-8.32-12.el7.i686 (pcre(x86-32)) policycoreutils-2.2.5-11.el7.x86_64 prelink-0.5.0-6.el7.x86_64 screen-4.1.0-0.19.20120314git3c2946.el7.x86_64 systemd-libs-208-11.el7.i686 systemd-libs-208-11.el7.x86_64 xz-libs-5.1.2-8alpha.el7.i686 (xz-libs(x86-32))

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
OL 7 **Note:** Symantec recommends that you install RHEL 7 as the operating system of Server GUI.	bc -1.06.95-13.el7.x86_64 coreutils-8.22-11.el7.x86_64 ed-1.9-4.el7.x86_64 findutils-4.5.11-3.el7.x86_64 gcc-c++-4.8.2-16.el7.x86_64 gcc-4.8.2-16.el7.x86_64 glibc-2.17-55.el7.i686 glibc-2.17-55.el7.x86_64 glibc-headers-2.17-55.el7.x86_64 glib-networking-2.36.2-3.el7.x86_64 glibmm24-2.36.2-4.el7.x86_64 glibc-common-2.17-55.el7.x86_64 glibc-devel-2.17-55.el7.x86_64 glibc-devel-2.17-55.el7.i686 glib2-2.36.3-5.el7.x86_64 glibc-utils-2.17-55.el7.x86_64 kmod-14-9.el7.x86_64 ksh-20120801-19.el7.x86_64

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
OL 7 (continued)	libacl-2.2.51-12.el7.i686 libacl-2.2.51-12.el7.x86_64 libaio-devel-0.3.109-12.el7.x86_64 libaio-devel-0.3.109-12.el7.i686 libaio-0.3.109-12.el7.i686 libaio-0.3.109-12.el7.x86_64 libgcc-4.8.2-16.el7.i686 libgcc-4.8.2-16.el7.x86_64 libstdc++-4.8.2-16.el7.i686 libstdc++-4.8.2-16.el7.x86_64 lsof-4.87-4.el7.x86_64 ncompress-4.2.4.4-3.el7.x86_64 ncurses-libs-5.9-13.20130511.el7.x86_64 nss-softokn-freebl-3.15.4-2.el7.i686 pam-1.1.8-9.el7.i686 parted-3.1-17.el7.x86_64 pcre-8.32-12.el7.i686 (pcre(x86-32)) policycoreutils-2.2.5-11.el7.x86_64 prelink-0.5.0-6.el7.x86_64 screen-4.1.0-0.19.20120314git3c2946.el7.x86_64 systemd-libs-208-11.el7.i686 systemd-libs-208-11.el7.x86_64 xz-libs-5.1.2-8alpha.el7.i686 (xz-libs(x86-32))

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
OL 6	coreutils-8.4-19.el6.x86_64.rpm ed-1.1-3.3.el6.x86_64.rpm findutils-4.4.2-6.el6.x86_64.rpm glibc-2.12-1.80.el6.i686.rpm glibc-2.12-1.80.el6.x86_64.rpm ksh-20100621-16.el6.x86_64.rpm libacl-2.2.49-6.el6.x86_64.rpm libgcc-4.4.6-4.el6.i686.rpm libgcc-4.4.6-4.el6.x86_64.rpm libstdc++-4.4.6-4.el6.i686.rpm libstdc++-4.4.6-4.el6.x86_64.rpm mksh-39-7.el6.x86_64.rpm module-init-tools-3.9-20.0.1.el6.x86_64.rpm ncurses-libs-5.7-3.20090208.el6.x86_64.rpm nss-softokn-freebl-3.12.9-11.el6.i686.rpm openssl-1.0.0-20.el6_2.5.x86_64.rpm pam-1.1.1-10.el6_2.1.i686.rpm parted-2.1-18.el6.x86_64.rpm perl-5.10.1-127.el6.x86_64.rpm policycoreutils-2.0.83-19.24.0.1.el6.x86_64.rpm readline-6.0-4.el6.x86_64.rpm

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
RHEL 6	coreutils-8.4-19.el6.x86_64.rpm ed-1.1-3.3.el6.x86_64.rpm findutils-4.4.2-6.el6.x86_64.rpm glibc-2.12-1.80.el6.i686.rpm glibc-2.12-1.80.el6.x86_64.rpm ksh-20100621-16.el6.x86_64.rpm libacl-2.2.49-6.el6.x86_64.rpm libgcc-4.4.6-4.el6.i686.rpm libgcc-4.4.6-4.el6.x86_64.rpm libstdc++-4.4.6-4.el6.i686.rpm libstdc++-4.4.6-4.el6.x86_64.rpm mksh-39-7.el6.x86_64.rpm module-init-tools-3.9-20.el6.x86_64.rpm ncurses-libs-5.7-3.20090208.el6.x86_64.rpm nss-softokn-freebl-3.12.9-11.el6.i686.rpm openssl-1.0.0-20.el6_2.5.x86_64.rpm pam-1.1.1-10.el6_2.1.i686.rpm parted-2.1-18.el6.x86_64.rpm policycoreutils-2.0.83-19.24.el6.x86_64.rpm readline-6.0-4.el6.x86_64.rpm zlib-1.2.3-27.el6.x86_64.rpm

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
SLES 11 SP2	coreutils-8.12-6.19.1.x86_64.rpm ed-0.2-1001.30.1.x86_64.rpm findutils-4.4.0-38.26.1.x86_64.rpm glibc-2.11.3-17.31.1.x86_64.rpm glibc-32bit-2.11.3-17.31.1.x86_64.rpm ksh-93u-0.6.1.x86_64.rpm libacl-2.2.47-30.34.29.x86_64.rpm libacl-32bit-2.2.47-30.34.29.x86_64.rpm libgcc46-32bit-4.6.1_20110701-0.13.9.x86_64.rpm libgcc46-4.6.1_20110701-0.13.9.x86_64.rpm libncurses5-5.6-90.55.x86_64.rpm libstdc++46-32bit-4.6.1_20110701-0.13.9.x86_64.rpm libstdc++46-4.6.1_20110701-0.13.9.x86_64.rpm module-init-tools-3.11.1-1.21.1.x86_64.rpm pam-32bit-1.1.5-0.10.17.x86_64.rpm parted-2.3-10.21.18.x86_64.rpm zlib-1.2.3-106.34.x86_64.rpm zlib-32bit-1.2.3-106.34.x86_64.rpm

Table 1-5 Required RPMs *(continued)*

Operating system	Required RPMs
SLES 11 SP3	coreutils-8.12-6.25.27.1.x86_64.rpm ed-0.2-1001.30.1.x86_64.rpm findutils-4.4.0-38.26.1.x86_64.rpm glibc-2.11.3-17.54.1.x86_64.rpm glibc-32bit-2.11.3-17.54.1.x86_64.rpm ksh-93u-0.18.1.x86_64.rpm libacl-2.2.47-30.34.29.x86_64.rpm libacl-32bit-2.2.47-30.34.29.x86_64.rpm libgcc_s1-32bit-4.7.2_20130108-0.15.45.x86_64.rpm libgcc_s1-4.7.2_20130108-0.15.45.x86_64.rpm libncurses5-5.6-90.55.x86_64.rpm libstdc++6-32bit-4.7.2_20130108-0.15.45.x86_64.rpm libstdc++6-4.7.2_20130108-0.15.45.x86_64.rpm module-init-tools-3.11.1-1.28.5.x86_64.rpm pam-32bit-1.1.5-0.10.17.x86_64.rpm parted-2.3-10.38.16.x86_64.rpm zlib-1.2.7-0.10.128.x86_64.rpm zlib-32bit-1.2.7-0.10.128.x86_64.rpm

Storage Foundation for Databases features supported in database environments

Storage Foundation for Databases (SFDB) product features are supported for the following database environments:

Table 1-6 SFDB features supported in database environments

Symantec Storage Foundation feature	DB2	Oracle	Oracle RAC	Sybase
Oracle Disk Manager	No	Yes	Yes	No
Cached Oracle Disk Manager	No	Yes	No	No
Concurrent I/O	Yes	Yes	Yes	Yes

Table 1-6 SFDB features supported in database environments *(continued)*

Symantec Storage Foundation feature	DB2	Oracle	Oracle RAC	Sybase
Storage Checkpoints	Yes	Yes	Yes	Yes
Flashsnap	Yes	Yes	Yes	Yes
SmartTier	Yes	Yes	Yes	Yes
Database Storage Checkpoints **Note:** Requires Enterprise license	Yes	Yes	Yes	No
Database Flashsnap **Note:** Requires Enterprise license	Yes	Yes	Yes	No
SmartTier for Oracle **Note:** Requires Enterprise license	No	Yes	Yes	No

Notes:

- SmartTier is an expanded and renamed version of Dynamic Storage Tiering (DST).
- Storage Foundation for Databases (SFDB) tools Database Storage Checkpoint, Database Flashsnap, and SmartTier for Oracle are supported with an Enterprise product license.

For the most current information on Storage Foundation products and single instance Oracle versions supported, see:

http://www.symantec.com/docs/DOC4039

Review the current Oracle documentation to confirm the compatibility of your hardware and software.

Symantec Storage Foundation memory requirements

Symantec recommends 2 GB of memory over the minimum requirement for the operating system.

Supported database software

For the latest information on supported database, see the following TechNote:http://www.symantec.com/docs/DOC4039

Additionally, see the following Oracle support site for information on patches that may be required by Oracle for each release.https://support.oracle.com

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/TECH211575

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

For information on specific HA setup requirements, see the *Veritas Cluster Server Installation Guide*.

Number of nodes supported

SFHA Solutions support cluster configurations with up to 64 nodes.

SmartIO writeback caching only supports cluster configurations with up to 2 nodes.

Fixed Issues

This section covers the fixed incidents.

See the `README_SYMC.`*`xxxxx-xx`* files in the /patches directory for the symptom, description, and resolution of the fixed issue.

- Installation and upgrade fixed issues
- Symantec Storage Foundation and High Availability fixed issues
- Symantec Storage Foundation for Databases (SFDB) tools fixed issues
- Symantec Cluster Server fixed issues
- Symantec Storage Foundation for Oracle RAC fixed issues
- Symantec Storage Foundation Cluster File System High Availability fixed issues
- Veritas File System fixed issues
- Veritas Volume Manager fixed issues
- Symantec ApplicationHA fixed issues
- Veritas Operations Manager fixed issues
- Cluster Volume Manager fixed issues
- Vxexplorer tool fixed issue

- LLT, GAB, and I/O fencing fixed issues

Installation and upgrade fixed issues

This section describes the incidents that are fixed related to installation and upgrades.

Installation and upgrade fixed issues in 6.2.1

Table 1-7 covers the incidents that are fixed related to installation and upgrade in 6.2.1.

Table 1-7 Installation and upgrade 6.2.1 fixed issues

Incident	Description
3656701	Oracle RAC supports IPv4 addresses only in Oracle High Availability IP (HAIP) configurations.
3719159	In Oracle RAC version 12.1.0.2, warning messages are reported during the post configuration checks.
3763571	The SFHA product installer reports incorrect minimal version for the required Oracle Linux 7 RPMs.
3739179	The module OpenSSL 1.0.1i in the VRTSperl package has security issues.

Installation and upgrade fixed issues in 6.2

Table 1-8 covers the incidents that are fixed related to installation and upgrade in 6.2.

Table 1-8 Installation and upgrade 6.2 fixed issues

Incident	Description
3182366	Adding a node to a cluster fails if you did not set up passwordless ssh or rsh.
2737124	If you upgrade the `VRTSvlic` RPM manually, the product levels that were set using `vxkeyless` may be lost. The output of the `vxkeyless display` command does not display correctly.
2141446	After upgrading from VCS 5.1 to higher versions of VCS, some keyless licenses may be left in the system. As a result periodic reminders get logged if Veritas Operations Manager Server is not configured.

Table 1-8 Installation and upgrade 6.2 fixed issues *(continued)*

Incident	Description
3224059	When you install VCS using vSphere Client menu, the menu shows a task that reads **ApplicationHA Installation**
3326196	Rolling upgrade may encounter a problem if open volumes from different disk groups have the same name.
3326639	CP server service group fails to come online with the default database path after the CP server is upgraded from 6.0 to 6.2 on a multi-node cluster.
3343592	`installer -license sys1` command does not show the check result if the system already has the SF Basic license key registered.
3442070	If you select rolling upgrade task from the Install Bundles menu, the Installer exits with an error.

Symantec Storage Foundation and High Availability fixed issues

This section includes issues fixed for Symantec Cluster Server, Veritas File System, and Veritas Volume Manager.

See "Symantec Cluster Server fixed issues" on page 29.

See "Veritas File System fixed issues" on page 37.

See "Veritas Volume Manager fixed issues" on page 43.

Symantec Storage Foundation for Databases (SFDB) tools fixed issues

This section describes fixed issues of Symantec Storage Foundation for Database (SFDB) tools.

Symantec Storage Foundation for Databases (SFDB) tools fixed issues in 6.2.1

Table 1-9 describes the Symantec Storage Foundation for Databases (SFDB) tools issues fixed in 6.2.1.

Table 1-9 SFDB tools 6.2.1 fixed issues

Incident	Description
3676518	For Oracle database 12.1.02 the new odm path is not being considered by dbed_codm_adm
3676521	dbed_codm_adm commands fail with an error when run as an Oracle user.

Symantec Storage Foundation for Databases (SFDB) tools fixed issues in 6.2

Table 1-10 describes the Symantec Storage Foundation for Databases (SFDB) tools issues fixed in 6.2.

Table 1-10 SFDB tools 6.2 fixed issues

Incident	Description
2869266	Checkpoint clone fails if the archive log destination is same as the datafiles destination.
3313775	SmartIO options are not restored after Reverse Resync Commit operation is performed.
3416155	The SFAE tools fail to perform with DB2 version 10.5.
3615735	During a Reverse Resync Begin operation, a mismatch in database control file version is observed.
3615745	For thin storage setups, the snapshot operation reports that the diskgroup cannot be split.
3199449	The dbed_clonedb(1M) command incorrectly allows the new clone to use other clone’s mount path.
3432740	DB2 checkpoint and flashSnap clone commands hang when the mirrorlogpath parameter is set.
3615764	The flashSnap operation fails to create a symlink on a Symantec Volume Replicator (VVR) secondary site.

Symantec Cluster Server fixed issues

This section describes Symantec Cluster Server fixed issues.

Symantec Cluster Server fixed issues in 6.2.1

Table 1-11 covers the fixed issues of Symantec Cluster Server in 6.2.1.

Table 1-11 Symantc Cluster Server 6.2.1 fixed issues

Incident	Description
3520211	The HostMonitor agent reports incorrect memory usage.
3652819	VxFS module fails to unload because the AMF module fails to decrement the reference count.
3662501	The notifier process fails to clearly distinguish whether the CPU, Memory, or Swap has exceeded the warning or critical threshold level.
3662508	The CmdServer log incorrectly reports warning messages relevant to licensing even when keyless licensing is enabled and the host is configured under Veritas Operations Manager (VOM).
3666049	VCS does not support SAP ASE 16 Sybase agent.
3668853	The halog(1M) command becomes unresponsive when VCS is in the REMOTE_BUILD state.
3699146	The Application agent reports an application resource as offline even when the resource is online.

Symantec Cluster Server fixed issues in 6.2

This section describes Symantec Cluster Server fixed issues in 6.2.

VCS engine fixed issues

Table 1-12 lists the fixed issues for VCS engine.

Table 1-12 VCS engine fixed issues

Incident	Description
3381042	The checkboot utility core dump or time difference between a system and Network Time Protocol (NTP) time leads to unexpected deletion of the temporary files. The deletion causes the VCS agents to report an incorrect state.
2834247	While initiating a global failover of multiple dependent service groups in a cluster, VCS fails to follow the group dependency order while initiating online of the service groups.

Table 1-12 VCS engine fixed issues *(continued)*

Incident	Description
3448510	The `hastatus` command fails and dumps core when it is run from a local zone.
3468891	Inconsistencies in `/etc/VRTSvcs/conf/attributes/cluster_attrs.xml` file and hide resource-level ContainerInfo attribute from `hares -display` command.
3211834	CurrentLimits attribute value is not updated correctly when a service group faults.
3385820	Sometimes the high availability daemon (HAD) crashes if it runs for a long duration.
3436617	When invoking triggers if some arguments are left unassigned, the `hatrigger` command fails due to compilation errors.
3471819	The service group fails to go online if the CurrentCount attribute value is incorrect.
3464981	The file size of Engine_A.log file could not be increased beyond 32 MB.
3580940	VCS configuration becomes unclean when incorrect filename is provided with the `ha` command for SourceFile attribute.
3603275	HAD and other nodes abort while shutting down two nodes simultaneously.

Bundled agents fixed issues

Table 1-13 lists the fixed issues for bundled agents.

Table 1-13 Bundled agents fixed issues

Incident	Description
2490296	Application agent cannot handle a case with user as root, envfile set and shell as `csh`.
2618482	Some agents may fail to come online after full upgrade to VCS 6.0 if they were online before the upgrade.
3354227	The clean entry point operation of the IPMultiNIC agent fails in the absence of a state file that contains current active device information.

Table 1-13 Bundled agents fixed issues *(continued)*

Incident	Description
3535942	The IP agent shows high CPU utilization and fails to stop even after VCS is stopped when IPv6 address is configured in the resource.
3408712	DiskGroup agent does not fail over the service group if storage connectivity is lost and I/O fencing is configured.
3573876	IP resource fails to go offline when network cable in unplugged.
3505202	VCS does not support non-default value for VCS_LOG environment variable.

Fixed issues related to AMF

Table 1-14 AMF fixed issues

Incident	Description
2848007	The libvxamf library encounters an error condition while doing a process table scan.
3333913	AMF may panic the system if it receives a request to unregister an already unregistered resource.
3407338	If one of the events of a group is in triggered state, then the group fails to unregister because of the triggered event.
3338946	Sometimes when a process offline registration is requested and the system is under heavy load, AMF library fails to verify whether the resource is actually offline. As a result, registration fails.

Symantec Storage Foundation for Oracle RAC fixed issues

This section describes the fixed issues of Symantec Storage Foundation for Oracle RAC.

Symantec Storage Foundation for Oracle RAC fixed issues in 6.2.1

There is no fixed issue for Symantec Storage Foundation for Oracle RAC in 6.2.1.

Symantec Storage Foundation for Oracle RAC fixed issues in 6.2

Table 1-15 lists the issues fixed in 6.2.

Table 1-15 Issues fixed in 6.2

Incident	Description
3321004	Installation of Oracle Clusterware using Oracle response file fails.
3348812	During HAIP configuration, the SF Oracle RAC web installer fails to update the /etc/hosts file with the HAIP alias.

Symantec Storage Foundation Cluster File System High Availability fixed issues

This section describes the fixed issues of Symantec Storage Foundation Cluster File System of High Availability.

Symantec Storage Foundation Cluster File System High Availability fixed issues in 6.2.1

This section lists the incidents that are fixed in Symantec Storage Foundation Cluster File System High Availability in 6.2.1.

See "Veritas File System fixed issues" on page 37.

See "Veritas Volume Manager fixed issues" on page 43.

Table 1-16 Symantec Storage Foundation Cluster File System High Availability 6.2.1 fixed issues

Incident	Description
3604071	High CPU usage consumed by the vxfs thread process.
3233276	With a large file system, primary to secondary migration takes longer duration.
3656155	Import of VxVM diskgroup triggered from CVMVolDg agent fails with error message.
3697141	Added support for Sles12
3737329	Added support for RHEL7.1
3513507	Filesystem umount() may hang due to deadlock in kernel
3702136	Link Count Table (LCT) corruption is observed while mounting a file system on a secondary node.
3633067	While converting from ext3 file system to VxFS using vxfsconvert, it is observed that many inodes are missing..

Table 1-16 Symantec Storage Foundation Cluster File System High Availability 6.2.1 fixed issues *(continued)*

Incident	Description
3757778	After executing the hastop -local command, the vxconfigd(1M) daemon is not accessible.
3760033	cfsshare command may report VCS error messages.

Symantec Storage Foundation Cluster File System High Availability fixed issues in 6.2

Table 1-17 lists the incidents that are fixed in Symantec Storage Foundation Cluster File System High Availability in 6.2.

See "Veritas File System fixed issues" on page 37.

See "Veritas Volume Manager fixed issues" on page 43.

Table 1-17 Symantec Storage Foundation Cluster File System High Availability 6.2 fixed issues

Incident	Description
3642894	VxFS agents for VCS should honor the customization of `VCS_LOG`.
3582470	Data change object (DCO) volume gets created using the same node's disks for both plexes.
3573908	Multiple `cbrbk.tmp$$` files in the /var/tmp folder on each node do not clean up properly.
3552008	The `vxconfigrestore` (vxvol resync) operation hangs on the master node while recovering a stripe-mirror volume.
3551050	The `vx*` commands are not able to connect to vxconfigd.
3547833	With Storage and I/Os from all three nodes, an I/O hang occurs.
3538683	After a master panic, the new master does not start plex resync when the older master comes online and joins the cluster.
3537519	The `vxdisk unexport` command hangs and then `vxconfigd` gets fault in an asymmetric array connection setup.
3534779	Internal stress testing on Cluster File System (CFS) hits a debug assert.
3528908	When the slave node contributing storage left the cluster, the `vxconfigd` command dumps core on the master node.

Table 1-17 Symantec Storage Foundation Cluster File System High Availability 6.2 fixed issues *(continued)*

Incident	Description
3523731	VxVM command check for device compliance prior to doing FSS operations on disks.
3517695	Storage failure in the FSS environment causes an I/O hang on all nodes.
3511444	Panics occur while checking memory pressure.
3508390	DCO object is unnecessarily marked BADLOG mode in cascade failure scenarios, and it results in requiring a full-recovery and can result in lost snapshots as well.
3505017	When the `da name` is the same as the existing `dm name`, the `vxdg addisk` operation from slave fails.
3496673	On a Flexible Storage Sharing (FSS) disk group, the read I/O performance is impacted.
3495811	When you create a disk group, the disk shows LMISSING state when the SCSI PGR operation fails.
3489167	Plex(es) on remote disks goes to DISABLED state because of a plex I/O error encountered after slave node reboot in cluster volume manger.
3484570	Accessing CVM message after decrementing reference count causes a panic.
3449152	The `vxtunefs`(1M) command fails to set the `thin_friendly_alloc` tunable in cluster file systems.
3444771	Internal noise test on cluster file system hits an debug assert when you are creating a file.
3430256	Space allocation for Volume: Single DAS disk in a disk group takes more preference than shared storage in that disk group.
3422704	Unique prefix generation algorithm redesign for forming cluster wide consistent name (CCN).
3411438	The `preferred` and `round-robin` read policy settings should be honoured irrespective of local connectivity to the plexes.
3394940	Anomaly numbers are displayed in the `vxstat` output.
3383625	When a cluster node that contributes the storage to the Flexible Storage Sharing (FSS) disk group rejoins the cluster, the local disks brought back by that node do not get reattached.

Table 1-17 Symantec Storage Foundation Cluster File System High Availability 6.2 fixed issues *(continued)*

Incident	Description
3373747	Adding new nodes to the 22-node cluster causes Cluster File System (CFS) failures after CVM deletes 2 nodes.
3370753	Internal tests with SmartIO writeback SSD cache hit debug asserts.
3370722	Operating system (OS) installation on virtual machines fails in two-node clusters with writeback caching enabled.
3329603	The `vxconfigd` related error messages are observed in system log files on every node for large cluster setups.
3301085	The `vxdg adddisk` operation fails when adding nodes containing disks with the same name.
3300418	VxVM volume operations on shared volumes cause unnecessary read I/Os.
3286030	Vxattachd debug messages get displayed on the console during a reboot.
3283518	Disk group deport operation reports messages in the syslog for remote disks.
3283418	Remote writes hang due to heavy sync workload on the target node in FSS environments.
3281160	When autoreminor is set off, no error is thrown when you import a disk group having the same minor number as that of the existing imported disk group.
3214542	Disk group creation or addition of a new disk to an existing disk group fails with "VxVM vxdg ERROR V-5-1-16087 Disk for disk group not found" error when the command is executed from the slave node.
3213411	A node join fails if a "disabled" Flexible Storage Sharing disk group exists in the cluster.
3198590	SmartIO VxVM caching is not supported for CFS.
3191807	CVM requires the T10 vendor provided ID to be unique.
3152304	When connectivity to some of the plexes of a volume is lost from all nodes, an I/O hang occurs.
3142109	The CFSMountAgent script does not parse the `MountOpt` properly if the `-O` overlay (native fs option) is used.

Table 1-17 Symantec Storage Foundation Cluster File System High Availability 6.2 fixed issues *(continued)*

Incident	Description
3117153	Disk group remains in deported state for remote disks after destroying the disk group from a node that is not exporting the disks.

3093407	When one host name in a cluster is a substring of other host name, with the superstring differentiated by a hyphen – for example, `abc` and `abc-01` – the `cfsmnatadm` utility may throw an error for some commands as follows:
	`# ` **`cfsmntadm modify /swapmnt/ add abc="rw"`**
	`  Nodes are being added...`
	`  Error: V-35-117: abc already associated with cluster-mount /`
	`  Nodes added to cluster-mount /swapmnt`
	`#`

3079819	`vxconfigbackup` fails on Flexible Storage Sharing disk groups.
1203819	In some cases, inode and allocation maps inconsistencies occur in the event of a node crash in clusters.
640213	The node panics in case of overlapping reconfigurations due to race conditions.

Veritas File System fixed issues

This section describes the fixed issues of Veritas File System.

Veritas File System fixed issues in 6.2.1

Table 1-18 lists the incidents that are fixed in Veritas File System (VxFS) in 6.2.1.

Table 1-18 Veritas File System 6.2.1 fixed issues

Incident	Description
2059611	The system panics due to a NULL pointer dereference while flushing bitmaps to the disk.
2439261	When the vx_fiostats_tunable value is changed from zero to non-zero, the system panics.
2919310	During stress testing on cluster file system, an assertion failure was hit because of a missing linkage between the directory and the associated attribute inode.

Table 1-18 Veritas File System 6.2.1 fixed issues *(continued)*

Incident	Description
3093821	The system panics due to referring freed super block after the vx_unmount() function errors.
3269553	VxFS returns inappropriate message for read of hole via Oracle Disk Manager (ODM).
3567027	During the File System resize operation, the "fullfsck flag is set.
3594386	On RHEL6u5, stack overflows lead to system panic.
3601943	Truncating corrupted block map of a file may lead to an infinite loop.
3602322	Panic while flushing the dirty pages of the inode
3604750	The kernel loops during the extent re-org.
3615043	Data loss when writing to a file while dalloc is on.
3616907	System is unresponsive causing the NMI watchdog service to stall.
3617191	Checkpoint creation takes a lot of time.
3621205	OpenSSL common vulnerability exposure (CVE): POODLE and Heartbleed.
3622323	Cluster Filesystem mounted as read-only panics when it gets sharing and/or compression statistics with the fsadm_vxfs(1M) command.
3622326	During a checkpoint promote, a file system is marked with a fullfsck flag because the corresponding inode is marked as bad.
3637636	Cluster File System (CFS) node initialization and protocol upgrade may hang during the rolling upgrade.
3767771	CVMVOLDG agent does not deport shared disk groups when these disks go into the disable state.
3642314	Umount operation reports error code 255 in case of write-back cache.
3682138	The VxVM symbols are released before the VxFS modules unload time.
3685391	Execute permissions for a file not honored correctly.
3690078	The system panics at vx_dev_strategy() routine due to stack overflow.
3697964	The vxupgrade(1M) command fails to retain the fs_flags after upgrading a file system.

Table 1-18 Veritas File System 6.2.1 fixed issues *(continued)*

Incident	Description
3709947	The SSD cache fails to go offline due to additional slashes "//" in the dev path of the cache device.
3710792	Unmount fails when the mount point contains a special character(colon).
3715566	VxFS fails to report an error when the maxlink and nomaxlink options are set on file systems having disk layout version (DLV) lower than 10.
3719523	'vxupgrade' retains the superblock replica of old layout versions.
3721466	After a file system is upgraded from version 6 to 7, the vxupgrade(1M) command fails to set the VX_SINGLEDEV flag on a superblock.
3723336	On RHEL 6.6, umount(8) system call hangs if an application is watching for inode events using inotify(7) APIs.
3727165	Enhance RHEV support for SF devices for identification in Guest
3729030	The fsdedupschd daemon failed to start on RHEL7.
3739618	sfcache command with "-i" option maynot show filesystem cache statistic periodically.
3743912	Users could create sub-directories more than 64K for disk layouts having versions lower than 10.
3744424	OpenSSL common vulnerability exposure (CVE): POODLE and Heartbleed.
3750187	Internal noise testing hits debug assert.
3756750	VxFS may leak memory when File Design Driver (FDD) module is unloaded before the cache file system is taken offline.

Veritas File System fixed issues in 6.2

Table 1-19 lists the incidents that are fixed in Veritas File System (VxFS) in 6.2.

Table 1-19 Veritas File System 6.2 fixed issues

Incident	Description
3641719	The `fallocate` may allocate a highly fragmented file when the size of the file is extremely large.

Table 1-19 Veritas File System 6.2 fixed issues *(continued)*

Incident	Description
3613048	VxFS does not correctly support IOCB_CMD_PREADV and IOCB_CMD_PREADV, which causes an error in the kernel code. Now the support for the vectored Asynchronous I/O commands is added to fix this issue.
3597482	The `pwrite(2)` function fails with the `EOPNOTSUPP` error.
3589264	The `fsadm` command shows an incorrect option for the file system type in usage.
3564076	The MongoDB noSQL database creation fails with an `ENOTSUP` error.
3563796	The file system `fullfsck` flag is set when the inode table overflows.
3560968	The `delicache_enable` tunable is not persistent in the Cluster File System (CFS) environment.
3560187	The kernel may panic when the buffer is freed in the `vx_dexh_preadd_space()` function with the message `Data Key Miss Fault in kernel mode`.
3557009	Run the `fallocate` command with `-l` option to specify the length of the reserve allocation. The file size is not expected, but multiple of file system block size.
3550103	After you upgrade or restart the system, mismatch in SSD cache usage may occur.
3523316	The writeback cache feature does not work for write size of 2MB.
3520349	When there is a huge number of dirty pages in the memory, and a sparse write is performed at a large offset of 4 TB or above on an existing file that is not null, the file system hangs
3506485	The code is modified to not allow writeback caching on a volume with Veritas Volume Replicator (VVR) enabled.
3486726	Veritas File Replicator (VFR) logs too much data on the target node.
3484336	The `fidtovp()` system call can panic in the `vx_itryhold_locked()` function.
3478017	Internal tests found assert in voprwunlock
3473390	The multiple stack overflows with Veritas File System (VxFS) on Red Hat Enterprise Linux (RHEL) 6 lead to panics or system crashes.

Table 1-19 Veritas File System 6.2 fixed issues *(continued)*

Incident	Description
3471245	The `mongodb` fails to insert any record.
3469644	The system panics in the `vx_logbuf_clean()` function.
3466020	The file system is corrupted with the error message `vx_direrr: vx_dexh_keycheck_1`.
3463464	Internal kernel functionality conformance tests hit a kernel panic due to null pointer dereference.
3457803	The file system gets disabled intermittently with metadata I/O errors.
3451284	While allocating extents during the write operation, if summary and bitmap data for file system allocation units get mismatched, a full `fsck` flag get set on the file system.
3449150	The `vxtunefs`(1M) command accepts garbage values for certain tunables.
3448702	Checkpoint creation of different file systems may get serialized.
3444775	Internal noise testing on cluster file system results in a kernel panic in `vx_fsadm_query()` function with an error message.
3444154	Reading from a de-duped file-system over NFS can result in data corruption seen on the NFS client.
3436326	The attribute validation (pass 1d) of the `full fsck` operation takes too much time to complete.
3434811	The `vxfsconvert`(1M) command in VxFS 6.1 hangs.
3430461	The nested unmounts fail if the parent file system is disabled.
3424564	`fsppadm` fails with `ENODEV` and `file is encrypted or is not a database` errors.
3417076	The `vxtunefs`(1M) command fails to set tunables when the file contains blank lines or white spaces.
3415639	The type of the `fsdedupadm`(1M) command always shows as MANUAL even when it is launched by the `fsdedupschd` daemon.
3412667	The RHEL 6 system panics with a stack overflow.
3394803	A panic is observed in the VxFS routine `vx_upgrade7`() function while running the `vxupgrade` command (1M).

Table 1-19 Veritas File System 6.2 fixed issues *(continued)*

Incident	Description
3370727	Internal tests with SmartIO writeback SSD cache hit debug asserts.
3356947	When there are multi-threaded writes with `fsync` calls between them, VxFS becomes slow.
3352883	During the rename operation, many nfsd threads hang.
3340286	After a file system is resized, the tunable setting `dalloc_enable` is reset to a default value.
3337806	The `find`(1) command may panic the systems with Linux kernels with versions greater than 3.0.
3335272	The `mkfs` (make file system) command dumps core when the log size provided is not aligned.
3332902	While shutting down, the system running the `fsclustadm`(1M) command panics.
3323866	Some Object Data Manager (ODM) operations fail with `ODM ERROR V-41-4-1-328-22 Invalid argument`.
3317368	File system operations needing a file system freeze may take longer in the presence of file level snapshots and when there is a heavy I/O load.
3301716	In a Veritas File System (VxFS), if a file system has compression enabled, the file system gets disabled due to the ENOSPC error. This occurs because of a defect in the delayed allocation feature.
3297840	VxFS corruption is detected during a dynamic LUN resize operation.
3294074	The `fsetxattr()` system call is slower on the Veritas File System (VxFS) than on the ext3 file system.
3285927	The `vfradmin` command does not validate job and consistency group names. It displays an improper error `Stale NFS file handle` for invalid job/consistency group.
3264062	The allocated space may be leaked from the free space while you are unsharing shared extents.
3121933	There is a DB2 crash or corruption when `EOPNOTSUPP` is returned from VxFS.

Veritas Volume Manager fixed issues

This section describes the incidents that are fixed in Veritas Volume Manager (VxVM).

Veritas Volume Manager fixed issues in 6.2.1

Table 1-20 lists the incidents that are fixed in Veritas Volume Manager (VxVM) in 6.2.1.

Table 1-20 Veritas Volume Manager 6.2.1 fixed issues

Incident	Description
2965910	Volume creation with the vxassist(1M) command dumps core when the non-disk parameters are specified along with the '-o ordered' option.
3322760	"vxdisk list" command may list detached disks, if the options are fullshared, partialshared, or local.
3414023	If a volume has preexisting snapshots, reattaching a detached plex would resync the extra data.
3420347	Write errors occur with "vxdg flush" running.
3496077	The vxvmconvert(1m) command fails with an error message while converting Logical Volume Manager (LVM) Volume Groups (VG) into VxVM disk group.
3506450	When migrating from PowerPath to Dynamic Multipathing (DMP), you may observe a system panic or VxVM configuration daemon (vxconfigd) core.
3518470	The 'vxdg adddisk' command fails with the following message: "*disk name* previous removed using -k option" Even though the disk was not removed using the -k option.
3564260	VVR commands are unresponsive when replication is paused and resumed in a loop.
3571434	DMP does not support NetApp cDOT cluster mode array with more than 2 nodes.
3588012	The vxconfigd(1M) daemon experiences a memory leak while printing I18N messages.
3594158	The spinlock and unspinlock are referenced to different objects when interleaving with a kernel transaction.

Table 1-20 Veritas Volume Manager 6.2.1 fixed issues *(continued)*

Incident	Description
3599977	During a replica connection, referencing a port that is already deleted in another thread causes a system panic.
3605036	VxDMP may fail to stop when Storage Foundation (SF) stop command is executed.
3616671	The number of transaction log files is reset to default value 10, even though it is explicitly set to the no_limit value.
3621232	The vradmin ibc command cannot be started or executed on Veritas Volume Replicators (VVR) secondary node.
3625890	vxdisk resize operation on CDS disks fails with an error message of "Invalid attribute specification"
3628860	The vxdisk(1M) command shows disks with status as nolabel in the outputs.
3628933	Volumes remain in the DETACHED state, even after nodes with storage join back to the cluster.
3631025	The I/O statistics derived using the vxstat utility with "-ft" or "-fi" options along with -i option do not provide the system name and its origin (source or destination).
3631989	The vxconfigd(1M) daemon becomes unresponsive on the joiner node.
3631990	VxVM fails to recognize iSCSI LUNs after a system restart.
3643910	The Intel NVMe ASL does not claim the devices with namingschme set to osn.
3644687	In a Veritas Volume Replicator (VVR) environment, any node on the Primary cluster may panic during the I/O error handling.
3645370	vxevac command fails to evacuate disks with Dirty Region Log(DRL) plexes.
3646712	The Huawei ASL sometimes skips claiming a path to a disk as it identifies it incorrectly as a command device.
3648719	The server panics while adding or removing LUNs or HBAs.
3651034	Temporary loss of storage results in application I/O failure.
3656539	I/O may hang when SmartIO VxVM block level is configured in only few nodes of cluster, while there are volumes with instant snapshots.

Table 1-20 Veritas Volume Manager 6.2.1 fixed issues *(continued)*

Incident	Description
3662392	In the Cluster Volume Manager (CVM) environment, if I/Os are getting executed on slave node, corruption can happen when the vxdisk resize(1M) command is executing on the master node.
3662845	Provide a UI plugin for supporting SF storage to virtual machines on Red Hat Enterprise Virtualization.
3665644	The system panics due to an invalid page pointer in the Linux bio structure.
3669863	"sfcache list" command doesn't show storage devices in the output if "cachearea" is created on stripe-mirror volume.
3671975	The system panics when Veritas Volume manager (VxVM) cachearea is configured in Cluster Volume Manager (CVM).
3672759	The vxconfigd(1M) daemon may core dump when DMP database is corrupted.
3674614	Restarting the vxconfigd(1M) daemon on the slave (joiner) node during node-join operation may cause the vxconfigd(1M) daemon to become unresponsive on the master and the joiner node.
3682651	Vxdiskunsetup fails with error "VxVM ERROR V-5-7-0 Can't find.
3688156	The output of vxdisk -o local|partialshared list command lists disks in the error state.
3697095	With root disk encapsulated or DMP Native Support set to on, and if ASLAPM is installed or upgraded, the old Array Support Library (ASL)/ Array Policy Module (APM) files and keys are used after a reboot.
3702387	The auto-mount operation corresponding to the fstab entry of (VxFS formatted VxVM) volume fails during the system startup in the systemd environment.
3719478	ZFS zpool auto LUN expansion is not detected when dmp_native_support is enabled.
3724580	Due to stale VxDMP devices mounted on partitions, the vxdmpadm settune dmp_native_support=on tunable reports an error.
3728181	The VRTSvxvm package fails to upgrade from VxVM 6.2 or uninstall due to an error reported while loading or unloading the VxDMP module.
3736515	VxVM disk group creation may fail with SCSI-3 Persistent Reservation (PR) errors on STEC SSD DAS devices.

Table 1-20 Veritas Volume Manager 6.2.1 fixed issues *(continued)*

Incident	Description
3749557	System hangs because of high memory usage by vxvm.

Veritas Volume Manager fixed issues in 6.2

Table 1-21 lists the incidents that are fixed in Veritas Volume Manager (VxVM) in 6.2.

Table 1-21 Veritas Volume Manager fixed issues

Incident	Description
3584341	The `vxdmpadm listapm` command prints error message VxVM ERROR V-5-2-14196.
3584311	The vxconfigd daemon hangs with "vol_rv_transaction_prepare+0005C8" on secondary site.
3580962	A panic occurs in VxDMP under high I/O load, and may cause complete storage disconnection.
3577957	Database instance is terminated while rebooting a node.
3567823	System reboot causes all PP_EMC devices to be lost if DMP devices are excluded.
3566493	Orphan cpmap objects cannot be removed after you disassociate unfinished snap plexes.
3555230	The `vxconfigd` daemon hangs in Veritas Volume Replicator (VVR) when writing to SRL volume during replication.
3554608	Mirroring a volume creates a larger plex than the original on a CDS disk.
3544972	620:dmp:coredump while rebooting the OS after dmp installation.
3542272	The `vxconfigbackupd` daemon never exits after reboot. The daemon remains active for a disk group because configuration has been changed after the backup is initiated.
3539548	Duplicate disks and I/O error occurs after dynamic LUN allocation.
3521726	When using Symantec Replication Option, system panics happens due to double freeing IOHINT memory.
3513392	Secondary panics when rebooted while heavy IOs are going on primary.

Table 1-21 Veritas Volume Manager fixed issues *(continued)*

Incident	Description
3503852	With multiple Replicated Volume Groups (RVGs), if you detach storage on a secondary master then reattach it back, rlinks are not able to connect. The rlink state is different on one of the three rlinks. .
3498228	The `vxconfigd` core dump occurs after port disable or enable operation with migration from PP to DMP.
3495553	DV:6.1 The `vxconfigd` daemon hangs on secondary in vol_ru_transaction_prepare.
3490458	After managing class under PP, some of the devices are seen in error state.
3489572	Slave nodes panic when volume with DCO hits storage failure while volume is online.
3482026	The `vxattachd`(1M) daemon reattaches plexes of manually detached site.
3478019	When VxVM fails to assign a unique name to a new DCL volume, the `vxsnap prepare` command fails silently without giving an error.
3466160	DMP does not coexist with `scsi_dh_emc` module on SLES11.
3456153	When Veritas Volume Replicator (VVR) replication is in progress, a Cluster Volume Manager (CVM) slave node reboot causes an I/O hang.
3455460	The `vxfmrshowmap` and the `verify_dco_header` utilities fail.
3450758	The slave node was not able to join CVM cluster and resulted in panic.
3446415	A pool may get added to the file system when the file system shrink operation is performed on FileStore.
3440790	The `vxassist` command with parameter mirror and the vxplex command(1M) with parameter att hang.
3433503	Due to an incorrect memory access, the `vxconfigd` daemon cores with a stack trace.
3428025	When heavy parallel I/O load is issued, the system that runs Symantec Replication Option (VVR) and is configured as VVR primary crashes.
3417044	System becomes unresponsive while creating a VVR TCP connection.
3415188	I/O hangs during replication in Veritas Volume Replicator (VVR).
3411668	Network and host endian difference is not handled in the nmcom_print_sock_storage() function.

Table 1-21 Veritas Volume Manager fixed issues *(continued)*

Incident	Description
3403390	After a crash, the linked-to volume goes into NEEDSYNC state.
3399131	For PowerPath (PP) enclosure, both DA_TPD and DA_COEXIST_TPD flags are set.
3390162	nmap scanning UDP port 4145 will cause vxnetd to consume 100% CPU and rlink disconnection resulting in system hangs.
3385905	Data corruption occurs after VxVM makes cache area offline and online again without a reboot.
3385753	Replication to the Disaster Recovery (DR) site hangs even though Replication links (Rlinks) are in the connected state.
3380481	When you select a removed disk during the "5 Replace a failed or removed disk" operation, the vxdiskadm(1M) command displays an error message.
3374200	A system panic or exceptional IO delays are observed while executing snapshot operations, such as, refresh.
3368361	When siteconsistency is configured within a private disk group (with LUNs mapped only to local server) and CVM is up, then the reattach operation of a detached site fails.
3336714	The slab of I/O request in Linux may get corrupted.
3326964	VxVM hangs in Clustered Volume Manager (CVM) environments in the presence of FMR operations.
3317430	The `vxdiskunsetup` utility throws error after upgrade from 5.1SP1RP4.
3287940	LUNs from any EMC CLARiiON arrays that have Not Ready state are shown in the "online invalid" state by Veritas Volume Manager (VxVM).
3279932	The `vxdisksetup` and `vxdiskunsetup` utilities fail for disks that are part of a deported disk group, even if "-f" option is specified.
	Heavy I/O loads on primary sites result in transaction/session timeouts between the primary and secondary sites.
3133854	SmartIO cache area does not come online after I/O error to the disk.
3124698	VxDMP memory allocation mechanism affects system performance, due to excessive swapping.

Table 1-21 Veritas Volume Manager fixed issues *(continued)*

Incident	Description
2882312	If an SRL fault occurs in the middle of an I/O load, and you immediately issue a read operation on data written during the SRL fault, the system returns old data.
2573229	On RHEL6, the server panics when DMP executes PERSISTENT RESERVE IN command with REPORT CAPABILITIES service action on powerpath controlled device.
2049371	DMP behavior on Linux SLES11 when connectivity to a path is lost.
1390029	The `vxconfigrestore` command fails when there is a dot in the disk group name, i.g., test.2

Symantec ApplicationHA fixed issues

This section describes the fixed issues of Symantec ApplicationHA.

Symantec ApplicationHA 6.2.1 fixed issues

Table 1-22 lists the fixed issue for Symantec ApplicationHA in 6.2.1.

Table 1-22 Symantec ApplicationHA 6.2.1 fixed issues

Incident	Description
3640275	ApplicationHA fails to exit maintenance mode and resume application monitoring

Symantec ApplicationHA 6.2 fixed issues

Table 1-23 describes the issues fixed in Symantec ApplicationHA 6.2.

Table 1-23 Symantec ApplicationHA 6.2 fixed issues

Incident number	Description
3335745	While upgrading ApplicationHA, the install program does not provide users with the option to specify keyless licensing.
3491170	ApplicationHA installer displays incorrect EULA path for non-English locales

Table 1-23 Symantec ApplicationHA 6.2 fixed issues *(continued)*

Incident number	Description
3491158	If you have configured Oracle database instances for detail monitoring with ApplicationHA 6.0 or earlier, you cannot perform a live upgrade to ApplicationHA 6.1.
3292905 and 3402560	If you use ApplicationHA to monitor multiple applications (component groups) on a virtual machine, and one application develops a fault, ApplicationHA restarts the faulted application. However, meanwhile, the VMWAppMonHB agent may start taking other healthy applications offline.
3536489	If you install ApplicationHA guests components from the VMware vSphere Client menu, the installer may not perform a pre-install check for ksh RPMs.

Symantec Dynamic Multi-Pathing fixed issues

This section describes the fixed issues of Symantec Dynamic Multi-Pathing (DMP) in this release.

Dynamic Multi-Pathing fixed issues in 6.2.1

There is no fixed issue in 6.2.1.

Dynamic Multi-Pathing fixed issues in 6.2

Table 1-24 lists the fixed issues for Dynamic Multi-Pathing 6.2.

Table 1-24 Dynamic Multi-Pathing 6.2 fixed issues

Incident	Description
3577586	Server panic while sending SCSI pkt from DMP.
3565212	IO failure during controller giveback operations on Netapp FAS31700 in ALUA mode.
3543284	FIO device not visible.
3542713	vxdmpadm listenclosure all displays a different ENCL from array console/VOM.
3531385	Asynchronous access to per dmpnode request queues may cause system panic.

Table 1-24 Dynamic Multi-Pathing 6.2 fixed issues *(continued)*

Incident	Description
3526500	DMP I/O getting timeout lot earlier than 300 seconds if I/O statistics daemon is not running.
3520991	vxconfigd core dumps during vxdisk scandisks.
3502923	ESX panic while running add/remove devices from smartpool with no license installed on server.
3399323	The reconfiguration of DMP DB failed.
3373208	DMP wrongly sends APTPL bit 0 to array.

Veritas Operations Manager fixed issues

This section describes the incidents that are fixed related to Veritas Operations Manager (VOM).

Veritas Operations Manager fixed issues in 6.2.1

Table 1-25 covers the incidents that are fixed related to Veritas Operations Manager (VOM) in 6.2.1.

Table 1-25 Veritas Operations Manager fixed issues in 6.2.1

Incident	Description
3517052	mismatch between VOM and Sort for SPVU calculation.
3526358	VOM 6.0 statistics 'Live' option shows incorrect 'free memory'.
3526792	VOM doesn't display RVG and host relationships properly in CVR environment.
3554764	Disk type resources from CVM were being shown twice in VOM availability perspective.
3558088	Switch configuration fails if password has single quotes (').
3560777	Issues with disk discovery when LUNZ devices are present.
3563150	VVR RVGs displayed on the wrong host in CMS Console with host aliasing.
3576824	vxdclid is opening too many file descriptors.
3577772	Layout is not displayed for volumes created by LVM.

Table 1-25 Veritas Operations Manager fixed issues in 6.2.1 *(continued)*

Incident	Description
3585566	Keyless License not detected.
3593632	Base Release displays Incorrect for SFHA-RHEL6_x86_64-6.2.
3615769	Add host failing with MH having english-UK locale.
3629745	VxFS file system report usage is not getting updated, reports are incorrect.
3636983	VOM 6.1 shows mh status as "Not Installed"
3642699	Set credential operation for secure databases fails.
3651166	VOM console sees Solaris 11 SFHA 6.1.1 as 6.1
3658760	Failed to remove MHs from VOM GUI and vomadm cli with --force
3663528	xprtld daemon cannot be started after install on RHEL 7.
3671234	HBA vendor name discovery corrupts the SF family sfm.dump and this results in filling up DB logs with error messages.
3688166	Adding host fails in VOM 6.1.

Veritas Operations Manager fixed issues in 6.2

There is no fixed issue for Veritas Operations Manager fixed issues in 6.2.

Cluster Volume Manager fixed issues

Table 1-26 describes the incidents that are fixed in Cluster Volume Manager (CVM) in 6.2.

Table 1-26 Cluster Volume Manager 6.2 fixed issues

Incident	Description
640213	The node panics in case of overlapping reconfigurations due to race conditions.
3592783	For the FSS partially shared storage configuration, after you run `hastop -all` and then `hastart`, remote disks, which are not part of the disk group, are not visible in `vxdisk -o alldgs list`.

Table 1-26 Cluster Volume Manager 6.2 fixed issues *(continued)*

Incident	Description
2705055	The `preferred` and `round-robin` read policy settings should be honoured irrespective of local connectivity to the plexes.

Vxexplorer tool fixed issue

This section describes the incidents that are fixed related to vxexplorer tool fixed issue.

Vxexplorer tool fixed issue in 6.2.1

Table 1-27 covers the incidents that are fixed related to vxexplorer tool fixed issue in 6.2.1.

Table 1-27 vxexplorer tool fixed issue in 6.2.1

Incident	Description
3739942	On Veritas Support Package 6.2.0, for vxexplorer, an End of Service Life (EOSL) message is displayed in error..

Vxexplorer tool fixed issue in 6.2

There is no fixed issue for Vxexplorer tool fixed issue in 6.2.

LLT, GAB, and I/O fencing fixed issues

This section describes the fixed issues of LLT, GAB and I/O fencing.

LLT, GAB, and I/O fencing fixed issues in 6.2.1

Table 1-28 lists the fixed issues for LLT, GAB, and I/O fencing in 6.2.1.

Table 1-28 LLT, GAB, and I/O fencing 6.2.1 fixed issues

Incident	Description
3567354	The Linux kernel panics when it receives a shared non-linear skb for linearization from the Low Latency Transport (LLT).
3663740	In a rare scenario, divide by zero error is seen when lltshow -p command is run.

Table 1-28 LLT, GAB, and I/O fencing 6.2.1 fixed issues *(continued)*

Incident	Description
3667755	Strict permission check for CPS configuration files.
3691202	Sometimes fencing in the customized mode fails to start when the number of files present in the current working directory is large.
3722178	The rpm --verify command on VXFEN changes the runlevel settings for the VXFEN service.
3728106	On Linux, the value corresponding to 15 minute CPU load average as shown in /proc/loadavg file wrongly increases to about 4.

LLT, GAB, and I/O fencing fixed issues in 6.2

Table 1-29 lists the fixed issues for LLT, GAB, and I/O fencing in 6.2.

Table 1-29 LLT, GAB, and I/O fencing fixed issues

Incident	Description
3335137	Fencing configuration fails if SysDownPolicy is set to AutoDisableNoOffline in online service groups.
3473104	When virtual NICs are configured under LLT without specifying the MTU size 1500 in llttab, cluster does not function properly. For example, VCS engine commands may hang and print below message in the engine logs: `VCS CRITICAL V-16-1-51135 GlobalCounter not updated`
3031216	The dash (-) in a disk group name causes vxfentsthdw(1M) and Vxfenswap(1M) utilities to fail.
3471571	Cluster nodes may panic if you stop the HAD process by force on a node and reboot that node.
3410309	LLT driver fails to load and logs the following message in the syslog when a mismatch is observed in the RDMA-specific symbols. llt: disagrees about version of symbol rdma_connect llt: Unknown symbol rdma_connect llt: disagrees about version of symbol rdma_destroy_id llt: Unknown symbol rdma_destroy_id
3532859	The Coordpoint agent monitor fails if the cluster has a large number of coordination points.

Known issues

This section covers the known issues in this release.

- Issues related to installation and upgrade
- Symantec Storage Foundation known issues
- Symantec Storage Foundation and High Availability known issues
- Symantec Cluster Server known issues
- Symantec Dynamic Multi-Pathing known issues
- Symantec Storage Foundation Cluster File System High Availability known issues
- Symantec Storage Foundation for Oracle RAC known issues
- Symantec Storage Foundation for Databases (SFDB) tools known issues
- Symantec Storage Foundation for Sybase ASE CE known issues
- Symantec ApplicationHA known issues
- LLT known issues
- I/O fencing known issues
- GAB known issues

Issues related to installation and upgrade

This section describes the known issues during installation and upgrade.

During an upgrade process, the AMF_START or AMF_STOP variable values may be inconsistent [3763790]

If the value of AMF_START or AMF_STOP variables in the driver configuration file is ‘0’ before an upgrade, then after the upgrade is complete, the installer changes the value to 1. Simultaneously, the installer also starts the Asynchronous Monitoring Framework (AMF) process.

Workaround: To resolve the issue, stop the AMF process and change the AMF_START or AMF_STOP value to **0**.

The tuneable values cannot persist after upgrade from the releases prior to 6.0 [3736830]

If you upgrade releases that are prior to 6.0 to 6.0 or later release, the tunable values which were set by vxtune will be replaced by default values.

Workaround: There is no workaround.

Stopping the installer during an upgrade and then resuming the upgrade might freeze the service groups (2574731)

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

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

To unfreeze the service groups manually

1 List all the frozen service groups

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

2 Unfreeze all the frozen service groups:

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

Issue with soft links getting deleted in a manual upgrade

While performing a manual upgrade (from 5.1 to 6.2.1) of the VRTSvlic RPM, some of the soft links created during your previous installation are deleted. As a result, `vxkeyless` binary is not found in its specified path.

To prevent this, use the `--nopreun` option.

For example: `rpm -Uvh --nopreun VRTSvlic-3.02.61.010-0.x86_64.rpm`

While upgrading the VCS stack from a version prior to VCS 5.1, reconfiguration of MultiNICA IPv4RouteOptions attribute is required (2003864)

The 5.1SP1 MultiNICA agent now uses `ip` command by default. Due to behavioral differences in `ip` and `ifconfig` commands in regards to route configuration, MultiNICA flushes routes and sets them back for the new active device. If the MultiNICA resource configuration is not intended to make use of `ifconfig` command (see table below), you must configure IPv4RouteOptions attribute in MultiNICA resource definition.

Note: RouteOptions values are used by the `route` command where as the IPv4RouteOptions value is used by the `ip route` command. The values to be configured for these two attribute are very specific to their respective commands.

Table 1-30 Whether attributes are configured and required actions that you need to perform during upgrade

Options	RouteOptions and/or IPv4AddrOptions	IPv4RouteOptions	Comment	Actions that you need to perform during upgrade
Configured	May or may not be configured	May or may not be configured	In this case the `ifconfig` command is used. If RouteOptions is set, attribute value is used to add/delete routes using command `route`. As the Options attribute is configured, IPv4RouteOptions values are ignored.	No need to configure IPv4RouteOptions .
Not configured	May or may not be configured	Must be configured	In this case the `ip` command is used. IPv4RouteOptions must be configured and are used to add/delete routes using the `ip route` command. As Options attribute is not configured, RouteOptions value is ignored.	Configure IPv4RouteOptions and set the IP of default gateway. The value of this attribute typically resembles: IPv4RouteOptions = “default via *gateway_ip*” For example: IPv4RouteOptions = “default via 192.168.1.1”

The uninstaller does not remove all scripts (2696033)

After removing DMP, SF, SFCFSHA, SFHA, SF Oracle RAC, SFSYBASECE or VCS, some of the RC scripts remain in the `/etc/rc*.d/` folder. This is due to an issue with the chkconfig rpm in RHEL6 and updates. You can manually remove the scripts from the `/etc/rc*.d/` folder after removing the VxVM RPMs.

Workaround: Install the chkconfig-1.3.49.3-1 chkconfig rpm from the RedHat portal. Refer to the following links:

http://grokbase.com/t/centos/centos/117pfhe4zz/centos-6-0-chkconfig-strange-behavior

http://rhn.redhat.com/errata/RHBA-2012-0415.html

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

If you install or configure DMP, SF, SFCFSHA, SFRAC or VCS and then close the Web installer, if you have other browser windows open, the Web installer does not ask for authentication in the subsequent sessions. Since there is no option to log out of the Web installer, the session remains open as long as the browser is open on the system.

Workaround: Make sure that all browser windows are closed to end the browser session and subsequently log in again.

Stopping the Web installer causes Device Busy error messages (2633924)

If you start the Web installer, and then perform an operation (such as prechecking, configuring, or uninstalling), you may get an error message saying the device is busy.

Workaround: Do one of the following:

- Kill the start.pl process.
- Start the webinstaller again. On the first Web page you see that the session is still active. Either take over this session and finish it or terminate it directly.

Rolling upgrade of VCS from pre-6.0 versions fails with CP server in secure mode [3262900]

If the CP server is configured in secure mode, rolling upgrade of VCS from versions lower than 6.0 to 6.1 is not supported. Since the `vxcpserv` process is not compatible with shared authentication, CP server service group fails to come online after performing phase 1 of the rolling upgrade.

Workaround: Use full upgrade or phased upgrade instead of rolling upgrade.

The Configure Sybase ASE CE Instance in VCS option creates duplicate service groups for Sybase binary mount points (2560188)

The CPI installer does not check to see if Sybase binary mount points are already configured on systems, nor does it give an error message. It creates a duplicate service group for Sybase binary mount points.

This issue will be resolved in a later release.

NetBackup 6.5 or older version is installed on a VxFS file system (2056282)

If you have NetBackup 6.5 or older version installed on a VxFS file system and before upgrading to Symantec Storage Foundation (SF) 6.2.1, if you unmount all VxFS file systems including the one that hosts the NetBackup binaries (`/usr/openv`), then while upgrading to SF 6.2.1, the installer fails to check if NetBackup is installed on the same machine and uninstalls the shared infrastructure RPMs `VRTSpbx`, `VRTSat`, and `VRTSicsco`. This causes NetBackup to stop working.

Workaround: Before you unmount the VxFS file system that hosts NetBackup, copy the `/usr/openv/netbackup/bin/version` file and `/usr/openv/netbackup/version` file to the `/tmp` directory. If you have clustered NetBackup installed, you must also copy the `/usr/openv/netbackup/bin/cluster/NBU_RSP` file to the `/tmp` directory. After you unmount the NetBackup file system, manually copy these two version files from `/tmp` to their original directories. If you have clustered NetBackup installed, you must also copy the `/usr/openv/netbackup/bin/cluster/NBU_RSP` file from `/tmp` to its original directory.

If the `version` files' directories do not exist, create the directories:

```
# mkdir -p /usr/openv/netbackup/bin
# mkdir -p  /usr/openv/netbackup/bin
```

Run the installer to finish the upgrade process. After upgrade process completes, remove the two version files and their directories.

If your system is already affected by this issue, then you must manually install the `VRTSpbx`, `VRTSat`, and `VRTSicsco` RPMs after the upgrade process completes.

Error messages in syslog (1630188)

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

```
Jul  6 10:58:50 swlx62 setroubleshoot: SELinux is preventing the
semanage from using potentially mislabeled files
(/var/tmp/installer-200907061052eVe/install.swlx62.VRTSvxvm). For
complete SELinux messages. run sealert -l ed8978d1-0b1b-4c5b-a086-
67da2a651fb3
Jul  6 10:58:54 swlx62 setroubleshoot: SELinux is preventing the
semanage from using potentially mislabeled files
(/var/tmp/installer-200907061052eVe/install.swlx62.VRTSvxvm). For
complete SELinux messages. run sealert -l ed8978d1-0b1b-4c5b-a086-
67da2a651fb3
Jul  6 10:58:59 swlx62 setroubleshoot: SELinux is preventing the
restorecon from using potentially mislabeled files
```

Ignore certain errors after an operating system upgrade—after a product upgrade with encapsulated boot disks (2030970)

Ignore certain errors after an operating system upgrade after a product upgrade with encapsulated boot disks.

You can ignore the following errors after you upgrade the operating system after a product upgrade that occurred with an encapsulated boot disk. Examples of the errors follow:

```
The partioning on disk /dev/sda is not readable by
The partioning tool parted, which is used to change the
partition table.
You can use the partitions on disk /dev/sda as they are.
You can format them and assign mount points to them, but you
cannot add, edit, resize, or remove partitions from that
disk with this tool.
```

Or

```
Root device: /dev/vx/dsk/bootdg/rootvol (mounted on / as reiserfs)
Module list: pilix mptspi qla2xxx silmage processor thermal fan
reiserfs aedd (xennet xenblk)

Kernel image; /boot/vmlinuz-2.6.16.60-0.54.5-smp
Initrd image: /boot/initrd-2.6.16.60-0.54.5-smp
```

The operating system upgrade is not failing. The error messages are harmless.

Workaround: Remove the /boot/vmlinuz.b4vxvm and /boot/initrd.b4vxvm files (from an un-encapsulated system) before the operating system upgrade.

After a locale change restart the vxconfig daemon (2417547, 2116264)

You need to restart the vxconfig daemon you change the locale of nodes that use it. The vxconfig daemon starts at boot. If you have changed locale, you need to restart the daemon.

Workaround: Refer to the *Symantec Storage Foundation Cluster File System High Availability Administrator's Guide* for the section, "vxconfigd daemon recovery."

After performing the first phase of a rolling upgrade, make sure the CVM is online on all nodes without errors (2595441)

Make sure that the CVM is online on all nodes without errors after you perform the first phase of a rolling upgrade. The CVM protocol version will not upgrade successfully on the nodes during rolling upgrade phase two where CVM is offline or has errors.

If the CVM protocol version does not upgrade successfully, upgrade the CVM protocol on the CVM master node.

To upgrade the CVM protocol on the CVM master node

1 Find out which node is the CVM master:

```
# vxdctl -c mode
```

2 On the CVM master node, upgrade the CVM protocol:

```
# vxdctl upgrade
```

Upgrading from Storage Foundation 5.1 Service Pack 1 Rolling Patch 2 to 6.2.1 with rootability enabled fails (2581313)

While upgrading from Storage Foundation (SF) 5.1 Service Pack (SP) 1 Rolling Patch (RP) 2 to 6.2.1 with intermediate patches (if any), if you use an encapsulated root disk, the upgrade fails because the `initrd` image creation fails during the VxVM upgrade.

Workaround: To upgrade from 5.1 SP1 RP2 to6.2.1 with intermediate patches (if any) using an encapsulated root disk, you must reinstall the nash utility on the system prior to the upgrade from 5.1 SP1 RP2.

To upgrade from 5.1 SP1 RP2 to 6.2.1 with intermediate patches (if any) using an encapsulated root disk:

1 Reinstall the nash utility.

2 Upgrade to the SF 6.2.1 release.

Dependency may get overruled when uninstalling multiple RPMs in a single command [3563254]

When performing uninstallation of multiple RPMs through a single comment, the system identifies and follows the specified dependency among the RPMs as the uninstallation progresses. However, if the pre-uninstallation script fails for any of the RPMs, the system does not abort the task but instead uninstalls the remaining RPMs.

For example, if you run `rpm -e VRTSllt VRTSgab VRTSvxfen` where the RPMs have a dependency between each other, the system bypasses the dependency if the pre-uninstallation script fails for any RPM.

Workaround: Uninstall the RPMs independently.

SF Oracle RAC installer does not support use of `makeresponsefile` option (2577669)

The SF Oracle RAC installer does not support the use of `makeresponsefile` option for configuring Oracle RAC settings. The following message is displayed when you attempt to configure Oracle RAC using the option:

```
Currently SFRAC installer does not support -makeresponsefile option.
```

Workaround: Configure Oracle RAC by editing the response file manually.

Only AppHA can be upgrade when AppHA and SF/DMP are installed on the same machine [3693146]

When you upgrade products on your machine, with 6.2.0 Application HA (AppHA) and 6.2.0 Storage Foundation (SF)/Dynamic Multi-Pathing (DMP) installed on it. CPI can detect the two products correctly, but the installer can only upgrade AppHA and fails to upgrade SF.

Workaround: To solve this issue, perform the following steps:

- If you upgrade from versions earlier than 6.2.0 to 6.2.1, upgrade SF and DMP to 6.2 with product specific script `install<prod>` first.
- If you upgrade from 6.2.0 to 6.2.1, upgrade the remaining product manually.

1. Stop SF/DMP.

2. Get the patches for SF/DMP. To get them, type: `# ./installmr -listpatches`.
3. Install the patches for SF/DMP with the OS command.
4. Start SF/DMP.

Symantec Storage Foundation known issues

This section describes the known issues in this release of Symantec Storage Foundation.

- Veritas Volume Manager known issues
- Veritas File System known issues
- Replication known issues
- Virtualization known issues

Veritas Volume Manager known issues

After installing DMP 6.0.1 on a host with the root disk under LVM on a cciss controller, the system is unable to boot using the vxdmp_kernel command [3599030]

The Dynamic Multi-Pathing (DMP) Native support feature is not supported for the COMPAQ SMART controllers which use device names of the form `/dev/cciss/cXdXpX`. When the `dmp_native_support` feature is enabled, it creates a new initrd image with a Logical Volume Manager (LVM) filter in `lvm.conf.filter=[ "a|/dev/vx/dmp/.*|", "r|.*/|" ]`. The filter only allows access to devices under `/dev/vx/dmp. But /dev/vx/dmp/cciss`, where the root disks DMP nodes are located, are not allowed.

VRAS `verifydata` command fails without cleaning up the snapshots created [3558199]

The `vradmin verifydata` and the `vradmin syncrvg` commands leave behind residues if terminated abnormally. These residues can be snapshot volumes or mount points.

Workaround: Remove the snapshot volumes and unmount the mount points manually.

SmartIO VxVM cache invalidated after relayout operation (3492350)

If a relayout operation is done on a volume that has SmartIO VxVM caching enabled, the contents of the cache for the volume may be invalidated.

Workaround:

This behavior is expected. There is no workaround.

Server panic after losing connectivity to the voting disk (2787766)

This issue occurs on A/P arrays. If the voting disk loses connectivty to the primary paths, DMP takes some time to analyze the error and fail over the paths. During this time, the `cssd` reports a timeout and panics. When using Oracle ASM over DMP devices, set the `disktimeout` parameter to an appropriate value. This parameter indicates the maximum time allowed for a voting file I/O to complete. If this time is exceeded, the voting disk is marked as offline.

The default of `disktimeout` is 200. If the value of the tunable is less that this value, reset the value to the default value.

Workaround:

To set the `disktimeout` to 200:

```
$CRS_HOME/bin/crsctl set css disktimeout 200 [-force] test
```

VxVM fails to create volume by the vxassist(1M) command with maxsize parameter on Oracle Enterprise Linux 6 Update 5 (OEL6U5) [3736647]

The data change object (DCO) volume can't be created when volume size gets too long with the maxsize parameter, otherwise it succeeds.

When Veritas Volume Manager (VxVM) calculates the maxsize parameter, it also accounts pending reclaimation disks in the maxsize_trans function. If some disks are not yet reclaimed, space from those disks is not available to create volume.

Workaround: To resolve this issue, follow the two steps:

1. `#vxdisk -o thin reclaim` *<diskgroup>*
2. `#vxassist -g <diskgroup> make vol maxsize` *<parameters>*

Performance impact when a large number of disks are reconnected (2802698)

If the storage connectivity is lost to part of the storage, the disk group configuration copy is rebalanced to the disks that have connectivity. For example, if the storage for an entire enclosure is removed from a disk group with muliple enclosures. The rebalancing process takes time, during which time the `vxconfigd` daemon is busy and does not respond to commands.

Machine fails to boot after root disk encapsulation on servers with UEFI firmware (1842096)

Certain new servers in the market such as IBM x3650 M2, Dell PowerEdge T610, come with support for the UEFI firmware. UEFI supports booting from legacy MBR type disks with certain restrictions on the disk partitions. One of the restrictions is that each partition must not overlap with other partitions. During root disk encapsulation, it creates an overlapping partition that spans the public region of the root disk. If the check for overlapping partitions is not disabled from the UEFI firmware, then the machine fails to come up following the reboot initiated after running the commands to encapsulate the root disk.

Workaround:

The following workarounds have been tested and are recommended in a single-node environment.

For the IBM x3650 series servers, the UEFI firmware settings should be set to boot with the "Legacy Only" option.

For the Dell PowerEdge T610 system, set "Boot Mode" to "BIOS" from the "Boot Settings" menu.

Veritas Volume Manager (VxVM) might report false serial split brain under certain scenarios (1834513)

VxVM might detect and report a false serial split brain when all of the following conditions are met:

- One or more arrays that provide the shared storage for the cluster are being powered off
- At the same time when the arrays are being powered off, an operation that requires an internal transaction is initiated (such as VxVM configuration commands)

In such a scenario, disk group import will fail with a split brain error and the vxsplitlines output will show 0 or 1 pools.

Workaround:

To recover from this situation

1. Retrieve the disk media identifier (dm_id) from the configuration copy:

   ```
   # /etc/vx/diag.d/vxprivutil dumpconfig device-path
   ```

   The dm_id is also the serial split brain id (ssbid)

2. Use the dm_id in the following command to recover from the situation:

   ```
   # /etc/vx/diag.d/vxprivutil set device-path ssbid=dm_id
   ```

Root disk encapsulation issue (1603309)

Encapsulation of root disk will fail if it has been assigned a customized name with vxdmpadm(1M) command. If you wish to encapsulate the root disk, make sure that you have not assigned a customized name to its corresponding DMP node.

See the vxdmpadm(1M) manual page.

See the "Setting customized names for DMP nodes" section of the *Symantec Storage Foundation Administrator's Guide*.

VxVM starts before OS device scan is done (1635274)

While working with some arrays, VxVM may start before all devices are scanned by the OS. This slow OS device discovery may result in malfunctioning of VM, fencing and VCS due to partial disks seen by VxVM.

Workaround:

After the fabric discovery is finished, issue the `vxdisk scandisks` command to bring newly discovered devices into the VxVM configuration.

DMP disables subpaths and initiates failover when an iSCSI link is failed and recovered within 5 seconds. (2100039)

When using iSCSI S/W initiator with an EMC CLARiiON array, iSCSI connection errors may cause DMP to disable subpaths and initiate failover. This situation occurs when an iSCSI link is failed and recovered within 5 seconds.

Workaround:

When using iSCSI S/W initiator with an EMC CLARiiON array, set the node.session.timeo.replacement_timeout iSCSI tunable value to 40 secs or higher.

During system boot, some VxVM volumes fail to mount (2622979)

During system boot, some VxVM volumes that exist in the `/etc/fstab` file fail to mount with the following error messages:

```
# fsck
Checking all file systems.
  error on stat() /dev/vx/dsk//volume: No such
file or directory
```

The load order of kernel modules in Linux results in the VxFS file system driver loading late in the boot process. Since the driver is not loaded when the `/etc/fstab` file is read by the operating system, file systems of the type vxfs will not mount.

Workaround:

To resolve the failure to mount VxFS file systems at boot, specify additional options in the `/etc/fstab` file. These options allow the filesystems to mount later in the boot process. An example of an entry for a VxFS file system:

```
/dev/vx/dsk/testdg/testvolume /mountpoint  vxfs  _netdev,hotplug  1 1
```

To resolve the issue, the fstab entry for VxVM data volumes should be as per following template:

```
/dev/vx/dsk/testdg/testvol    /testmnt    vxfs   _netdev     0 0
```

Unable to upgrade the kernel on an encapsulated boot disk on SLES 11 (2612301)

Upgrading the kernel on an encapsulated boot disk does not work on SUSE Linux Enterprise Server (SLES) 11.

Workaround: Perform the following procedure on the system with the encapsulated root disk to upgrade the kernel.

To upgrade the kernel on a system with an encapsulated root disk

1 Unroot the encapsulated root disk:

```
# /etc/vx/bin/vxunroot
```

2 Upgrade the kernel:

```
# rpm -Uvh Kernel-upgrade_version
```

3 Reboot the system.

4 Re-encapsulated the root disk:

```
# /etc/vx/bin/vxencap -c -g root_diskgroup rootdisk=root_disk
```

Removing an array node from an IBM Storwize V7000 storage system also removes the controller (2816589)

When using an IBM Storwize V7000 storage system, after removing one array node, the corresponding controller is also removed.

Workaround: The following procedure resolves this issue.

To resolve this issue

1 Set the `iotimeout` tunable to 600:

```
# vxdmpadm setattr enclosure encl1 recoveryoption=throttle \
 iotimeout=600
```

2 After you re-add the SAN VC node, run the `vxdctl enable` command for Dynamic Multi-Pathing (DMP) to detect the added paths:

```
# vxdctl enable
```

Upgrading from Symantec Storage Foundation and High Availability Solutions 5.x to 6.2.1 may fail for IBM XIV Series arrays (2715119)

Starting in the Symantec Storage Foundation and High Availability Solutions 5.1 SP1 release, the Array Support Library (ASL) for the IBM XIV enclosures converts the LUN Serial Number from hexadecimal to decimal. Because of this change, the enclosure names differ from releases prior to the 5.1 SP1 releases. When you upgrade Symantec Storage Foundation and High Availability Solutions from a release prior to that release to the current 6.2.1 release, XIV LUNs may go into an error state. Note that the latest RPs on 5.1/5.1SP1 are already modified to use the same logic for enclosure naming.

Workaround:

After the upgrade, run `vxddladm assign names`.

Cannot grow Veritas Volume Manager (VxVM) disk using the vxdisk resize command during Dynamic LUN Expansion operation (2064510)

The following error message is displayed during the Dynamic LUN Expansion operation of a LUN with the SIMPLE format:

```
VxVM vxdisk ERROR V-5-1-8643 Device <device name>: resize failed:
Invalid data in request
```

The `vxdisk resize` command keeps the cylinder size (number of the heads * total number of the sectors per track) constant before and after the resize operation, unless the number of cylinders go beyond 2^16-1 (65535) . Because of the VTOC limitation of storing geometry values only till 2^16 -1, if the number of cylinders increases beyond the limit, `vxdisk resize` increases the cylinder size. If this happens, the private region will overlap with the public region data and corrupt the user data.

As a result of this LUN geometry change, VxVM is unable to complete `vxdisk resize` on simple format disks. VxVM was not designed to handle such geometry changes during Dynamic LUN Expansion operations on simple disks.

Workaround:

The VxVM `vxdisk resize` command behaves differently depending on whether the disk is simple, sliced, or CDS format.

The problem shown above only occurs on simple disk configurations. As a result of this difference in behavior, if the geometry changes during a Dynamic LUN Expansion operation at the LUN level, you can convert the disk to a CDS format disk. Use the `vxcdsconvert` command on the disk. Then you can issue the `vxdisk resize` command.

See http://www.symantec.com/docs/TECH136240 for more information.

Continuous trespass loop when a CLARiiON LUN is mapped to a different host than its snapshot (2761567)

If a CLARiiON LUN is mapped to a different host than its snapshot, a trespass on one of them could cause a trespass on the other. This behavior could result in a loop for these LUNs, as DMP tries to fail back the LUNs if the primary paths are available.

Workaround

To avoid this issue, turn off the `dmp_monitor_ownership` tunable:

```
# vxdmpadm settune dmp_monitor_ownership=off
```

Disk group import of BCV LUNs using -o updateid and -ouseclonedev options is not supported if the disk group has mirrored volumes with DCO or has snapshots (2831658)

VxVM uses guid stored in configuration to uniquely identify all objects. The data change object (DCO) volume stores the guid of mirrors and snapshots. If the disk group is imported with `-o updateid` and `-o useclonedev`, it changes the guid of objects in VxVM configuration database and the guids stored in the DCO volume are not updated. The operations involving DCO cannot find objects with the stored guid. This could lead to failure of certain operations involving DCO or could lead to unexpected behavior.

Workaround:

No workaround available.

After devices that are managed by EMC PowerPath lose access to storage, Veritas Volume Manager commands are delayed (2757198)

In an enviroment which includes devices that are managed by EMC PowerPath, a storage loss causes Veritas Volume Manager commands to be delayed. In the event of storage loss, VxVM sends SCSI inquiry to each LUN path to check the health of path, which are delayed by the presence of EMC PowerPath.

Workaround:

There is no workaround available.

vxresize does not work with layered volumes that have multiple plexes at the top level (3301991)

If a layered volume has multiple plexes at the top level, `vxresize` does not work. For example, if you add a mirror to a concat-mirror volume for a third mirror snapshot. The `vxresize` operation fails with the following message:

```
VxVM vxassist ERROR V-5-1-2528 Volume volname built on layered volumes
have multiple plexes
VxVM vxresize ERROR V-5-1-4703 Problem running vxassist command for
volume volname, in diskgroup dgname
```

Workaround:

To resize the volume

1. After adding the mirror to the volume, take a snapshot using the plex.
2. Grow the volume and snapshot volume with `vxresize`
3. Reattach the snapshot volume to the source volume.

The DMP EMC CLARiiON ASL does not recognize mirror view not ready LUNs (3272940)

On hosts that have EMC CLARiiON mirror view not ready LUNs, if you enable or disable the switch port and then issue the `vxdisk scandisks` or `vxdctl enable` command, I/O error messages are written continuously in the syslog.

The dynamic multi-pathing (DMP) request for providing information to identify mirror view not ready LUNs through in-band SCSI command is pending with EMC engineering. Not ready LUNs are special kind of LUNs which reject all kinds of I/O requests.

Because DMP does not recognize not ready LUNs, Veritas Volume Manager (VxVM) tries to bring them online. As part of the online process, VxVM issues I/Os to read the disk private region. These I/Os fail and generate error messages in syslog.

Because of events that are generated as part of the online process, the `vxattachd` script triggers the vxdisk scandisks command again. This cycle causes continuous I/O error messages. This problem can also cause other commands to run slowly because the VxVM configuration daemon (`vxconfigd`) is busy servicing `vxdisk scandisks`.

Workaround: Stop the `vxattachd` script and set EMC CLARiiON values, as follows:

1 Disable the `vxattachd` process.

For more information on how to disable `vxattachd` and what features you lose if `vxattachd` is disabled, see the `vxattachd` man page

2 Set the following EMC CLARiiON values:

- `recoveryoption=fixedretry`
- `retrycount=5`

Enter:

```
vxdmpadm setattr enclosure enclosure_name recoveryoption=fixedretry \
retrycount=5
```

Changes in enclosure attributes are not persistent after an upgrade from release prior to VxVM 5.1SP1 (2082414)

The Veritas Volume Manager (VxVM) 6.2.1 includes several array names that differ from the array names in releases 5.1SP1 or prior. Therefore, if you upgrade to VxVM 6.2.1 from a release 5.1SP1 or earlier, changes in the enclosure attributes may not remain persistent. Any enclosure attribute set for these arrays may be reset to the default value after an upgrade to VxVM 6.2.1.

Workaround:

Manually reconfigure the enclosure attributes to resolve the issue.

Table 1-31 shows the Hitachi arrays that have new array names.

Table 1-31 Hitachi arrays with new array names

Previous name	New name
TagmaStore-USP	Hitachi_USP
TagmaStore-NSC	Hitachi_NSC
TagmaStoreUSPV	Hitachi_USP-V
TagmaStoreUSPVM	Hitachi_USP-VM
Hitachi AMS2300 Series arrays	New array names are based on the Model Number 8x. For example, AMS_100, AMS_2100, AMS_2300, AMS_2500, etc.

In addition, the Array Support Library (ASL) for the enclosures XIV and 3PAR now converts the cabinet serial number that is reported from Hex to Decimal, to correspond with the value shown on the GUI. Because the cabinet serial number has changed, any enclosure attribute set for these arrays may be reset to the default value after an upgrade to VxVM 6.2.1. Manually reconfigure the enclosure attributes to resolve the issue.

The cabinet serial numbers are changed for the following enclosures:

- IBM XIV Series arrays
- 3PAR arrays

Running the vxdisk *disk* set clone=off command on imported clone disk group luns results in a mix of clone and non-clone disks (3338075)

If you do not specify a disk group name, the `vxdisk set` operation works on the `dmname` rather than the `daname`. If a `dmname` is the same as an existing `daname`, the vxdisk set operation reflects on the dm name.

Workaround: Use the following command syntax to set the attributes:

```
vxdisk -g diskgroup_name set dmname clone=off
```

For example:

```
vxdisk -g dg1 set eva4k6k0_12 clone=off
```

vxunroot cannot encapsulate a root disk when the root partition has XFS mounted on it (3614362)

If the root partition has the XFS file system mounted on it, you cannot change the root partition's Universally Unique IDentifier (UUID). However, changing the UUID of the partitions of the root disk is necessary in root disk encapsulation. Given the limitation above, Symantec does not support root disk encapsulation where the root partition has an XFS file system.

Workaround:

None.

Restarting the vxconfigd daemon on the slave node after a disk is removed from all nodes may cause the disk groups to be disabled on the slave node (3591019)

The issue occurs if the storage connectivity of a disk is removed from all the nodes of the cluster and the `vxconfigd` daemon is restarted on the slave node before the disk is detached from the slave. All the disk groups are in the `dgdisabled` state on the slave node, but show as `enabled` on the other nodes.

If the disk was detached before the `vxconfigd` daemon is restarted, the issue does not occur.

In a Flexible Shared Storage (FSS) environment, removing the storage connectivity on a node that contributes DAS storage to a shared disk group results in global connectivity loss because the storage is not connected elsewhere.

Workaround:

To prevent this issue:

Before restarting the `vxconfigd` daemon, if a disk in a shared disk group has lost connectivity to all nodes in the cluster, make sure that the disk is in the `detached` state. If a disk needs to be detached, use the following command:

```
# vxdisk check diskname
```

To resolve the issue after it has occurred:

If `vxconfigd` is restarted before the disks got detached, remove the node from the cluster and rejoin the node to the cluster.

DMP panics if a DDL device discovery is initiated immediately after loss of connectivity to the storage (2040929)

When using EMC Powerpath with VxVM 5.1SP1 on SLES11, set the fast_io_fail_tmo on the HBA port to any non-zero value that is less than the dev_loss_tmo value so as to avoid a panic in case a DDL device discovery is initiated by the `vxdisk scandisks` command or the `vxdctl enable` command immediately after loss of connectivity to the storage.

Failback to primary paths does not occur if the node that initiated the failover leaves the cluster (1856723)

When CVM is configured on non-A/A storage, if a node loses access to the storage through all the primary paths, then all the nodes in the cluster switches to the secondary paths. If the node which raised the protocol leaves the cluster and if all the rest of the nodes in the cluster are seeing the primary paths as healthy, then failback to primary paths never happens.

Issues if the storage connectivity to data disks is lost on a CVM slave node while vxconfigd was not running on the node (2562889)

If storage connectivity to data disks is lost on a CVM slave node while vxconfigd was not running on the node, this may result in following issues when `vxconfigd` comes up on this node:

- The shared disk groups on the disconnected storage are marked as dgdisabled on the slave node only.
- The shared disk groups are available to rest of the cluster nodes but no transactions, such as VxVM configuration changes, are possible on any shared disk group.

- Attempts to deport such shared disk groups will fail.

Workaround:

Do one of the following:

- Remove the faulty slave node out of CVM cluster, restore storage connectivity, and rejoin the node to the cluster.
- Restart `vxconfigd` on the CVM master node.

The vxcdsconvert utility is supported only on the master node (2616422)

The `vxcdsconvert` utility should be run only from the master node, not from the slave nodes of the cluster.

Re-enabling connectivity if the disks are in local failed (lfailed) state (2425977)

In a Cluster Volume Manager (CVM) cluster, you can disable connectivity to the disks at the controller or enclosure level with the `vxdmpadm disable` command. In this case, CVM may place the disks into the `lfailed` state. When you restore connectivity with the `vxdmpadm enable` command, CVM may not automatically clear the `lfailed` state. After enabling the controller or enclosure, you must run disk discovery to clear the locally failed state.

To run disk discovery

◆ Run the following command:

```
# vxdisk scandisks
```

Issues with the disk state on the CVM slave node when vxconfigd is restarted on all nodes (2615680)

When a CVM master node and a slave node have lost storage access, and `vxconfigd` is restarted on all nodes, the disk state on the CVM slave node shows as invalid.

Plex synchronization is not completed after resuming synchronization on a new master when the original master lost connectivity (2788077)

When you run `vxrecover -o force`, it recovers only one subvolume and it cannot detect that the rest of the volume needs recovery.

When you run the `vxassist mirror` command, you run the `vxplex att`command serially on each subvolume. If the failure happens before you start the `attach`operation (need to mark the concerned plex as the attach operation is in progress), `vxrecover` will not redo the attach operation because it cannot find any record of the attach operation in progress.

Workaround:

Run the following command on each subvolume to manually recover the complete volume:

```
# usr/lib/vxvm/type/fsgen/vxplex -U fsgen -g diskgroup \
 -o force useopt att volume plex
```

A master node is not capable of doing recovery if it cannot access the disks belonging to any of the plexes of a volume (2764153)

A master node with missing disks is not capable of doing recovery, as it does not have access to the disks belonging to any of the plexes of a volume.

Workaround:

If other nodes have access to the storage, they can do the recovery. Switch the master role to some other node with better storage connectivity.

CVM fails to start if the first node joining the cluster has no connectivity to the storage (2787713)

If the first node joining the cluster has no connectivity to disks, the import of shared disk groups fails. Other nodes that join the cluster later assume that the auto-import of disk groups is already done as part of the existing cluster processing.

Workaround:

Perform a master switch to the node that has connectivity to the disks. Then import the disk groups manually.

Dynamic LUN expansion is not supported for EFI disks in simple or sliced format and non-EFI disks greater than 1TB in simple or sliced format.(2836798)

Dynamic LUN expansion is not supported for EFI (Extensible Firmware Interface) disks in simple or sliced format and non-EFI disks greater than 1TB in simple or sliced format. The recommended format is the Cross-platform Data Sharing (CDS) disk format.

Workaround:

Convert the disk format to CDS using the `vxcdsconvert` utility.

CVMVolDg agent may fail to deport CVM disk group when CVMDeportOnOffline is set to 1

When CVMDeportOnOffline is set to 1, the CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported.

Workaround: If multiple CVMVolDg resources are configured for a shared disk group and the disk group is required to be deported during offline, set the value of the `CVMDeportOnOffline` attribute to 1 for all of the resources.

cvm_clus resource goes into faulted state after the resource is manually panicked and rebooted in a 32 node cluster (2278894)

The `cvm_clus` resource goes into faulted state after the resource is manually panicked and rebooted in a 32 node cluster.

Workaround: There is no workaround for this issue.

DMP uses OS device physical path to maintain persistence of path attributes from 6.0 [3761441]

From release 6.0, DMP uses OS device physical path instead of logical name to maintain persistence of path attributes. Hence after upgrading to DMP 6.0 or later releases, path attributes are reset to the default values. You must reconfigure any path-level attributes that were defined in the /etc/vx/dmppolicy.info file.

Workaround:

To configure path-level attributes

1. Remove the path entries from the `/etc/vx/dmppolicy.info` file.
2. Reset the path attributes.

The vxsnap print command shows incorrect value for percentage dirty [2360780]

The `vxsnap print` command can display the percentage of regions that differ between snapshots, shown as the %dirty. In SF 6.0, if this command is run while the volumes are online and being actively used, the shown %dirty may lag from actual percentage dirty for instant snap data cache object (DCO) volumes. That is, the command output may show less %dirty than actual.

device.map must be up to date before doing root disk encapsulation (3761585, 2202047)

If you perform root disk encapsulation while the `device.map` file is not up to date, the `vxdiskadm` command displays the following error:

```
/etc/vx/bin/vxinitrd: line 447: printf: e0: invalid number
```

```
VxVM vxencap INFO V-5-2-5327 Missing file: /boot/grub/device.map
```

Workaround:

Before you perform root disk encapsulation, run the the following command to regenerate the device.map file:

```
grub-install --recheck <diskname>
```

In the above command line, the <*diskname*> is the disk booted with. Ideally it should be the root disk. For eg., `grub-install --recheck /dev/sdb`

Virtualization known issues

This section describes the virtualization known issues in this release.

Configuring application for high availability with storage using VCS wizard may fail on a VMware virtual machine which is configured with more than two storage controllers [3640956]

Application configuration from VCS wizard may fail on VMware virtual machine which is configured with multiple SCSI controllers.

Workaround: There is no workaround available.

Agent kill on source during migration may lead to resource concurrency violation (3042499)

In the case of a migration initiated outside Symantec Cluster Server (VCS) control, there is a very small window in which the agent restart might not be able to recognize the migration event. As this is initiated outside VCS, there is no way to synchronize the agent restart and the migration., Also, there is no intermediate state in KVM that can indicate that the event was a migration. This problem does not occur in Red Hat Enterprise Virtualization (RHEV), as there are clear states visible that can specify the virtual machine events. This is applicable to KVM environment only.

Workaround: There is no workaround for this issue.

Host fails to reboot when the resource gets stuck in ONLINE|STATE UNKNOWN state [2738864]

In a Red Hat Enterprise Virtualization environment, if a host reboot is performed on which the KVMGuest resource monitoring the virtual machine is ONLINE, then the host reboot fails. This is because the VDSM is getting stopped before VCS could shutdown the virtual machine. In this case, the virtual machine state remains ONLINE|STATE UNKNOWN, and hence VCS stop fails eventually failing the host reboot as well.

Workaround: Switch the service group to other node before initiating a host reboot.

VM state is in PAUSED state when storage domain is inactive [2747163]

If the storage domain associated with the running virtual machine becomes inactive, the virtual machine may go to **paused** state.

Workaround: Make sure that the storage domain is always active when running virtual machine.

Switching KVMGuest resource fails due to inadequate swap space on the other host [2753936]

Virtual machine fails to start on a host if the host does not have the sufficient swap space available.

Workaround: Please make sure that each host has sufficient swap space available for starting the virtual machine.

Policies introduced in SLES 11SP2 may block graceful shutdown if a VM in SUSE KVM environment [2792889]

In a SUSE KVM environment, virtual machine running SLES11 SP2 inside may block the virtual machine graceful shutdown request due to some policies introduced in SLES 11SP2. SUSE recommends turning off the policy with `polkit-gnome-authorization` for a virtual machine.

Workaround: Make sure that all the policies blocking any such request are turned off.

Load on `libvirtd` may terminate it in SUSE KVM environment [2824952]

In a SUSE KVM environment, occasionally `libvirtd` process may get terminated and `/etc/init.d/libvirtd status` command displays:

```
#/etc/init.d/libvirtd  status
Checking status of libvirtd                    dead
```

This may be due to heavy load on `libvirtd` process.

Workaound: Restart the `libvirtd` process and run:

```
# service libvirtd stop
# service libvirtd start
```

Offline or switch of KVMGuest resource fails if the VM it is monitoring is undefined [2796817]

In a SUSE KVM environment, if a running virtual machine is undefined using `virsh undefine` command, an attempt to offline or switch the KVM guest resource monitoring that VM fails because the agent is not able to get the information from the KVM hypervisor.

Workaround: To undefine the VM on a particular node, first switch the service group containing the KVMGuest resource to another node and then undefine the VM on the first node.

Increased memory usage observed even with no VM running [2734970]

Increased memory usage was observed on the hosts even when VMs were either not running or had stopped. This is due to the RHEV behavior.

Workaround: No workaround.

Resource faults when it fails to ONLINE VM beacuse of insufficient swap percentage [2827214]

In virtualization environment, if VCS fails to start the virtual machine due to unavailability of required virtualization resources such as CPU, memory, or disks, the resource goes into FAULTED state.

Workaround: Make sure that the required virtualization resources are always available in a virtualization environment.

Migration of guest VM on native LVM volume may cause libvirtd process to terminate abruptly (2582716)

When the guest VM image is on native LVM volume, then the migration of that guest initiated by the administrator may cause `libvirtd` process to terminate abruptly.

Workaround: Start the `libvirtd` process manually.

Virtual machine may return the not-responding state when the storage domain is inactive and the data center is down (2848003)

In a Red Hat Enterprise Virtualization Environment, if the storage domain is in an inactive state and the data center is in down state, the virtual machine may return a not-responding state and the KVMGuest resource in OFFLINE state.

Workaround: To resolve this issue:

1. Activate the storage domain in RHEV-M.
2. Check that the data center is in the up state.

Guest virtual machine may fail on RHEL 6.1 if KVM guest image resides on CVM-CFS [2659944]

If a KVM guest image file resides on CVM-CFS, the migration of that guest virtual machine may fail with "Permission Denied" error on RHEL 6.1. This causes guest virtual machine to go in "shut-off" state on both source and destination node, and the associated VCS KVMGuest.

Workaround: Make sure that the guest image file is having 777 permission.

System panics after starting KVM virtualized guest or initiating KVMGuest resource online [2337626]

System panics when the KVM guest is started or when the KVMGuest resource online is initiated. This issue is rarely observed.

The issue is observed due to the file descriptor leak in the libvirtd process. The maximum file open limit of file descriptor for libvirtd process is 1024. You may sometimes observe that more than 1024 file descriptors are opened when the KVM guest is started. Therefore, if the maximum file open limit is crossed, any attempt to start the KVM guest or to open a new file causes the system to panic. VCS cannot control this behavior as it suspects a file descriptor leak in the libvirtd process.

Workaround: There is no definite resolution for this issue; however, you can check the number of files opened by the libvirtd process in `/proc/<pid of libvirtd>/fd/`. If the file count exceeds 1000, restart libvirtd with the following command:

```
/etc/init.d/libvirtd restart
```

KVMGuest agent fail to online the resource in a DR configuration with error 400 [3056096]

In a disaster recovery configuration, a replication agent is used to manage the replication of the storage domain containing the virtual machine boot disks. The agent makes sure that the storage is in primary role on the RHEL-H hosts, where the resource goes online. When you switch the replication resource to the remote cluster, the replication direction is reversed and it takes some time for the RHEV-M to detect the change in the storage parameters. At the same time if you attempt to online the KVMGuest resource, the operation fails since the storage domain is still not activated on the RHEL-H host.

Workaround: You can try to online the virtual machines after some time.

CD ROM with empty file vmPayload found inside the guest when resource comes online [3060910]

When you unset the DROpts attribute on a KVMGuest resource and online the resource on the host, a CD ROM with an empty file vmPayload is available inside the guest.

The KVMGuest agent adds a CD ROM to the virtual machine configuration when you online a KVMGuest resource with the DROpts attribute set. The CD ROM carries some site-specific parameters to be used inside the guest. When you offline the same resource, the agent removes the CD ROM, but for some reason, the CD ROM does not get removed completely. If you unset the DROpts attribute and online the resource later, a CD ROM with an empty file vmPayload continues to be available inside the guest.

Workaround: This does not impact the functionality of the virtual machine in any way and can be ignored.

VCS fails to start virtual machine on another node if the first node panics [3042806]

In the KVM environment, if a node on which a virtual machine is running panics, then VCS fails to start that virtual machine on another node. This issue occurs because KVM Hypervisor is not able to acquire lock on the virtual machine. This issue is due to KVM Hypervisor behavior and is very rarely observed.

Workaround: Restart libvirtd process to resolve this issue. Command to restart libvirtd:

```
# service libvirtd restart
```

VM fails to start on the target node if the source node panics or restarts during migration [3042786]

If a virtual machine (VM) migration is initiated and the source node (node on which VM was running) panics or is restarted forcefully, VM fails to start on any other node in a KVM environment. This issue is due to the KVM locking mechanism. The VM start fails with the following error:

```
error: Failed to start domain VM1
error: Timed out during operation: cannot acquire state change lock
```

Workaround: Restart (kill and start) the libvirtd daemon on the second node using the following command:

```
# service libvirtd restart
```

Symantec High Availability tab does not report LVMVolumeGroup resources as online [2909417]

The Symantec High Availability tab does not automatically report the online status of activated LVMVolumeGroup resources in the following case:

- If you created the VCS cluster as part of the Symantec High Availability Configuration Wizard workflow.

Workaround: Start the LVMVolumeGroup resources from the Symantec High Availability tab. For more information, see the Symantec High Availability Solutions Guide for VMware.

Cluster communication breaks when you revert a snapshot in VMware environment [3409586]

If VCS is running on the guest operating system when a VMware virtual machine snapshot is taken, the virtual machine snapshot contains the run-time state of the cluster. When you restore the snapshot, the state of the cluster which is restored can be inconsistent with other nodes of the cluster. Due to the inconsistent state, VCS is unable to communicate with other nodes of the cluster.

Workaround: Before you take a snapshot of the virtual machine, Symantec recommends that you stop VCS services running inside the virtual machine.

VCS may detect the migration event during the regular monitor cycle due to the timing issue [2827227]

In a virtualization environment, VCS detects the virtual machine migration initiated outside VCS and changes the state accordingly. However, occasionally, VCS may miss the migration event due to timing issue and detect the migration during the regular monitor cycle. For example, if you set OfflineMonitorInterval as 300sec, it takes up to 5 minutes for VCS to report ONLINE on the node where the virtual machine got migrated.

Workaround: No workaround available.

The `vxrhevadm` CLI is missing after upgrading the `VRTSrhevm` package from 6.2 to 6.2.1 [3733178]

When the `VRTSrhevm` package is upgraded from 6.2 to 6.2.1, the `vxrhevadm` CLI from the package is missing. As a result, corresponding functionality of attaching and detaching Storage Foundation devices to the virtual machines in Red Hat Enterprise Virtualization is not available.

The upgrade option of the RPM package manager installs the newer package first and removes the older package later. Because this behavior is not handled correctly in the `VRTSrhevm` RPM, the `vxrhevadm` CLI gets deleted during the upgrade scenario. As a result, the CLI is missing and the expected functionality is broken.

Workaround:

Remove the existing `VRTSrhevm` package and install the newer package with the following commands:

# rpm -e VRTSrhevm

# rpm -ivh VRTSrhevm-*version*-RHEL6.x86_64.rpm

Veritas File System known issues

This section describes the known issues in this release of Veritas File System (VxFS).

On RHEL7 onwards, Pluggable Authentication Modules(PAM) related error messages for Samba daemon might occur in system logs [3765921]

After adding Common Internet File System(CIFS) share and the CIFS share is might not be accessible from windows client, the PAM related error messages for Samba daemon might occur.

This issue occurred because the`/etc/pam.d/samba` file is not available by default on RHEL 7 onwards and the `obey pam restrictions` attribute from`smb.conf` file, which is Samba configuration file, is set to `yes`, where default is `no`. This parameter controls whether or not Samba should obey PAM's account and session management directives. The default behavior is to use PAM for clear text authentication only and to ignore any account or session management. Samba always ignores PAM for authentication in the case of `encrypt passwords = yes`.

Workaround: Set `obey pam restrictions = no` in the`/opt/VRTSvcs/bin/ApplicationNone/smb.conf` file before configuring cfsshare and adding share.

Delayed allocation may be turned off automatically when one of the volumes in a multi-volume file system nears 100%(2438368)

Delayed allocation may be turned off automatically when one of the volumes in a multi-volume file system is in almost full usage, even if other volumes in the file system have free space.

Workaround: After sufficient space is freed from the volume, the delayed allocation automatically resumes.

The file system deduplication operation fails with the error message "DEDUP_ERROR Error renaming X checkpoint to Y checkpoint on filesystem Z error 16" (3348534)

The file system deduplication operation fails with the error message "DEDUP_ERROR Error renaming X checkpoint to Y checkpoint on filesystem Z error 16", due to the failure in unmounting the checkpoint.

Workaround: Retry the deduplication operation to resolve the problem.

Enabling delayed allocation on a small file system may disable the file system (2389318)

When you enable the delayed allocation on a small file system, such as around 100 MB, the file system may be disabled. In this case, the following error message is displays in the system console log:

```
mesg 001: V-2-1: vx_nospace - file_system file
system full (size block extent)
```

Workaround: Use the `vxtunefs` command for turning off the delayed allocation for the file system.

After upgrading a file system using the vxupgrade(1M) command, the sfcache(1M) command with the stat option shows garbage value on the secondary node. [3759788]

After upgrading a file system from any lower disk layout version to version 10, the fset unique identifier is not updated in-core on the secondary node. So the `sfcache` command with the `stat` option picks the wrong statistics for the upgraded file system on the secondary side.

Workaround:

Unmount the file system on the secondary node, and mount it again with appropriate SmartIO options.

XFS file system is not supported for RDE

The Root Disk Encapsulation (RDE) feature is not supported if the root partition is mounted with XFS file system.

Workaround: There is no workaround available.

In a CFS cluster, that has multi-volume file system of a small size, the fsadm operation may hang (3348520)

In a CFS cluster, that has multi-volume file system of a small size, the fsadm operation may hang, when the free space in the file system is low.

Workaround: There is no workaround for this issue.

When hard links are present in the file system, the sfcache list command shows incorrect cache usage statistics (3059125, 3760172)

If a hard link is present for a file that is loaded in the cache, the `sfcache list` command shows the cache usage for both files: the original file and the hard link. The resulting statistics are incorrect, because the cache usage is shown to be twice the actual usage.

For example:

```
# sfcache list -r /mnt1
/mnt1:
CACHE-USED(MB) MODE PINNED NAME
0 read no /mnt1/test_10
0 read no /mnt1/test_20
0 read no /mnt1/test_50
0 read no /mnt1/test_100
0 read no /mnt1/test_200
```

```
0 read no /mnt1/test_300
0 read no /mnt1/test_400
500 read yes /mnt1/test_500
0 read no /mnt1/test_1024
500 read yes /mnt1/dir/hardlink
500 read no /mnt1/dir
1000 read no /mnt1
```

```
# sfcache list fs1

Cachearea: fs1
Assoc Type: AUTO
Type: VxFS
Size: 1.00g
State: ONLINE
/dev/vx/dsk/sfcache_defaultdg/fs1:
FSUUID CACHE-USED(MB) MODE MOUNTPOINT
23642651-81a5-0d00-1a26-0000911ec26c 1000 read /mnt1
```

Workaround: There is no workaround for this issue.

The command tab auto-complete fails for the `/dev/vx/` file tree; specifically for RHEL 7 (3602082)

The command tab auto-complete operation fails because the following RPM is installed on the machine:

"bash-completion-2.1-6.el7.noarch"

This somehow overwrites the default auto-complete rules. As a result, some issues are observed with the VxFS commands. However, the issue is not observed with all the VxFS commands. The issue is observed with the `mkfs`(1M) command, but is not observed with the `mount`(1M) command.

Workaround: Please remove the "bash-completion-2.1-6.el7.noarch" RPM, so that the command tab auto-complete does not fail for the `/dev/vx/` file tree.

Task blocked messages display in the console for RHEL5 and RHEL6 (2560357)

For RHEL5 and RHEL6, the kernel occasionally displays messages in the console similar to the following example:

```
INFO: task seq:16957 blocked for more than 120 seconds.
```

These messages display because the task is blocked for a long time on the sleep locks. However, the task is not hung and the messages can be safely ignored.

Workaround: You can disable these messages by using the following command:

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

Deduplication can fail with error 110 (3741016)

In some cases, data deduplication fails with a message similar to the following example:

```
Saving    Status    Node            Type        Filesystem
---------------------------------------------------------------------
00%       FAILED    node01          MANUAL      /data/fs1
        2011/10/26 01:38:58 End full scan with error
```

In addition, the deduplication log contains an error similar to the following example:

```
2011/10/26 01:35:09 DEDUP_ERROR AddBlock failed. Error = 110
```

These errors indicate that the deduplication process is running low on space and needs more free space to complete.

Workaround: Make more space available on the file system.

System unable to select ext4 from the file system (2691654)

The system is unable to select ext4 from the file system.

Workaround: There is no workaround.

The system panics with the panic string "kernel BUG at fs/dcache.c:670!" (3323152)

The umount of the file system under high-memory-pressure condition may lead to a system panic. The panic string is displayed as following: "kernel BUG at fs/dcache.c:670!"

Workaround: There is no workaround for this issue.

A restored volume snapshot may be inconsistent with the data in the SmartIO VxFS cache (3760219)

The data in a volume snapshot may have data that is inconsistent with the VxFS level SmartIO cache. When the volume snapshot is restored and mounted, then before using that file system you should purge the corresponding cache data. Or, disable the caching for that file system.

Workaround:

Purge the file system data from the SmartIO cache after restoring the volume snapshot.

```
# sfcache purge {mount_point|fsuuid}
```

When in-place and relocate compression rules are in the same policy file, file relocation is unpredictable (3760242)

You cannot have in-place compress/uncompress rules and relocate compress/uncompress rules in the same policy file. If they are in the same file, file relocation is unpredictable.

Workaround: Create a different policy file for each policy, and enforce the policy as per the required sequence.

During a deduplication operation, the spoold script fails to start (3196423)

This issue occurs because a port is not available during the operation; therefore the spoold script fails to start with the the following error:

```
DEDUP_ERROR INIT: exec spoold failed (1024)
```

Workaround:

Check the `spoold.log` file for specific error messages, and if the log indicates a port is not available, you can check if the port is in use with the `netstat/lsof` command. If the port is not open, you can retry the deduplication operation; if the port is open, you can wait for the port to close, and then try the deduplication operation again.

For example, the following error message in the `spoold.log` file indicates that port `51003` is not available:

```
ERR [140399091685152]: -1: NetSetup: NetBindAndListen returned error,
unable to bind to localhost:51003
```

The file system may hang when it has compression enabled (3331276)

In a VxFS file system that has compression enabled, a deadlock in page fault handler can lead to the file system hang.

Workaround:

There is no workaround for this issue.

“rpc.statd” in the “nfs-utils” RPM in the various Linux distributions does not properly cleanse the untrusted format strings (3335691)

"rpc.statd” in the “nfs-utils” RPM in various Linux distributions does not properly cleanse untrusted format strings. This vulnerability may allow remote attackers to gain root privileges.

Workaround: Update to version 0.1.9.1 of the “nfs-utils” RPM to correct the problem.

Replication known issues

This section describes the replication known issues in this release of Symantec Storage Foundation and High Availability Solutions.

RVGPrimary agent operation to start replication between the original Primary and the bunker fails during failback (2036605)

The RVGPrimary agent initiated operation to start replication between the original Primary and the bunker fails during failback – when migrating back to the original Primary after disaster recovery – with the error message:

```
VxVM VVR vxrlink ERROR V-5-1-5282 Error getting information from
remote host. Internal Error.
```

The issue applies to global clustering with a bunker configuration, where the bunker replication is configured using storage protocol. It occurs when the Primary comes back even before the bunker disk group is imported on the bunker host to initialize the bunker replay by the RVGPrimary agent in the Secondary cluster.

Workaround:

To resolve this issue

1. Before failback, make sure that bunker replay is either completed or aborted.
2. After failback, deport and import the bunker disk group on the original Primary.
3. Try the start replication operation from outside of VCS control.

Bunker replay did not occur when the Application Service Group was configured on some of the systems in the Primary cluster, and ClusterFailoverPolicy is set to "AUTO" (2036644)

The time that it takes for a global cluster to fail over an application service group can sometimes be smaller than the time that it takes for VVR to detect the configuration change associated with the primary fault. This can occur in a bunkered, globally clustered configuration when the value of the `ClusterFailoverPolicy` attribute is `Auto` and the `AppGroup` is configured on a subset of nodes of the primary cluster.

This causes the RVGPrimary online at the failover site to fail. The following messages appear in the VCS engine log:

```
RVGPrimary:RVGPrimary:online:Diskgroup bunkerdgname could not be
imported on bunker host hostname. Operation failed with error 256
and message VxVM VVR vradmin ERROR V-5-52-901 NETWORK ERROR: Remote
server unreachable... Timestamp VCS ERROR V-16-2-13066 (hostname)
Agent is calling clean for resource(RVGPrimary) because the resource
is not up even after online completed.
```

Workaround:

To resolve this issue

- When the configuration includes a bunker node, set the value of the `OnlineRetryLimit` attribute of the RVGPrimary resource to a non-zero value.

A snapshot volume created on the Secondary, containing a VxFS file system may not mount in read-write mode and performing a read-write mount of the VxFS file systems on the new Primary after a global clustering site failover may fail [3761497]

Issue 1:

When the `vradmin ibc` command is used to take a snapshot of a replicated data volume containing a VxFS file system on the Secondary, mounting the snapshot volume in read-write mode may fail with the following error:

```
UX:vxfs mount: ERROR: V-3-21268: /dev/vx/dsk/dg/snapshot_volume
is corrupted. needs checking
```

This happens because the file system may not be quiesced before running the `vradmin ibc` command and therefore, the snapshot volume containing the file system may not be fully consistent.

Issue 2:

After a global clustering site failover, mounting a replicated data volume containing a VxFS file system on the new Primary site in read-write mode may fail with the following error:

```
UX:vxfs mount: ERROR: V-3-21268: /dev/vx/dsk/dg/data_volume
is corrupted. needs checking
```

This usually happens because the file system was not quiesced on the original Primary site prior to the global clustering site failover and therefore, the file systems on the new Primary site may not be fully consistent.

Workaround: The following workarounds resolve these issues.

For issue 1, run the `fsck` command on the snapshot volume on the Secondary, to restore the consistency of the file system residing on the snapshot.

For example:

```
# fsck -t vxfs /dev/vx/dsk/dg/snapshot_volume
```

For issue 2, run the `fsck` command on the replicated data volumes on the new Primary site, to restore the consistency of the file system residing on the data volume.

For example:

```
# fsck -t vxfs /dev/vx/dsk/dg/data_volume
```

Transactions on VVR secondary nodes may timeout waiting for I/O drain [3236772]

If the VVR secondary node receives updates out of order from the Primary, and a transaction starts on the secondary site, then the transaction may timeout waiting for I/O drain. This issue may occur in situations where the gaps created by out of order updates are not filled within the transaction timeout period.

Workaround:

Pause replication and make configuration changes.

In an IPv6-only environment RVG, data volumes or SRL names cannot contain a colon (1672410, 1672417, 1825031)

Issue: After upgrading VVR to an IPv6-only environment in release 6.0 or later, `vradmin` commands may not work when a colon is specified in the RVG, data volume(s) and/or SRL name. It is also possible that after upgrading VVR to an IPv6-only environment, `vradmin createpri` may dump core when provided with RVG, volume and/or SRL names containing a colon in it.

Workaround: Make sure that colons are not specified in the volume, SRL, and RVG names in the VVR configuration

vxassist relayout removes the DCM (145413)

If you perform a relayout that adds a column to a striped volume that has a DCM, the DCM is removed. There is no message indicating that this has happened. To replace the DCM, enter the following:

```
#vxassist -g diskgroup addlog vol logtype=dcm
```

vradmin functionality may not work after a master switch operation [2158679]

In certain situations, if you switch the master role, `vradmin` functionality may not work. The following message displays:

```
VxVM VVR vxrlink ERROR V-5-1-15861  Command is not supported for
command shipping. Operation must be executed on master
```

Workaround:

To restore vradmin functionality after a master switch operation

1 Restart `vradmind` on all cluster nodes. Enter the following:

```
# /etc/init.d/vras-vradmind.sh restart
```

2 Re-enter the command that failed.

Cannot relayout data volumes in an RVG from concat to striped-mirror (2129601)

This issue occurs when you try a relayout operation on a data volume which is associated to an RVG, and the target layout is a striped-mirror.

Workaround:

To relayout a data volume in an RVG from concat to striped-mirror

1 Pause or stop the applications.

2 Wait for the RLINKs to be up to date. Enter the following:

```
# vxrlink -g diskgroup status rlink
```

3 Stop the affected RVG. Enter the following:

```
# vxrvg -g diskgroup stop rvg
```

4 Disassociate the volumes from the RVG. Enter the following:

```
# vxvol -g diskgroup dis vol
```

5 Relayout the volumes to striped-mirror. Enter the following:

```
# vxassist -g diskgroup relayout vol layout=stripe-mirror
```

6 Associate the data volumes to the RVG. Enter the following:

```
# vxvol -g diskgroup assoc rvg vol
```

7 Start the RVG. Enter the following:

```
# vxrvg -g diskgroup start rvg
```

8 Resume or start the applications.

vradmin verifydata operation fails when replicating between versions 5.1 and 6.0 (2360713)

When replicating in a cross-version VVR environment consisting of hosts running Storage Foundation 5.1 and hosts running Storage Foundation 6.0, the `vradmin verifydata` command fails with the following error:

```
VxVM VVR vxrsync ERROR V-5-52-2222 [from host]: VxVM in.vxrsyncd
ERROR V-5-36-2125 Server volume access error during [assign volids]
volume path: [/dev/vx/dsk/dg/snapshot_volume] reason: [this could be
because a target volume is disabled or an rlink associated with a
target volume is not detached during sync operation].
```

Workaround: There are two workarounds for this issue.

- Upgrade the hosts running Storage Foundation 5.1 to Storage Foundation 5.1SP1 or later and re-run the `vradmin verifydata` command.
- Follow the offline verification procedure in the "Verifying the data on the Secondary" section of the *Symantec Storage Foundation and High Availability Solutions Replication Administrator's Guide*. This process requires ensuring that the secondary is up-to-date, pausing replication, and running the `vradmin syncrvg` command with the `-verify` option.

vradmin verifydata may report differences in a cross-endian environment (2834424)

When replicating between two nodes in a cross-platform environment, and performing an autosync or replication, the vradmin verifydata command may report differences. This is due to different endianness between the platforms. However, the file system on the secondary node will be consistent and up to date.

vradmin verifydata operation fails if the RVG contains a volume set (2808902)

In a VVR environment, the `vradmin verifydata` command fails with the following error if the replicated volume group (RVG) contains any volume set:

```
Message from Primary:
VxVM VVR vxrsync ERROR V-5-52-2009 Could not open device
/dev/vx/dsk/vvrdg/<volname> due to: stat of raw character volume path
failed
```

Plex reattach operation fails with unexpected kernel error in configuration update (2791241)

In a VVR environment with layered volumes, if a DCM plex becomes detached because of a storage failure, reattaching the plex after fixing the storage issue fails with the following error:

```
VxVM vxplex ERROR V-5-1-10128  Unexpected kernel error in configuration
update
```

Workaround:

There is no workaround for this issue.

Bunker replay does not occur with volume sets (3329970)

There are issues with bunker replication using Volume Replicator (VVR) with volume sets. Do not upgrade to Symantec Storage Foundation HA 6.2.1 if you have configured or plan to configure bunker replication using VVR with volume sets.

Workaround:

Contact Symantec Technical Support for a patch that enables you to use this configuration.

SmartIO does not support write-back caching mode for volumes configured for replication by Volume Replicator (3313920)

SmartIO does not support write-back caching mode for volumes that are configured for replication by Volume Replicator (VVR).

Workaround:

If you have configured volumes for replication by VVR, do not enable write-back caching

During moderate to heavy I/O, the vradmin verifydata command may falsely report differences in data (3270067)

While an application is online at the Volume Replicator primary site, the `vradmin verifydata` command may fail. The command output shows the differences between the source data volume and the target data volume.

Workaround:

The reason for this error is that the cache object that is used for the verification might be under allocated. You might need to allocate more space for the shared cache object. For guidelines on shared cache object allocation, see the section "Creating a shared cache object" in the *Symantec Storage Foundation Administrator's Guide*.

The vradmin repstatus command does not show that the SmartSync feature is running [3343141]

In a Volume Replicator (VVR) environment, after you start the initial synchronization with the `vradmin -a startrep` command with file system mounted on the primary data volumes, the `vradmin repstatus` command does not show that the SmartSync feature is running. This is an only issue with the output of the `vradmin repstatus` command.

Workaround:

To confirm that SmartSync is running, enter:

```
vxrlink status rlink
```

While vradmin commands are running, vradmind may temporarily lose heartbeats (3347656, 3724338)

This issue may occasionally occur when you use `vradmin` commands to administer Volume Replicator (VVR). While the `vradmin` commands run, `vradmind` may temporarily lose heartbeats, and the commands terminate with the following error message:

```
VxVM VVR vradmin ERROR V-5-52-803 Lost connection to host host;
terminating command execution.
```

Workaround:

To resolve this issue:

1. Depending on the application I/O workload and the network environment, uncomment and increase the value of the `IPM_HEARTBEAT_TIMEOUT` variable in the`/etc/vx/vras/vras_env` on all the hosts of the replicated data set (RDS) to a higher value. The following example increases the timeout value to 120 seconds:

   ```
   export IPM_HEARTBEAT_TIMEOUT
   IPM_HEARTBEAT_TIMEOUT=120
   ```

2. Restart `vradmind` on all the hosts of the RDS to put the new`IPM_HEARTBEAT_TIMEOUT` value into affect. Enter the following on all the hosts of the RDS:

   ```
   # /etc/init.d/vras-vradmind.sh stop
   # /etc/init.d/vras-vradmind.sh start
   ```

Write I/Os on the primary logowner may take a long time to complete (2622536)

Under a heavy I/O load, write I/Os on the Volume Replicator (VVR) primary logowner take a long time to complete.

Workaround:

There is no workaround for this issue.

After performing a CVM master switch on the secondary node, both rlinks detach (3642855)

If the VVR logowner (master) node on the secondary site goes down during initial synchronization, then during the RVG recovery (initiated on any secondary side node as a result of node crash), the replication links detach with the following error:

```
WARNING: VxVM VVR vxio V-5-0-187 Incorrect magic number or unexpected
upid (1) rvg rvg1
WARNING: VxVM VVR vxio V-5-0-287 rvg rvg1, SRL srl1: Inconsistent log
 - detaching all rlinks.
```

Workaround:

Restart replication using the autosync operation.

`vradmin -g dg repstatus` rvg displays the following configuration error: vradmind not reachable on cluster peer (3648854)

`vradmin -g dg rep` status rvg displays the following configuration error:

vradmind is not reachable on the cluster peer

However, replication is an ongoing process. The reason is that an unclean disconnect left the `vradmind` port open and in the **TIME_WAIT** state. An instance is as following:

```
# netstat -n | grep 8199
tcp        0      0 1:44781    1:8199
TIME_WAIT
tcp        0      0 1:44780    1:8199
TIME_WAIT
```

The following error message appear in **/var/vx/vras/log/vradmind_log_A**:

```
VxVM VVR Notice V-5-20-0 TAG_D IpmHandle:recv peer closed errno=0
VxVM VVR Debug V-5-20-8690 VRASCache TAG_E Cache_RLink
repstatus UPDATE message created for rlink rlk_192.168.111.127_rvg1
VxVM VVR Warning V-5-20-0 TAG_C IpmHandle::handleTo
vvr_sock_host_serv failed for l111031
VxVM VVR Warning V-5-20-0 TAG_C IpmHandle::open: getaddrinfo
error(could not resolve srchost l111032, error: Connection refused)
```

Workaround: Restart the `vradmind` daemon.

```
/etc/init.d/vras-vradmind.sh stop
/etc/init.d/vras-vradmind.sh start
```

The RVGPrimary agent may fail to bring the application service group online on the new Primary site because of a previous primary-elect operation not being run or not completing successfully (3761555, 2043831)

In a primary-elect configuration, the RVGPrimary agent may fail to bring the application service groups online on the new Primary site, due to the existence of previously-created instant snapshots. This may happen if you do not run the `ElectPrimary` command to elect the new Primary or if the previous `ElectPrimary` command did not complete successfully.

Workaround: Destroy the instant snapshots manually using the `vxrvg -g` *`dg`* `-P` *`snap_prefix`* `snapdestroy` *`rvg`* command. Clear the application service group and bring it back online manually.

A snapshot volume created on the Secondary, containing a VxFS file system may not mount in read-write mode and performing a read-write mount of the VxFS file systems on the new Primary after a global clustering site failover may fail (1558257)

Issue 1:

When the `vradmin ibc` command is used to take a snapshot of a replicated data volume containing a VxFS file system on the Secondary, mounting the snapshot volume in read-write mode may fail with the following error:

```
UX:vxfs mount: ERROR: V-3-21268: /dev/vx/dsk/dg/snapshot_volume
is corrupted. needs checking
```

This happens because the file system may not be quiesced before running the `vradmin ibc` command and therefore, the snapshot volume containing the file system may not be fully consistent.

Issue 2:

After a global clustering site failover, mounting a replicated data volume containing a VxFS file system on the new Primary site in read-write mode may fail with the following error:

```
UX:vxfs mount: ERROR: V-3-21268: /dev/vx/dsk/dg/data_volume
is corrupted. needs checking
```

This usually happens because the file system was not quiesced on the original Primary site prior to the global clustering site failover and therefore, the file systems on the new Primary site may not be fully consistent.

Workaround: The following workarounds resolve these issues.

For issue 1, run the `fsck` command on the snapshot volume on the Secondary, to restore the consistency of the file system residing on the snapshot.

For example:

```
# fsck -t vxfs /dev/vx/dsk/dg/snapshot_volume
```

For issue 2, run the `fsck` command on the replicated data volumes on the new Primary site, to restore the consistency of the file system residing on the data volume.

For example:

```
# fsck -t vxfs /dev/vx/dsk/dg/data_volume
```

Symantec Storage Foundation and High Availability known issues

Cache area is lost after a disk failure (3158482)

SmartIO supports one VxFS cache area and one VxVM cache area. If you create one cache area, and the disk fails, the cache area becomes disabled. If you attempt to create a second cache area of the other type before the cache disk group is enabled, then the first cache area is lost. It cannot be brought online.

For example, first you created a VxFS cache area. The disk failed and the cache area is disabled. Now create the VxVM cache area. While creating VxVM cache area, SmartIO looks for an existing default cache area. Due to the failed disk, the existing cache area cannot be found. So SmartIO creates a VxVM cache area with the same name. Now even if disk containing VxFS cache area comes up, SmartIO cannot access the original cache area. In this scenario, the VxFS cache area is lost. Losing the cache area in this case does not result into any data loss or data inconsistency issues.

Workaround:

Create a new VxFS cache area.

Installer exits upgrade to 5.1 RP1 with Rolling Upgrade error message (1951825, 1997914)

Installer exits upgrade to 5.1 RP1 with Rolling Upgrade error message, if protocol version entries are present in `/etc/gabtab` and `/etc/vxfenmode` files. Installer program may exit with either one of the following error messages during upgrade from 5.1 to 5.1 RP1:

```
SF51 is installed. Rolling upgrade is only supported from 5.1 to
higher version for the products
```

Or

```
To do rolling upgrade, VCS must be running on <node>.
```

Workaround: If the protocol version entries are present in `/etc/gabtab` and `/etc/vxfenmode` files, then installer detects it as Rolling Upgrade (RU). If you are not attempting RU, and doing full upgrade to 5.1 RP1, remove the protocol version entries from these two files for installer to proceed with regular upgrade.

In an IPv6 environment, db2icrt and db2idrop commands return a segmentation fault error during instance creation and instance removal (1602444)

When using IBM DB2 `db2icrt` command to create a DB2 database instance on a pure IPv6 environment, the `db2icrt` command returns segmentation fault error message. For example:

```
$ /opt/ibm/db2/V9.5/instance/db2icrt -a server -u db2fen1 db2inst1
/opt/ibm/db2/V9.5/instance/db2iutil: line 4700: 26182 Segmentation fault
$ {DB2DIR?}/instance/db2isrv -addfcm -i ${INSTNAME?}
```

The `db2idrop` command also returns segmentation fault, but the instance is removed successfully after the `db2idrop` command is issued. For example:

```
$ /opt/ibm/db2/V9.5/instance/db2idrop db2inst1
/opt/ibm/db2/V9.5/instance/db2iutil: line 3599:  7350 Segmentation fault
$ {DB2DIR?}/instance/db2isrv -remove -s DB2_${INSTNAME?} 2> /dev/null

DBI1070I  Program db2idrop completed successfully.
```

This happens on DB2 9.1, 9.5, and 9.7.

This issue has been identified as an IBM issue. Once IBM has fixed this issue, then IBM will provide a hotfix for this segmentation problem.

At this time, you can communicate in a dual-stack to avoid the segmentation fault error message until IBM provides a hotfix.

To communicate in a dual-stack environment

- Add an IPv6 hostname as an IPv4 loopback address to the /etc/hosts file. For example:

  ```
  127.0.0.1 swlx20-v6
  ```

  Or

  ```
  127.0.0.1 swlx20-v6.punipv6.com
  ```

  127.0.0.1 is the IPv4 loopback address.

  swlx20-v6 and swlx20-v6.punipv6.com are the IPv6 hostnames.

Process start-up may hang during configuration using the installer (1678116)

After you have installed a Storage Foundation product, some Veritas Volume Manager processes may hang during the configuration phase.

Workaround: Kill the installation program, and rerun the configuration.

Oracle 11gR1 may not work on pure IPv6 environment (1819585)

There is problem running Oracle 11gR1 on a pure IPv6 environment.

Tools like dbca may hang during database creation.

Workaround: There is no workaround for this, as Oracle 11gR1 does not fully support pure IPv6 environment. Oracle 11gR2 release may work on a pure IPv6 enviroment, but it has not been tested or released yet.

Not all the objects are visible in the VOM GUI (1821803)

After upgrading SF stack from 5.0MP3RP2 to 5.1, the volumes are not visible under the Volumes tab and the shared diskgroup is discovered as Private and Deported under the Diskgroup tab in the VOM GUI.

Workaround:

To resolve this known issue

- On each manage host where VRTSsfmh 2.1 is installed, run:

  ```
  # /opt/VRTSsfmh/adm/dclisetup.sh -U
  ```

An error message is received when you perform off-host clone for RAC and the off-host node is not part of the CVM cluster (1834860)

There is a known issue when you try to perform an off-host clone for RAC and the off-host node is not part of the CVM cluster. You may receive a similar error message:

```
Cannot open file /etc/vx/vxdba/rac11g1/.DB_NAME
(No such file or directory).
SFORA vxreptadm ERROR V-81-8847 Cannot get filename from sid
for 'rac11g1', rc=-1.
SFORA vxreptadm ERROR V-81-6550 Could not connect to repository
database.
VxVM vxdg ERROR V-5-1-582 Disk group SNAP_rac11dg1: No such disk
group SFORA
vxsnapadm ERROR V-81-5623 Could not get CVM information for
SNAP_rac11dg1.
SFORA dbed_vmclonedb ERROR V-81-5578 Import SNAP_rac11dg1 failed.
```

Workaround: Currently there is no workaound for this known issue. However, if the off-host node is part of the CVM cluster, then off-host clone for RAC works fine.

Also the `dbed_vmclonedb` command does not support LOCAL_LISTENER and REMOTE_LISTENER in the `init.ora` parameter file of the primary database.

A volume's placement class tags are not visible in the Veritas Enterprise Administrator GUI when creating a dynamic storage tiering placement policy (1880081)

A volume's placement class tags are not visible in the Veritas Enterprise Administrator (VEA) GUI when you are creating a SmartTier placement policy if you do not tag the volume with the placement classes prior to constructing a volume set for the volume.

Workaround: To see the placement class tags in the VEA GUI, you must tag the volumes prior to constructing the volume set. If you already constructed the volume set before tagging the volumes, restart `vxsvc` to make the tags visible in the GUI.

Symantec Cluster Server known issues

This section describes the known issues in this release of Symantec Cluster Server (VCS).

- Operational issues for VCS

- Issues related to the VCS engine
- Issues related to the bundled agents
- Issues related to the VCS database agents
- Issues related to the agent framework
- Issues related to Intelligent Monitoring Framework (IMF)
- Issues related to global clusters
- VCS Cluster Configuration wizard issues
- Issues related to the Cluster Manager (Java Console)

Operational issues for VCS

This section describes the Operational known issues for VCS.

LVM SG transition fails in all paths disabled status [2081430]

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

Workaround: You need to restore at least one path.

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

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

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

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 *Symantec 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.

Switching service group with DiskGroup resource causes reservation conflict with UseFence set to SCSI3 and powerpath environment set [2749136]

If UseFence is set to SCSI3 and powerpath environment is set, then switching the service group with DiskGroup resource may cause following messages to appear in syslog:

```
reservation conflict
```

This is not a SFHA Solutions issue. In case UseFence is set to SCSI3, the diskgroups are imported with the reservation. This message gets logged while releasing and reserving the disk.

Workaround: See the tech note available at http://www.symantec.com/business/support/index?page=content&id=TECH171786.

Stale NFS file handle on the client across failover of a VCS service group containing LVMLogicalVolume resource (2016627)

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

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

NFS cluster I/O fails when storage is disabled [2555662]

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.

VVR configuration may go in a primary-primary configuration when the primary node crashes and restarts [3314749]

The AutoResync attribute of the RVGPrimary and RVGSharedPri agent control whether the agent must attempt to automatically perform a fast-failback resynchronization of the original primary after a takeover and after the original primary returns. The default value of this attribute is 0, which instructs the agent not to perform a fast-failback resynchronization of the original primary after a takeover and after the original primary returns. The takeover is performed automatically since the default value of the AutoTakeover attribute of the RVGPrimary and RVGShared agents is 1. Thus, the default settings of AutoTakeover and AutoResync set to 1 and 0 respectively cause the first failover to succeed when the original primary goes down, and on return of the original primary, the Replicated Data Set (RDS) ends up with a primary-primary configuration error.

Workaround: Set the default value of the AutoResync attribute of the RVGPrimary agent to 1 (one) when you want the agent to attempt to automatically perform a fast-failback resynchronization of the original primary after a takeover and after the original primary returns. This prevents the primary-primary configuration error. Do not set AutoResync to 1 (one) if you intend to use the Primary-Elect feature.

Moreover, if you want to prevent VCS from performing an automatic takeover and fast-failback resynchronization, set AutoTakeover and AutoResync attributes to 0 for all the RVGPrimary and RVGSharedPri resources in your VCS configuration. For more information, refer to the RVGPrimary and RVGSharedPri agent sections of the *Replication Agents chapter*in the *Symantec Cluster Server Bundled Agents Reference Guide*.

CP server does not allow adding and removing HTTPS virtual IP or ports when it is running [3322154]

CP server does not support adding and removing HTTPS virtual IPs or ports while the CP server is running. However, You can add or remove the IPM virtual IPs or ports.

Workaround: No workaround. If you want to add a new virtual IP for HTTPS, you must follow the entire manual procedure for generating HTTPS certificate for the CP server (server.crt), as documented in the *Symantec Cluster Server Installation Guide*.

CP server does not support IPv6 communication with HTTPS protocol [3209475]

CP server does not support IPv6 communication when using the HTTPS protocol. This implies that in VCS 6.1, CP servers listening on HTTPS can only use IPv4. As a result, VCS 6.1 fencing clients can also use only IPv4.

Workaround: No workaround.

VCS fails to stop volume due to a transaction ID mismatch error [3292840]

If VCS imports a disk group *A* on node *sys1*, which implies that the DiskGroup resource is online on *sys1*. If you run `vxdg -C import <dg_name>` outside VCS on node *sys2*, then the disk group gets imported on node *sys2* and `-C` clears the import locks and host tag. However on node *sys1*, disk group *A* continues to appear as imported and enabled, and hence, VCS continues to report the resource state as ONLINE on node *sys1*. Subsequently, when VCS detects the imported disk group on *sys2*, it deports the disk group from *sys2*, and imports it on *sys1* to resolve concurrency violation. At this point, the disk group deported from node *sys2* is shown as imported and enabled on node *sys1*. If you stop any volume from within or outside VCS, it fails with the `Transaction ID mismatch` error, but the read and write operations continue to function so the data continues to be accessible. This situation may lead to data corruption if the disk group appears enabled on multiple nodes. This issue is due to the Volume Manager behavior.

Workaround: Do not import a disk group using `-C` option if that diskgroup is under VCS control.

Some VCS components do not work on the systems where a firewall is configured to block TCP traffic [3545338]

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

Issues related to the VCS engine

This section describes the knonw issues about the VCS engine.

Extremely high CPU utilization may cause HAD to fail to heartbeat to GAB [1744854]

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

The hacf -cmdtocf command generates a broken main.cf file [1919951]

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

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

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 [2653688]

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 parent 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 [2490331]

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: Terminate 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.

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.

Elevated TargetCount prevents the online of a service group with `hagrp -online -sys` command [2871892]

When you initiate an offline of a service group and before the offline is complete, if you initiate a forced flush, the offline of the service group which was initiated earlier is treated as a fault. As start bits of the resources are already cleared, service group goes to OFFLINE|FAULTED state but TargetCount remains elevated.

Workaround: No workaround.

Auto failover does not happen in case of two successive primary and secondary cluster failures [2858187]

In case of three clusters (clus1, clus2, clus3) in a GCO with steward not configured, if clus1 loses connection with clus2, it sends the inquiry to clus3 to check the state of clus2 one of the following condition persists:

1. If it is able to confirm that clus2 is down, it will mark clus2 as FAULTED.
2. If it is not able to send the inquiry to clus3, it will assume that a network disconnect might have happened and mark clus2 as UNKNOWN

In second case, automatic failover does not take place even if the ClusterFailoverPolicy is set to Auto. You need to manually failover the global service groups.

Workaround: Configure steward at a geographically distinct location from the clusters to which the above stated condition is applicable.

GCO clusters remain in INIT state [2848006]

GCO clusters remain in INIT state after configuring GCO due to :

- Trust between two clusters is not properly set if clusters are secure.
- Firewall is not correctly configured to allow WAC port (14155).

Workaround: Make sure that above two conditions are rectified. Refer to *Symantec Cluster Server Administrator's Guide* for information on setting up Trust relationships between two clusters.

The `ha` commands may fail for non-root user if cluster is secure [2847998]

The `ha` commands fail to work for one of the following reasons:

- If you first use a non-root user without a home directory and then create a home directory for the same user.
- If you configure security on a cluster and then un-configure and reconfigure it.

Workaround

1. Delete /var/VRTSat/profile/<user_name>,
2. Delete /home/user_name/.VRTSat.
3. Delete /var/VRTSat_lhc/<cred_file> file which same non-root user owns.
4. Run `ha` command with same non-root user (this will pass).

Running `-delete -keys` for any scalar attribute causes core dump [3065357]

Running `-delete -keys` for any scalar attribute is not a valid operation and must not be used. However, any accidental or deliberate use of this command may cause engine to core dump.

Workaround: No workaround.

SFHA Solutions enters into admin_wait state when Cluster Statistics is enabled with load and capacity defined [3199210]

SFHA Solutions enters into admin_wait state when started locally if:

1. Statistics attribute value is set to Enabled, which is its default value.

2. Group Load and System Capacity values are defined in units in `main.cf`.

Workaround:

1. Stop SFHA Solutions on all nodes in the cluster.
2. Perform any one of the following steps:
   - Edit the `main.cf` on one of the nodes in the cluster and set the Statistics attribute to Disabled or MeterHostOnly.
   - Remove the Group Load and System Capacity values from the `main.cf`.
3. Run `hacf -verify` on the node to verify that the configuration is valid.
4. Start SFHA Solutions on the node and then on the rest of the nodes in the cluster.

Agent reports incorrect state if VCS is not set to start automatically and `utmp` file is empty before VCS is started [3326504]

If you have not configured VCS to start automatically after a reboot and have tmptied the `utmp` file before starting VCS manually with the hastart command, some agents might report an incorrect state.

The `utmp` file (file name may differ on different operating systems) is used to maintain a record of the restarts done for a particular machine. The checkboot utility used by `hastart` command uses the functions provided by the OS which in turn use the `utmp` file to find if a system has been restarted so that the temporary files for various agents can be deleted before agent startup. If OS functions do not return correct value, High Availability Daemon (HAD) starts without deleting the stale agent files. This might result in some agents reporting incorrect state.

Workaround: If a user wishes to delete the `utmp` file this should be done only when VCS is already running or the customer should delete the temporary files in`/var/VRTSvcs/lock/volatile/` manually before starting VCS.

Site preference fencing policy value fails to set on restart of a site-aware cluster [3380586]

If you restart VCS on a site-aware cluster, the PreferredFencingPolicy fails to reset to the value ‘Site’ assigned to it before the restart.

Workaround: Reassign the fencing policy value manually to the cluster.

Log messages are seen on every systemctl transaction on RHEL7 [3609196]

On RHEL7 systems, a log message stating `VCS dependency is not met` is logged in system logs with every `systemctl` transaction. Currently, all the `init` scrips for VCS modules (such as LLT, GAB, I/O fencing, and AMF) bypass systemctl.

However, systemctl attempts to validate the dependency check before bypassing the service start operation. This generates the log messages in the system log.

Workaround: You can ignore the log messages as they do not affect the init script operation.

VCS crashes if feature tracking file is corrupt [3603291]

VCS keeps a track of some specific features used in the VCS cluster. For example, if a Global service group is brought online then the feature is logged in a specific feature tracking file. If the file however is corrupt, then VCS may dump core when attempting to write data to the file.

Workaround: Delete the corrupt feature tracking file (/var/vx/vftrk/vcs) and restart VCS.

RemoteGroup agent on versions lower than 6.2 reports service group status as UNKNOWN [3638347]

When the RemoteGroup agent running on a VCS version lower than 6.2 tries to monitor a service group on a 6.2 cluster, it reports the service group status as UNKNOWN.

Workaround: No workaround.

RemoteGroup agent and non-root users may fail to authenticate after a secure upgrade [3649457]

On upgrading a secure cluster to 6.2, the following issues may occur with unable to open a secure connection error:

- The RemoteGroup agent may fail to authenticate with remote cluster.
- Non-root users may fail to authenticate.

Workaround

1. Set LC_ALL=C on all nodes before upgrade or perform the following steps after the upgrade on all nodes of the cluster:
    - Stop HAD.
    - Set LC_ALL=C.
    - Start HAD using hastart.
2. Reset LC_ALL attribute to the previous value once the non-root users are validated.

Global Cluster Option (GCO) require NIC names in specific format [3641586]

The `gcoconfig` script requires the NIC names in the letters followed by numbers format. For example, NIC names can be `eth0`, `eth123`, `xyz111` and so on. The script fails to configure GCO between NICs which do not comply with this naming format.

Workaround: Rename the NIC name and use the letters followed by numbers format to configure GCO.

Issues related to the bundled agents

This section describes the known issues of the bundled agents.

LVM Logical Volume will be auto activated during I/O path failure [2140342]

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

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

KVMGuest monitor entry point reports resource ONLINE even for corrupted guest or with no OS installed inside guest [2394235]

The VCS KVMGuest monitor entry point reports resource state as ONLINE in spite of the operating system inside the guest being corrupted or even if no operating system is installed inside the guest. The VCS KVMGuest agent uses `virsh` utility to determine the state of the guest. When the guest is started, the `virsh` utility reports the state of the running guest as running. Based on this running state, VCS KVMGuest agent monitor entry point reports the resource state as ONLINE.

In case the operating system is not installed inside the guest or the installed operating system is corrupted, `virsh` utility still reports the guest state as running. Thus, VCS also reports the resource state as ONLINE. Since RedHat KVM does not provide the state of the operating system inside guest, VCS cannot detect the guest state based on the state of the operating system.

Workaround: No workaround for this known issue.

Concurrency violation observed during migration of monitored virtual machine [2755936]

If a VCS service group has more than one KVMGuest resource monitoring virtual machine and one of the virtual machines is migrated to another host, a service group level concurrency violation occurs as the service group state goes into PARTIAL state on multiple nodes.

Workaround: Configure only one KVMGuest resource in a Service group.

LVM logical volume may get stuck with reiserfs file system on SLES11 [2120133]

LVM logical volume may get stuck with reiserfs file system on SLES11 if the service group containing the logical volume is switched continuously between the cluster node.

This issue may be observed:

- During the continuous switching of the service group having the LVM logical volume with reiserfs file system.
- On SLES11 and with reiserfs file system only.
- Due to the behavior of device-mapper on SLES11.

However, the issue is not consistent. Sometimes, the device-mapper gets stuck while handling the logical volumes and causes the logical volume to hang. In such a case, LVM2 commands also fail to clear the logical volume. VCS cannot handle this situation as the LVM2 commands are unable to deactivate the hung logical volume.

Resolution: You must restart the system on which the logical volumes are stuck in this situation.

KVMGuest resource comes online on failover target node when started manually [2394048]

The VCS KVMGuest resource comes online on failover target node when VM guest started manually, even though the resource is online on the primary node.

Kernel-based virtual machine (KVM) allows you to start the guest using same guest image on multiple nodes. The guest image is residing on the cluster file system. If the guest image is stored on the cluster file system, then it becomes available on all the cluster nodes simultaneously.

If the KVMGuest resource of VCS has made the guest online on one node by starting it using the guest image on cluster file system and if you manually start the same guest on the other node, KVM does not prevent you from doing so. However, as this particular guest is under VCS control, VCS does not allow the resource to be ONLINE on multiple nodes simultaneously (unless it is in parallel service group configuration). VCS detects this concurrency violation and brings down the guest on the second node.

Note: This issue is also observed with CVM raw volume.

Workaround: No workaround required in VCS. VCS concurrency violation mechanism handles this scenario appropriately.

DiskReservation agent may call clean if you configure large number of its resources in a single service group [2336391]

DiskReservation agent may call clean if you configure large number of DiskReservation resource (more than 400 resources) in a single service group and try to offline the service group.

In a single service group configuration with more than 400 DiskReservation resources and equal number of Mount resources, the service group offline may cause the DiskReservation agent to call clean entry point. This issue is not observed if you configure about 150 resources.

Workaround: No workaround.

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 *Symantec Cluster Server Administrator's Guide*.

DiskGroup agent is unable to offline the resource if volume is unmounted outside VCS

DiskGroup agent is unable to offline the resource if volume is unmounted using the `umount -l` command outside VCS.

A service group contains DiskGroup, Volume and Mount resources and this service group is online. Volume is mounted by Mount resource with VxFSMountLock enabled. An attempt to manually unmount the volume using `umount -l` system command causes the mount point to go away; however, the file system lock remains as it is. The volume cannot be stopped as it is mount locked and hence the disk group cannot be imported. This causes the disk group resource to go into UNABLE to OFFLINE state. Also, any attempt to again mount the file system fails, because it is already mount locked. This issue is due to file system behavior on Linux.

Workaround: Do not use `umount -l` command to unmount the VxFS file system when the mount lock is enabled. Instead, first unlock the mount point using the`/opt/VRTS/bin/fsadm` command and then unmount the file system.

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.

VVR setup with FireDrill in CVM environment may fail with CFSMount Errors [2564411]

When you try to bring the FireDrill service group online through Java Console or `hagrp -online` command, the CFSMount resource goes into faulted state.

Workaround: Run the `fsck` command.. You can find these commands in the engine logs.

CoordPoint agent remains in faulted state [2852872]

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

Workaround: After HAD has stopped, reconfigure fencing.

RVGsnapshot agent does not work with volume sets created using vxvset [2553505]

RVGsnapshot agent does not work with volume sets created using `vxvset`. This happens during FireDrill in a VVR einviroment.

Workaround: No workaround.

No log messages in engine_A.log if VCS does not find the Monitor program [2563080]

No message is logged in the engine_A.log, when VCS cannot find the Monitor program with KVM guest with service group online.

Workaround: In case resource state is unknown , also refer to agent log files for messages.

No IPv6 support for NFS [2022174]

IPv6 is not supported for NFS.

Workaround: No workaround.

KVMGuest agent fails to recognize paused state of the VM causing KVMGuest resource to fault [2796538]

In a SUSE KVM environment, when a virtual machine is saved, its state is changed to paused and then shut-off. The paused state remains for a very short period of time, due to timing in case that the KVMGuest agent misses this state. Then the resource state will be returned as OFFLINE instead of INTENTIONAL OFFLINE, which causes the KVMGuest resource to fault and failover.

This is due to the limitation of SUSE KVM as it does not provide a separate state for such events.

Workaround: No workaround.

Concurrency violation observed when host is moved to maintenance mode [2735283]

When a Red Hat Enterprise Virtualization host running a virtual machine is moved to maintenance state, the virtual machine migration is initiated by RHEV. SFHA Solutions detects the migration according to virtual machine state, such as "migrating". Due to timing issue RHEV Manager occasionally sends the virtual machine state as "up" even if the migration is in progress. Due to this state, the resource is marked ONLINE on the node to which it migrates and may cause concurrency violation.

Workaround: No workaround.

Logical volume resources fail to detect connectivity loss with storage when all paths are disabled in KVM guest [2871891]

In a KVM environment if all storage paths are disabled, then LVMLogicalVolume and LVMVolumeGroup resources fails to detect the loss of connectivity with the storage. This occurs because of LVM2 commands return success even if all the paths to storage are disabled. Moreover, the LVMVolumegroup and LVMLogicalVolume agents report the resource state as ONLINE.

Workaround: Verify the multi-pathing environment and make sure that all the read and write operations to the disk are blocked when all paths to the storage are disabled.

Resource does not appear ONLINE immediately after VM appears online after a restart [2735917]

During a VM restart the resource does not come ONLINE immediately after the VM starts running. As the VM state is 'Reboot in Progress' it reports INTENTIONAL OFFLINE and after VM is UP the resource cannot immediately detect it as the next monitor is scheduled after 300 seconds.

Workaround: Reduce the OfflineMonitorInterval and set it to suitable value.

Unexpected behavior in VCS observed while taking the disk online [3123872]

If the VMwareDisks resource is configured for a disk connected to another virtual machine outside of an ESX cluster and if you bring the disk online on the configured node, you may observe unexpected behavior of VCS (like LLT connection break). The behavior is due to a known issue in VMware.

Workaround: Remove the disk from the other virtual machine and try again.

LVMLogicalVolume agent clean entry point fails to stop logical volume if storage connectivity is lost [3118820]

If storage connectivity is lost on a system on which the LVM resources are in ONLINE state and a volume is mounted using the Mount resource, LVMVolumeGroup agent monitor entry point detects the loss of connectivity and returns the resource state as offline. This causes agent framework to call clean entry point of LVMVolumeGroup agent; however, the state of the resource stays online. Agent framework waits for the clean entry point to return success so that the resource can be moved to the offline|faulted state. At this stage, the clean entry point fails as it is not able deactivate and export the volume group because the logical volume is mounted. There is no option available to forcefully deactivate and export the volume group. Hence, the service groups get stuck in this state. Even if the storage connectivity is restored, the problem does not resolve because the logical volume remains mounted. If the logical volume is unmounted, then the LVMVolumeGroup resource goes into FAULTED state and service group fails over.

Workaround: Manually unmount the logical volume.

VM goes into paused state if the source node loses storage connectivity during migration [3085214]

During virtual machine migrations in a RHEV environment, the VM may freeze in paused state if the source host loses storage connectivity.This issue is specific to RHEV environment.

Workaround: No workaround.

Virtual machine goes to paused state during migration if the public network cable is pulled on the destination node [3080930]

The virtual machine goes into paused state during migration if the public network cable is pulled on the destination node. This behavior depends on the stage at which the migration is disrupted. The virtual machine rolls back to the source node if the network cable is pulled during migration. Resource on the source node reports this as an online virtual machine that is in running state. On the destination node, the virtual machine goes into shut-off state.

If the virtual machine migration gets disrupted during the transfer from source to destination, it may happen that the virtual machine remains in paused state on the source node. In such a case, you must manually clear the state of the virtual machine and bring the it online on any one node.

This operational issue is a behavior of the technology and has no dependency on SFHA Solutions. This behavior is observed even if the migration is invoked outside VCS control. Due to the disruption in virtual machine migration, it may happen that the locking mechanism does not allow the virtual machine to run on any host, but again, this is a virtualization technology issue.

Workaround: No workaround. Refer to the virtualization documentation.

NFS resource faults on the node enabled with SELinux and where rpc.statd process may terminate when access is denied to the PID file [3248903]

If SELinux is enabled on a system, it blocks `rpc.statd` process from accessing the PID file at `/var/run/rpc.statd.pid`. This may cause `rpc.statd` process to terminate on the system. NFS resource, which monitors the NFS services on the node, detects this and returns unexpected OFFLINE as `statd` process is not running. This is because SELinux does not allow `statd` process to access the PID file and may occur with VCS monitoring the NFS resources.

Workaround: There is no prescribed solution available from Red Hat. You can perform the following steps as a workaround for this issue:

1. Disable SELinux.
2. Use `audit2allow` utility to create a policy to allow access to `rpc.statd` process.
3. Run `semodule -i <policy_module_name>.pp` to install the policy module generated by `audit2allow` utility.

NFS client reports I/O error because of network split brain [3257399]

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

Workaround: Configure the preonline trigger for the service groups containing DiskGroup resource with reservation 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 the preonline trigger for the service group.

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

System having DiskReservation resource online panics with the loss of storage connectivity (3321322)

If the storage connectivity is lost on the system where DiskReservation resource is online, that system panics.

Workaround: No workaround.

Mount resource does not support spaces in the MountPoint and BlockDevice attribute values [3335304]

Mount resource does not handle intermediate spaces in the configured MountPoint or BlockDevice attribute values.

Workaround: No workaround.

LVMVolumeGroup agent does not report UNKNOWN if invalid volume group is configured [3246748]

VCS LVMVolumeGroup agent can identify whether configured volume group is valid or not based on the error code returned by the native LVM2 commands. If a DiskReservation resource is configured along with LVMVolumeGroup resource and is in online state on any of the node, then LVM2 commands from the node on which the resource is offline fail to read the disk. Hence, LVMVolumeGroup agent cannot validate the volume group. Currently, if LVM2 command returns failure, the resource state is returned as OFFLINE.

Workaround: No workaround.

Manual configuration of RHEVMInfo attribute of KVMGuest agent requires all its keys to be configured [3277994]

The RHEVMInfo attribute of KVMGuest agent has 6 keys associated with it. When you edit main.cf to configure RHEVMInfo attribute manually, you must make sure that all the keys of this attribute are configured in main.cf. If any of its keys is left unconfigured, the key gets deleted from the attribute and agent does not receive the complete attribute. Hence, it logs a Perl error `Use of uninitialized value` in the engine log. This is due to the VCS engine behavior of handling the attribute with key-value pair.

Workaround: Use `ha` commands to add or modify RHEVMInfo attribute of KVMGuest resource.

NFS lock failover is not supported on Linux [3331646]

If a file is locked from an NFS client, the other client may also get the lock on the same file after failover of the NFS share service group. This is because of the changes in the format of the lock files and the lock failover mechanism.

Workaround: No workaround.

SambaServer agent may generate core on Linux if LockDir attribute is changed to empty value while agent is running [3339231]

If LockDir attribute is changed to an empty value while agent is running and debugging is enabled, the logging function may access invalid memory address resulting in SambaServer agent to generate core dump.

Workaround: When LockDir attribute is changed while agent is running, ensure that its new value is set to a non-empty valid value.

Independent Persistent disk setting is not preserved during failover of virtual disks in VMware environment [3338702]

VMwareDisks agent supports Persistent disks only. Hence, Independent disk settings are not preserved during failover of virtual disk.

Workaround: No workaround.

LVMLogicalVolume resource goes in `UNABLE TO OFFLINE` state if native LVM volume group is exported outside VCS control [3606516]

If you export the LVM volume group without stopping LVM logical volumes, the LVMLogicalVolume resource falsely reports online. If offline is initiated for LVMLogicalVolume resource, it fails as the volume group was not exported cleanly and LVMLogicalVolume Agent fails to deactivate the logical volume causing LVMLogicalVolume to go in `UNABLE TO OFFLINE` state.

Workaround: Make sure volume group is deactivated and exported using VCS or manually deactivate the LVM logical volumes.

DiskGroup resource online may take time if it is configured along with VMwareDisks resource [3638242]

If a service group is configured with VMwareDisks and DiskGroup resource, the DiskGroup resource may take time to come online during the service group online. This is because VxVM takes time to recognize a new disk that is attached by VMwareDisks resource. A VMwareDisks resource attaches a disk to the virtual machine when the resource comes online and a DiskGroup resource, which depends on VMwareDisks resource, tries to import the disk group. If `vxconfigd` does not detect the new disk attached to the virtual machine, the DiskGroup resource online fails with the following error message because the resource is not up even after the resource online is complete.

```
VCS ERROR V-16-2-13066 ... Agent is calling clean for resource(...)
```

Workaround: Configure OnlineRetryLimit to appropriate value.

For example, if the DiskGroup resource name is `res_rawdg`:

```
# hares -override res_rawdg OnlineRetryLimit
# hares -modify res_rawdg  OnlineRetryLimit 2
```

SFCache Agent fails to enable caching if cache area is offline [3644424]

SFCache agent cannot enable caching if cache area associate with this particular object is in offline state. User need to manually online the cache area to make sure that caching can be enabled/disabled.

Workaround: Online the cache area using `sfcache` command

```
# sfcache online <cache_area_name>
```

RemoteGroup agent may stop working on upgrading the remote cluster in secure mode [3648886]

RemoteGroup agent may report the resource state as UNKNOWN if the remote cluster is upgraded to VCS 6.2 in secure mode.

Workaround: Restart the RemoteGroup agent.

VMwareDisks agent may fail to start or storage discovery may fail if SELinux is running in enforcing mode [3106376]

The VMwareDisks agent and discFinder binaries refer to the `libvmwarevcs.so`shared library. SELinux security checks prevent discFinder from loading the`libvmwarevcs.so` library, which requires text relocation. If SELinux is running in enforcing mode, these two executables may report the "Permission denied" error and may fail to execute.

Workaround: Enter the following command and relax the security check enforcement on the Symantec libvmwarevcs.so library:

```
# chcon -t textrel_shlib_t '/opt/VRTSvcs/lib/libvmwarevcs.so'
```

Issues related to the VCS database agents

This section describes the known issues about VCS database agents.

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 Symantec 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 *Symantec 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.

Oracle agent fails to offline pluggable database (PDB) resource with PDB in backup mode [3592142]

If the PDB is in backup mode and if you attempt to offline the corresponding PDB resource, this will cause PDB resource to go into “Unable to Offline” state.

Workaround: Manually remove the PDB from the backup mode before attempting to take the PDB resource offline.

Clean succeeds for PDB even as PDB staus is UNABLE to OFFLINE [3609351]

Oracle does not allow any operation on a PDB when the PDB is in backup mode. This is an expected behavior of Oracle. Therefore, a shutdown fails when it is initiated on a PDB in backup mode and returns an UNABLE TO OFFLINE status for the PDB. If PDB is removed from the backup mode using the SQL script, the agent framework is unable to change the UNABLE TO OFFLINE status of the PDB as clean is called. Since Oracle does not differntiate between clean and offline for PDB, clean succeeds for the PDB in spite of being in UNABLE TO OFFLINE state.

Workaround: No workaround.

Second level monitoring fails if user and table names are identical [3594962]

If the table inside CDB has same name as the user name, second level monitoring fails and Oracle agent fails to update the table. For example, if user name is `c##pdbuser1` and table is created as `c##pdbuser1.vcs`, then Oracle agent is unable to update it.

Workaround: Avoid having identical user and CDB table names.

Monitor entry point times out for Oracle PDB resources when CDB is moved to suspended state in Oracle 12.1.0.2 [3643582]

In Oracle-12.1.0.2.0, when CDB is in SUSPENDED mode, then the SQL command for PDB view (`v$pdbs`) hangs. Due to this, the monitor entry point in PDB gets timed out and there is no issue found in oracle-12.1.0.1.0 .

Workaround: No workaround.

Oracle agent fails to online and monitor Oracle instance if threaded_execution parameter is set to true [3644425]

In Oracle 12c, the threaded execution feature is enabled. The multithreaded Oracle Database model enables Oracle processes to execute as operating system threads in separate address spaces. If Oracle Database 12c is installed, the database runs in the process mode. If you set a parameter to run the database in threaded mode, some background processes on UNIX and Linux run with each process containing one thread, whereas the remaining Oracle processes run as threads within the processes.

When you enable this parameter, Oracle agent is unable to check smon (mandatory process check) and lgwr (optional process check) processes which where tradtionally used for monitoring and which now run as threads.

Workaround: Disable the threaded execution feature as it is no supported on Oracle 12C.

Issues related to the agent framework

This section describes the known issues about the agent framework.

Agent may fail to heartbeat under heavy load [2073018]

An agent may fail to heart beat with the VCS engine under heavy load.

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

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

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

Agent framework cannot handle leading and trailing spaces for the dependent attribute (2027896)

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 [1442255]

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.

Delayed response to VCS commands observed on nodes with several resources and system has high CPU usage or high swap usage [3208239]

You may experience a delay of several minutes in the VCS response to commands if you configure large number of resources for monitoring on a VCS node and if the CPU usage is close to 100 percent or swap usage is very high.

Some of the commands are mentioned below:

- `# hares -online`
- `# hares -offline`
- `# hagrp -online`
- `# hagrp -offline`
- `# hares -switch`

The delay occurs as the related VCS agent does not get enough CPU bandwidth to process your command. The agent may also be busy processing large number of pending internal commands (such as periodic monitoring of each resource).

Workaround: Change the values of some VCS agent type attributes which are facing the issue and restore the original attribute values after the system returns to the normal CPU load.

1. Back up the original values of attributes such as MonitorInterval, OfflineMonitorInterval, and MonitorFreq of IMF attribute.
2. If the agent does not support Intelligent Monitoring Framework (IMF), increase the value of MonitorInterval and OfflineMonitorInterval attributes.

   ```
   # haconf -makerw
   # hatype -modify <TypeName> MonitorInterval <value>
   # hatype -modify <TypeName> OfflineMonitorInterval <value>
   # haconf -dump -makero
   ```

   Where <TypeName> is the name of the agent with which you are facing delays and <value> is any numerical value appropriate for your environment.

3. If the agent supports IMF, increase the value of MonitorFreq attribute of IMF.

   ```
   # haconf -makerw
   # hatype -modify <TypeName> IMF -update MonitorFreq <value>
   # haconf -dump -makero
   ```

   Where <value> is any numerical value appropriate for your environment.

4. Wait for several minutes to ensure that VCS has executed all pending commands, and then execute any new VCS command.
5. If the delay persists, repeat step 2 or 3 as appropriate.
6. If the CPU usage returns to normal limits, revert the attribute changes to the backed up values to avoid the delay in detecting the resource fault.

CFSMount agent may fail to heartbeat with VCS engine and logs an error message in the engine log on systems with high memory load [3060779]

On a system with high memory load, CFSMount agent may fail to heartbeat with VCS engine resulting into V-16-1-53030 error message in the engine log.

VCS engine must receive periodic heartbeat from CFSMount agent to ensure that it is running properly on the system. The heartbeat is decided by AgentReplyTimeout attribute. Due to high CPU usage or memory workload (for example, swap usage greater than 85%), agent may not get enough CPU cycles to schedule. This causes heartbeat loss with VCS engine and as a result VCS engine terminates the agent and starts the new agent. This can be identified with the following error message in the engine log:

```
V-16-1-53030 Termination request sent to CFSMount
agent process with pid %d
```

Workaround: Increase the AgentReplyTimeout value and see if CFSMount agent becomes stable. If this does not resolve the issue then try the following workaround. Set value of attribute NumThreads to 1 for CFSMount agent by running following command:

```
# hatype -modify CFSMount NumThreads 1
```

Even after the above command if CFSMount agent keeps on terminating, report this to Symantec support team.

Logs from the script executed other than the agent entry point goes into the engine logs [3547329]

The agent logs of C-based and script-based entry points get logged in the agent log when the attribute value of LogViaHalog is set to 1 (one). To restore to the older logging behavior in which C-based entry point logs were logged in agent logs and script-based entry point logs were logged in engine logs, you can set the LogViaHalog value as 0 (zero). However, it is observed that some C-based entry point logs continue to appear in the engine logs even when LogViaHalog is set to 1 (one). This issue is observed on all the database agents.

Workaround: No workaround.

Issues related to Intelligent Monitoring Framework (IMF)

This section describes the known issues of 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 provide notification for a registered disk group if it is imported using a different name (2730774)

If a disk group resource is registered with the AMF and the disk group is then imported using a different name, AMF does not recognize the renamed disk group and hence does not provide notification to DiskGroup agent. Therefore, the DiskGroup agent keeps reporting the disk group resource as offline.

Workaround: Make sure that while importing a disk group, the disk group name matches the one registered with the AMF.

Direct execution of `linkamf` displays syntax error [2858163]

Bash cannot interpret Perl when executed directly.

Workaround: Run `linkamf` as follows:

```
# /opt/VRTSperl/bin/perl /opt/VRTSamf/imf/linkamf <destination-directory>
```

Error messages displayed during reboot cycles [2847950]

During some reboot cycles, the following message might get logged in the engine log:

```
AMF libvxamf ERROR V-292-2-149 Cannot unregister event: no rid -1 found
AMF libvxamf ERROR V-292-2-306 Unable to unregister all events (errno:405)
```

This does not have any effect on the functionality of IMF.

Workaround: No workaround.

Error message displayed when ProPCV prevents a process from coming ONLINE to prevent concurrency violation does not have I18N support [2848011]

The following message is seen when ProPCV prevents a process from coming ONLINE to prevent concurrency violation. The message is displayed in English and does not have I18N support.

```
Concurrency Violation detected by VCS AMF.
Process <process-details> will be prevented from startup.
```

Workaround: No Workaround.

AMF displays StartProgram name multiple times on the console without a VCS error code or logs [2872064]

When VCS AMF prevents a process from starting, it displays a message on the console and in syslog. The message contains the signature of the process that was prevented from starting. In some cases, this signature might not match the signature visible in the PS output. For example, the name of the shell script that was prevented from executing will be printed twice.

Workaround: No workaround.

Core dump observed when `amfconfig` is run with set and reset commands simultaneously [2871890]

When you run `amfconfig -S -R` on a node, a command core dump is observed, instead of displaying the correct usage of the command. However, this core dump has no effect on the AMF functionality on that node. You need to use the correct command syntax instead.

Workaround: Use the correct commands:

```
# amfconfig -S <options>
# amfconfig -R <options>
```

VCS engine shows error for cancellation of reaper when Apache agent is disabled [3043533]

When `haimfconfig` script is used to disable IMF for one or more agents, the VCS engine logs the following message in the engine log:

```
AMF imf_getnotification ERROR V-292-2-193
Notification(s) canceled for this reaper.
```

This is an expected behavior and not an issue.

Workaround: No workaround.

Terminating the `imfd` daemon orphans the `vxnotify` process [2728787]

If you terminate imfd daemon using the `kill -9` command, the `vxnotify` process created by imfd does not exit automatically but gets orphaned. However, if you stop `imfd` daemon with the `amfconfig -D` command, the corresponding `vxnotify` process is terminated.

Workaround: The correct way to stop any daemon is to gracefully stop it with the appropriate command (which is `amfconfig -D` command in this case), or to terminate the daemon using Session-ID. Session-ID is the -PID (negative PID) of the daemon.

For example:

```
# kill -9 -27824
```

Stopping the daemon gracefully stops all the child processes spawned by the daemon. However, using `kill -9` *`pid`* to terminate a daemon is not a recommended option to stop a daemon, and subsequently you must kill other child processes of the daemon manually.

Agent cannot become IMF-aware with agent directory and agent file configured [2858160]

Agent cannot become IMF-aware if Agent Directory and Agent File are configured for that agent.

Workaround: No workaround.

ProPCV fails to prevent a script from running if it is run with relative path [3617014]

If the absolute path is registered with AMF for prevention and the script is run with the relative path, AMF fails to prevent the script from running.

Workaround: No workaround.

Issues related to global clusters

This section describes the known issues about global clusters.

The engine log file receives too many log messages on the secure site in global cluster environments [1919933]

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 the Cluster Manager (Java Console)

This section describes the known issues about Symantec Cluster Server Manager (Java Console).

Cluster Manager (Java Console) may display an error while loading templates (1433844)

You can access the Template View in the Cluster Manager from the Tools > Templates menu. If you have Storage Foundation configured in a VCS cluster setup, the following error may occur while the Cluster Manager loads the templates.

```
VCS ERROR V-16-10-65 Could not load :-
/etc/VRTSvcs/Templates/DB2udbGroup.tf
```

Workaround: Ignore the error.

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

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

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

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

VCS Cluster Configuration wizard issues

VCS Cluster Configuration wizard does not automatically close in Mozilla Firefox [3281450]

You can use the `haappwizard` utility to launch the Symantec High Availability wizard to configure application monitoring with Symantec Cluster Server (VCS) on Linux systems. If you configure the utility to launch the wizard in Mozilla Firefox browser, the browser session does not automatically close after the VCS configuration is complete.

Workaround: Use one of the following workarounds:

- Close the Mozilla Firefox browser session once the wizard-based configuration steps are complete.
- Specify a different browser while configuring the `haappwizard` utility.

Configuration inputs page of VCS Cluster Configuration wizard shows multiple cluster systems for the same virtual machine [3237023]

The **Configuration inputs** panel of the VCS Cluster Configuration wizard shows multiple cluster systems for the same virtual machine. This occurs because the value specified for the node in the SystemList attribute is different than the one returned by the `hostname` command.

Workaround: Ensure that the value specified for the node in the SystemList attribute and the one returned by the `hostname` command is the same.

VCS Cluster Configuration wizard fails to display mount points on native LVM if volume groups are exported [3341937]

On storage selection page of application wizard, mount points mounted on native LVM devices are not shown. If you have one or more native LVM volume groups, and one of them is exported, the application wizard fails to detect mount points configured on these devices.

Workaround: Ensure that you do not have any native volumes exported if you want to configure application that uses native LVM storage.

IPv6 verification fails while configuring generic application using VCS Cluster Configuration wizard [3614680]

The VCS Cluster Configuration wizard fails to check whether IPv6 IP is already plumbed while configuring a generic application through the Virtual IP page. The wizard does neither displays a warning if IPv6 IP is already plumbed elsewhere nor indicates whether it is reachable through a ping.

Workaround: Manually ensure that IPv6 is not plumbed elsewhere on the network before configuring the generic application through the wizard.

Symantec Dynamic Multi-Pathing known issues

This section describes the known issues in this release of Symantec Dynamic Multi-pathing (DMP).

VxDMP console installation fails if installed in a folder having Japanese character in it (2670506)

When you install VxDMP on a host with a Japanese OS, if you select for installation a directory having a Japanese character in its name, the installation fails.

Workaround:

When installing VxDMP on a host with a Japanese OS, use the default installation directory:`C:\program files(x86)\symantec\DMP\`

I/O statistics are not available if overlapping filters are applied in the VxDMP tab of the vSphere Web Client (3306319)

The `Manage > VxDMP` tab of the vSphere Web Client does not support mixing filters for I/O statistics. In the Connctivity Map, the I/O statistics pie chart does not display if you specify an unsupported filter combination, such as specifying both a controller name and a DMP node name.

The VxDMP tab supports the following filters for I/O statistics:

- [vm=*virtual-machine-name*] ctlr=*ctlr-name*
- [vm=*virtual-machine-name*] dmpnodename=*dmp-device-name*
- [vm=*virtual-machine-name*] enclosure=*enclr-name* [portid=*array-portid*] [ctlr=*ctlr-name*]
- [vm=*virtual-machine-name*] pathname=*path-name*
- [vm=*virtual-machine-name*] pwwn=*array-port-wwn* [ctlr=*ctlr-name*]

Workaround:

There is no workaround.

Drop-down list for filter on LUNs tab in the Web client fails to load (3189918)

When you click on the drop-down list for filter on the LUNs tab in the Web client, the drop-down list fails to load.

Configuration of the VxDMP Console server and registering the DMP plugin fails if the installation directory contains special characters (2671487)

If you install DMP Console in a directory that has a name with unsupported special characters, then the post-installation configuration fails. The special characters that are not supported include the following: percent sign (%); ampersand (&); tilde (~); apostrophe ('); exclamation point (!); at sign (@); number sign (#); dollar sign ($); carat (^); plus sign (+); equal sign (=}; brackets ([ ]) and semicolon (;).

If the directory contains unsupported characters, you cannot configure Symantec DMP Console server, or register the DMP plug-in.

If you try to uninstall VxDMP from the system, then a fatal error occurs.

Workaround:

The installation directory name must not have special characters other than dash (-); underscore (_); parenthesis (()); or period (.).

Issues related to installation (2642164)

Repair of the DMP console installation fails if the *InstallDirectory*/DMP/bin directory is missing, or if files are missing from this directory.

Workaround:

If the repair fails, you must uninstall and reinstall the package.

On ESXi 5.0, DMP may fail to fetch any data (2733610)

Small Footprint CIM Broker (SFCB) on ESXi 5.0 is incompatible with JRE 1.6 u29 or later. As a result, the VxDMP tab in the vSphere Client UI fails to fetch any data. The remote CLI displays the Operation execution failed message as shown in the following example:

```
C:\Program Files (x86)\Symantec\DMP\bin> vxdmpadm vcenter=10.209.62.226
vc_user=zen\administrator vc_passwd=Merlin@123 host=10.217.56.157 gettune
VxVM vxdmpcmd ERROR V-5-1-18620 Operation execution failed.
```

To avoid this issue, upgrade to ESXi 5.0 Update 1 or higher.

On ESXi 5.0, run the following on every reboot of ESX server:

```
# /etc/init.d/sfcbd-watchdog restart
```

Additionally, perform the following workaround after installing DMP:

Workaround for vSphere Client UI:

1. Add **sblim.wbem.httpPoolSize=0** in `cimclinet.properties` file, which is located on the Console server:

   ```
   %AllUsersProfile%\Symantec\DMP\Conf\
   ```

2. Restart the VxDMP console service.

Workaround for CLI:

1. Create a new file and name it as **sblim-cim-client2.properties**.
2. In the file, add **sblim.wbem.httpPoolSize=0**, and copy the file to the following location:

   ```
   VxDMP Console install directory\DMP\bin\
   ```

Workaround for Web Client: There is no workaround for vSphere Web Client.

Downloading the ESXi bundle for an ESXi server requires that the Internet Explorer Enhanced Security is off (2843571)

To be able to download the ESXi offline bundle from the home view, make sure that for the logged in user, the Internet Explorer Enhanced Security setting is set to "Off".

VxDMP fails to detect the virtual machines with special characters (3249544)

In the Web Client, VxDMP fails to detect the virtual machines that contain special characters in their names. The special characters that are not supported include the following: bracket ([); slash (\); carat (^); dollar sign ($); period (.); pipe (|); question mark (?); asterisk (*); plus sign (+); parenthesis (()); and braces ({ }).

Workaround: Rename the virtual machine, such that it does not contain a special character.

The Connectivity Map of the VxDMP Web Client is blank (3581542)

When you select **Manage > VxDMP** tab, the VxDMP Web Client does not display the Connectivity Map.

Workaround:

Select the refresh operation on your browser (F5) to display the Connectivity Map.

Devices for newly added claim rules do not show in the list of storage arrays (3615915)

When you add a new claim rule, the devices claimed by that rule do not show in the list of storage arrays in the VxDMP tab of the vSphere Web Client.

Workaround:

Log in again to the vSphere Web Client.

The connection lines in the Connectivity Map fail to appear as expected when you resize the Web Client view (3356063)

In the VxDMP Web Client view, with multiple tabs open if you unpin the panels to resize the view or resize the browser, then the connection lines in the Connectivity Map do not appear as expected. You may observe this issue in the Connectivity Map tab after resizing the view in a different tab.

Workaround: To fix this issue, in the **Connectivity Map** view, click **Reset**.

The VxDMP Web Client does not display LUNs with names longer than 51 characters (3306263)

The VxDMP Web Client does not display LUNs with names longer than 51 characters.

Workaround:

Rename the LUN so that the name has 51 characters or less.

Adding a device to a SmartPool displays the progress as Loading (3570852)

After you add a device to the SmartPool, the progress bar displays Loading when you view the performance data (**ESX** > **Monitor** > **Performance** > **SmartPool**).

The issue is fixed by VMware in ESX 6.0.

Workaround:

Use the `F5` key to refresh the view.

DMP shows errors if the ESXi server is disconnected (3405262)

DMP shows errors if the ESXi server is disconnected. This issue is seen with both the DMP Web Client and the DMP vSphere Client. If you click the Settings tab, DMP displays an Action script error.

There is no workaround.

The DMP CLI for remote management of an ESXi 5.0 host requires configuration (3389530)

By default, the DMP CLI is not configured for remote management of an ESXi 5.0 host. The configuration step is not required for hosts with ESXi 5.0 update 1 or later.

Workaround:

Upgrade to ESXi 5.0 update 1

OR

Use the following procedure to configure the DMP CLI.

To configure the DMP CLI for remote management of an ESXi 5.0 host

1. Stop the console service.
2. Add the following line to the file `C:\ProgramData\Symantec\DMP\conf\cimclient.properties`:

   ```
   sblim.wbem.httpPoolSize=0
   ```

3. Restart the console service.

The vxcache device assigned from SmartPool to a Virtual Machine shows with different names (3556478)

The vxcache device assigned from SmartPool to a Virtual Machine shows with different names like vxcache0_1, vxcache0_2, vxcache0_3.

The vxcache device LUN serial number is created using the virtual machine UUID. Therefore, if the virtual machine UUID changes with operations like cloning, then the LUN serial number of vxcache device also changes. This causes the vxcache device name to change.

Workaround:

This behavior does not have any functional impact.

To display the original default device name, clear the vxcache device name with the following command:

```
# vxddladm -c assign names
```

Symantec Storage Foundation Cluster File System High Availability known issues

This section describes the known issues in this release of Symantec Storage Foundation Cluster File System High Availability (SFCFSHA).

On CFS, SmartIO is caching writes although the cache appears as nocache on one node (3760253)

On CFS, SmartIO is caching writes although the `sfcache list` output shows the cache in `nocache` mode on one node. The OS `mount` command also shows the file systems as unmounted. This issue is due to a known bug that is documented in the Linux `mount` manual page. The `/etc/mtab` file and the `/proc/mounts` file, which are expected to have entries for all the mounted file systems, do not match. When the `sfcache list` command displays the list of file systems that are mounted in writeback mode, `sfcache list` refers to the `/etc/mtab` entries for the mount status of the file systems. As a result, `sfcache list` may sometimes show a writeback enabled file system as umounted while in reality the file system is still mounted. The `/proc/mounts` file correctly shows the file systems as mounted.

Workaround:

Verify that the file system is mounted through the contents of the `/proc/mounts` file.

Unmounting the checkpoint using cfsumount(1M) may fail if SElinux is in enforcing mode [3766074]

If SElinux is in enforcing mode, then cfsumount might fail to unmount the checkpoint. cfsumount returns the following error:

```
# cfsumount /mnt1_clone1
  Unmounting...
  WARNING: Unmount of /mnt1_clone1 initiated on [  ]
  WARNING: Could not determine the result of the unmount operation
```

SElinux prevents mounting vxfs from writing access on the mount point for checkpoint. Because of this, cfsmount cannot set mount lock for the mount point for checkpoint.

Workaround:

1. Remove mntlock=VCS from /etc/mtab and retry the cfsumount.
2. To prevent future cfsumount failure follow the below steps:

   ```
   # grep mount.vxfs /var/log/audit/audit.log | audit2allow -M mypol

   # semodule -i mypol.pp
   ```

tail -f run on a cluster file system file only works correctly on the local node [3741020]

When you use the `tail -f` command(1M) to monitor a file on a cluster file system, changes to the file made on remote nodes are not detected. This is due to the tail command now utilizing inotify. Symantec is currently unable to support inotify with a cluster file system due to GPL restrictions.

Workaround: To revert to the old behavior, you can specify the ---disable-inotify option with the tail command.

In SFCFS on Linux, stack may overflow when the system creates ODM file [3758102]

In Symantec Cluster File System (SFCFS), when the system creates an ODM file, the cluster inode needs initialization, which takes Group Lock Manager (GLM) locked.

During the locked period, processing within GLM module may lead to stack overflow on Linux when the system is allocating memory.

Workaround: There is no workaround.

CFS commands might hang when run by non-root (3038283)

The CFS commands might hang when run by non-root.

Workaround

To resolve this issue

◆ Use `halogin` command to save the authentication information before running any CFS commands on a non-root session.

  When you run the `halogin` command, VCS stores encrypted authentication information in the user’s home directory.

The fsappadm subfilemove command moves all extents of a file (3258678)

This issue occurs under following conditions:

- You run the `fsppadm subfilemove` command from a cluster file system (CFS) secondary node.
- You specify a range of extents for relocation to a target tier.

If the extent size is greater than or equal to 32768, the `fsppadm subfilemove` command moves all extents of the specified table to the target tier. The expectation is to move a specified range of extents.

Workaround:

◆ On the CFS primary node, determine the primary node using one of the following commands:

```
# fsclustadm showprimary mountpoint
```

```
# fsclustadm idtoname nodeid
```

Certain I/O errors during clone deletion may lead to system panic. (3331273)

Certain I/O errors during clone deletion may lead to system panic.

Workaround:

There is no workaround for this issue.

Panic due to null pointer de-reference in vx_bmap_lookup() (3038285)

If you use the `fsadm -b` command on a CFS secondary node to resize the file system, it might fail with the following error message printed in the syslog:

```
Reorg of inode with shared extent larger than 32768 blocks
can be done only on the CFS Primary node
```

Workaround: Resize the file system with the `fsadm` command from the primary node of the cluster.

Symantec Storage Foundation for Oracle RAC known issues

This section describes the known issues in this release of Symantec Storage Foundation for Oracle RAC.

Oracle RAC known issues

This section lists the known issues in Oracle RAC.

During installation or system startup, Oracle Grid Infrastructure may fail to start

After successful installation of Oracle RAC 11g Release 2 Grid Infrastructure, while executing the `root.sh` script, `ohasd` may fail to start. Similarly, during system startup, Oracle Grid Infrastructure may fail to start though the VCS engine logs may indicate that the cssd resource started Oracle Grid Infrastructure successfully.

The following message may be displayed on running the `strace` command:

```
# /usr/bin/strace -ftt -p pid_of_ohasd.bin
14:05:33.527288 open("/var/tmp/.oracle/npohasd",
O_WRONLY <unfinished ...>
```

For possible causes and workarounds, see the Oracle Metalink document: 1069182.1

Oracle Grid Infrastructure installation may fail with internal driver error

The Oracle Grid Infrastructure installation may fail with the following error:

```
[INS-20702] Unexpected Internal driver error
```

Workaround:

Perform one of the following steps depending on the type of installer you use for the installation:

- Script-based installer
  Export the `OUI_ARGS` environment variable, before you run the SF Oracle RAC installation program:

  ```
  export OUI_ARGS=-ignoreInternalDriverError
  ```

  For more information, see the Oracle Metalink document: 970166.1
- Web-based installer
  When you run the Web-based installer, in the **Enter the arguments to be passed to the Oracle installer** text box, enter the value `-ignoreInternalDriverError`.
  For more information, see the *Symantec Storage Foundation for Oracle RAC Installation and Configuration Guide*.

SF Oracle RAC issues

This section lists the known issues in SF Oracle RAC for this release.

ASM disk groups configured with normal or high redundancy are dismounted if the CVM master panics due to network failure in FSS environment or if CVM I/O shipping is enabled (3600155)

Disk-level remote write operations are paused during reconfiguration for longer than the default ASM heartbeat I/O wait time in the following scenarios:

- CVM master node panics
- Private network failure

As a result, the ASM disk groups get dismounted.

Workaround: See to the Oracle metalink document: 1581684.1

PrivNIC and MultiPrivNIC agents not supported with Oracle RAC 11.2.0.2 and later versions

The PrivNIC and MultiPrivNIC agents are not supported with Oracle RAC 11.2.0.2 and later versions.

For more information, see the following Technote:

http://www.symantec.com/business/support/index?page=content&id=TECH145261

CSSD agent forcibly stops Oracle Clusterware if Oracle Clusterware fails to respond (3352269)

On nodes with heavy load, the CSSD agent attempts to check the status of Oracle Clusterware till it reaches the`FaultOnMonitorTimeouts` value. However, Oracle Clusterware fails to respond and the CSSD agent forcibly stops Oracle Clusterware. To prevent the CSSD agent from forcibly stopping Oracle Clusterware, set the value of the `FaultOnMonitorTimeouts` attribute to 0 and use the `AlertOnMonitorTimeouts` attribute as described in the following procedure.

Perform the following steps to prevent the CSSD agent from forcibly stopping Oracle Clusterware:

1. Change the permission on the VCS configuration file to read-write mode:

   ```
   # haconf -makerw
   ```

2. Set the `AlertOnMonitorTimeouts` attribute value to 4 for the CSSD resource:

   ```
   # hatype -display CSSD | grep AlertOnMonitorTimeouts
   CSSD  AlertOnMonitorTimeouts 0
   # hares -override cssd_resname AlertOnMonitorTimeouts
   # hatype -modify CSSD AlertOnMonitorTimeouts 4
   ```

3. Set the `FaultOnMonitorTimeouts` attribute value to 0 for the CSSD resource:

   ```
   # hatype -display CSSD | grep FaultOnMonitorTimeouts
   CSSD  FaultOnMonitorTimeouts 4
   # hares -override cssd_resname FaultOnMonitorTimeouts
   # hatype -modify CSSD FaultOnMonitorTimeouts 0
   ```

4 Verify the `AlertOnMonitorTimeouts` and `FaultOnMonitorTimeouts` settings:

```
# hatype -display CSSD | egrep \
"AlertOnMonitorTimeouts|FaultOnMonitorTimeouts"
CSSD  AlertOnMonitorTimeouts 4
CSSD  FaultOnMonitorTimeouts 0
```

5 Change the permission on the VCS configuration file to read-only mode:

```
# haconf -dump -makero
```

Intelligent Monitoring Framework (IMF) entry point may fail when IMF detects resource state transition from online to offline for CSSD resource type (3287719)

When IMF detects a state transition from ONLINE to OFFLINE state for a registered online resource, it sends a notification to the CSSD agent. The CSSD agent schedules a monitor to confirm the state transition of the resource. The resources of type CSSD takes more time to go online or offline fully. Therefore, if this immediate monitor finds the resource still in online state, it assumes that the IMF notification is false and attempts to register the resource in online state again.

In such partial state transitions, the agent repeatedly attempts to register the resource until the`RegisterRetryLimit` is reached (default value is 3) or the resource registration is successful. After the resource is completely offline, the next resource registration with IMF will be successful.

Workaround: Increase the value of the `RegisterRetryLimit` attribute if multiple registration attempts fail.

Node fails to join the SF Oracle RAC cluster if the file system containing Oracle Clusterware is not mounted (2611055)

The sequence number of the startup script for Oracle High Availability Services daemon (ohasd) is lower than some of the SF Oracle RAC components such as VXFEN and VCS. During system startup, if the file system containing Oracle Clusterware does not get mounted before the ohasd startup script is executed, the script continuously waits for the file system to become available. As a result, the other scripts (including those of SF Oracle RAC components) are not executed and the node being started does not join the SF Oracle RAC cluster.

Workaround: If the rebooted node does not join the SF Oracle RAC cluster, the cluster can be started manually using the following command:

```
# installsfrac -start node1 node2
```

The vxconfigd daemon fails to start after machine reboot (3566713)

The `shutdown -r` command makes sure that the file contents on the OS file system are written properly to the disk before a reboot. The `volboot` file is created in the OS file system, and is used to bring up the `vxconfigd` daemon after the system reboot. If the machine reboots for any reason without proper shutdown, and the `volboot` file contents are not flushed to the disk, `vxconfigd` will not start after the system reboots.

Workaround:

You must rerun the `vxinstall` script to re-create the `volboot` file and to start the `vxconfigd` daemon and other daemons.

Health check monitoring fails with policy-managed databases (3609349)

The health check option of the Symantec Cluster Server agent for Oracle fails to determine the status of the Oracle resource in policy-managed database environments. This is because the database SID is dynamically created during the time of the health check as a result of which the correct SID is not available to retrieve the resource status.

Issue with format of the last 8-bit number in private IP addresses (1164506)

The PrivNIC/MultiPrivNIC resources fault if the private IP addresses have a leading 0 in any of the octets that comprise the IP address, for example X.X.X.01 or X.X.0X.1. or X.0X.X.1 or 0X.X.X.1, where X is an octet of the IP address.

When you configure private IP addresses for Oracle Clusterware, ensure that the IP addresses have a format as displayed in the following two-node example:

- On galaxy: 192.168.12.1
- On nebula: 192.168.12.2

Confirm the correct format by viewing the PrivNIC or MultiPrivNIC resource in the `/etc/VRTSvcs/conf/config/main.cf` file.

CVMVolDg agent may fail to deport CVM disk group

The CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported.

Workaround: If multiple CVMVolDg resources are configured for a shared disk group, set the value of the `CVMDeportOnOffline` attribute to 1 for all of the resources.

Rolling upgrade not supported for upgrades from SF Oracle RAC 5.1 SP1 with fencing configured in `dmp`mode.

Rolling upgrade is not supported if you are upgrading from SF Oracle RAC 5.1 SP1 with fencing configured in `dmp`mode. This is because fencing fails to start after the system reboots during an operating system upgrade prior to upgrading SF Oracle RAC.

The following message is displayed:

```
VxVM V-0-0-0 Received message has a different protocol version
```

Workaround: Perform a full upgrade if you are upgrading from SF Oracle RAC 5.1 SP1 with fencing configured in `dmp`mode.

"Configuration must be ReadWrite : Use haconf -makerw" error message appears in VCS engine log when hastop -local is invoked (2609137)

A message similar to the following example appears in the `/var/VRTSvcs/log/engine_A.log`log file when you run the `hastop -local`command on any system in a SF Oracle RAC cluster that has `CFSMount`resources:

```
2011/11/15 19:09:57 VCS ERROR V-16-1-11335 Configuration must be
ReadWrite : Use haconf -makerw
```

The `hastop -local` command successfully runs and you can ignore the error message.

Workaround: There is no workaround for this issue.

Veritas Volume Manager can not identify Oracle Automatic Storage Management (ASM) disks (2771637)

Veritas Volume Manager (VxVM) commands can not identify disks that are initialized by ASM. Administrators must use caution when using the VxVM commands to avoid accidental overwriting of the ASM disk data.

vxdisk resize from slave nodes fails with "Command is not supported for command shipping" error (3140314)

When running the `vxdisk resize` command from a slave node for a local disk, the command may fail with the following error message:

```
VxVM vxdisk ERROR V-5-1-15861 Command is not supported for command
shipping.
Operation must be executed on master
```

Workaround: Switch the master to the node to which the disk is locally connected and run the `vxdisk resize` on that node.

vxconfigbackup fails on Flexible Storage Sharing disk groups (3079819)

The `vxconfigbackup` command fails on disk groups with remote disks that have the Flexible Storage Sharing attribute set with the following error messages:

```
VxVM vxconfigbackup ERROR V-5-2-3719 Unable to get the disk serial number.
VxVM vxconfigbackup ERROR V-5-2-6144 configbackup cannot proceed without
uuid.
    FAILED:EXEC /usr/lib/vxvm/bin/vxconfigbackup
```

Workaround: There is no workaround for this issue.

CVR configurations are not supported for Flexible Storage Sharing (3155726)

Cluster Volume Replicator (CVR) configurations are not supported in a Flexible Storage Sharing environment.

CVM requires the T10 vendor provided ID to be unique (3191807)

For CVM to work, each physical disk should generate a unique identifier (UDID). The generation is based on the T10 vendor provided ID on SCSI-3 vendor product descriptor (VPD) page 0x83. In some cases, the T10 vendor provided ID on SCSI-3 VPD page 0x83 is the same for multiple devices, which violates the SCSI standards. CVM configurations should avoid using such disks.

You can identify the T10 vendor provided ID using the following command:

```
# sq_inq --page=0x83 /dev/diskname
```

On VxVM you can identify the T10 vendor provided ID using the following command:

```
# /etc/vx/diag.d/vxscsiinq -e 1 -p 0x83 /dev/vx/rdmp/diskname
```

You can verify the VxVM generated UDID on the disk using the following command:

```
# vxdisk list diskname | grep udid
```

Default volume layout with DAS disks spans across different disks for data plexes and DCO plexes (3087867)

The default volume layout for Flexible Storage Sharing disk groups is a two-way mirrored volume with a DCO log. The DCO log plexes may be allocated using host class instances that may be different from the ones used for the data plexes.

Workaround: Use the command line `alloc` attributes to explicitly set allocation requirements. For example, you can specify `alloc=host:host1,host:host2` during volume creation on an FSS disk group, and allocate DCO plexes on the same host (failure domain) as the data plexes.

SG_IO ioctl hang causes disk group creation, CVM node joins, and storage connects/disconnects, and vxconfigd to hang in the kernel (3193119)

In RHEL 5.x, the `SG_IO ioctl` process hangs in the kernel. This causes disk group creation and CVM node joins to hang. The `vxconfigd` thread hangs in the kernel during storage connects/disconnects and is unresponsive.

Workaround: This issue is fixed in RHEL 6.3. Upgrade to RHEL 6.3.

Preserving Flexible Storage Sharing attributes with vxassist grow and vxresize commands is not supported (3225318)

Preservation of FSS attributes using `vxasssist grow` and `vxresize` is not supported. FSS attributes include the attributes that are specified on the command line as well as the attributes implicitly assumed for FSS disk groups. These attributes are not reused with further `vxassist` orpations on the volume such as the `growby` and the `vxresize` commands.

Workaround:

There is no workaround for this issue.

vxdg adddisk operation fails when adding nodes containing disks with the same name (3301085)

On a slave node, when using the `vxdg adddisk` command to add a disk to a disk group, and if the device name already exists in the disk group as disk name (disk media name), the operation fails with the following message:

```
VxVM vxdg ERROR V-5-1-599 Disk disk_1: Name is already used.
```

Workaround: Explicitly specify the disk media name, which is different from the existing disk media name in the disk group, when running the `vxdg adddisk` command on the slave node.

For example:

```
# vxdg -g diskgroup adddisk dm1=diskname1 dm2=diskname2 dm3=diskname3
```

In a Flexible Storage Sharing disk group, the default volume layout is not mirror when creating a volume with the mediatype:ssd attribute (3209064)

As per current VxVM behavior, specifying a subset of disks, such as mediatype:ssd, as a command line argument during volume creation, takes precedence over internal FSS attributes. VxVM does not implicitly apply by default the mirrored volume layout for a FSS volume.

Workaround: Explicitly specify the `layout=mirror` attribute during volume creation.

```
# vxassist -g diskgroup make volume size mediatype:ssd layout=mirror
```

FSS Disk group creation with 510 exported disks from master fails with Transaction locks timed out error (3311250)

Flexible Storage Sharing (FSS) Disk group creation for local disks that are exported may fail if the number of disks used for disk group creation is greater than 150, with the following error message:

```
VxVM vxdg ERROR V-5-1-585 Disk group test_dg: cannot create: Transaction
    locks timed out
```

A similar error can be seen while adding more that 150 locally exported disks (with `vxdg adddisk`) to the FSS disk group, with the following error message:

```
VxVM vxdg ERROR V-5-1-10127 associating disk-media emc0_0839 with emc0_0839:
        Transaction locks timed out
```

Workaround:

Create an FSS disk group using 150 or less locally exported disks and then do an incremental disk addition to the disk group with 150 or less locally exported disks at a time.

vxconfigrestore is unable to restore FSS cache objects in the pre-commit stage (3461928)

While restoring a Flexible Storage Sharing (FSS) disk group configuration that has cache objects configured, the following error messages may display during the pre-commit phase of the restoration:

```
VxVM vxcache ERROR V-5-1-10128  Cache object meta-data update error
VxVM vxcache ERROR V-5-1-10128  Cache object meta-data update error
VxVM vxvol WARNING V-5-1-10364 Could not start cache object
VxVM vxvol ERROR V-5-1-11802 Volume volume_name cannot be started
VxVM vxvol ERROR V-5-1-13386 Cache object on which Volume volume_name
 is constructed is not enabled
VxVM vxvol ERROR V-5-1-13386 Cache object on which Volume volume_name
 is constructed is not enabled
```

The error messages are harmless and do not have any impact on restoration. After committing the disk group configuration, the cache object and the volume that is constructed on the cache object are enabled.

Change in naming scheme is not reflected on nodes in an FSS environment (3589272)

In a Flexible Storage Sharing (FSS) environment, if you change the naming scheme on a node that has local disks, the remote disk names are not reflected with the corresponding name change. If you change the naming scheme on a node where exported disks are present, to reflect the updated remote disk names, you must either export the disks again or restart the node where the remote disks are present

Workaround:

There is no workaround for this issue.

vxassist does not create data change logs on all mirrored disks, if an FSS volume is created using DM lists (3559362)

When a Flexible Storage Sharing (FSS) volume is created using DM lists, the `vxassist` command does not create data change logs on all the mirrored disks; the number of DCO mirrors is not equal to the number of data mirrors. The `vxassist` command creates a two-way DCO volume.

Workaround:

Manually add a DCO mirror using the `vxassist -g` *`diskgroup`* `mirror` *`dco_volume`* command.

Intel SSD cannot be initialized and exported (3584762)

Initializing an Intel SSD with the Flexible Storage Sharing (FSS) export option may fail with the following error message:

```
VxVM vxedpart ERROR V-5-1-10089 partition modification failed: Device
or resource busy
```

Workaround:

Initialize the private region of the SSD disk to 0 and retry the disk initialization operation.

For example:

```
# dd if=/dev/zero of=/dev/vx/dmp/intel_ssd0_0 bs=4096 count=1
```

```
# vxdisksetup -i intel_ssd0_0 export
```

VxVM may report false serial split brain under certain FSS scenarios (3565845)

In a Flexible Storage Sharing (FSS) cluster, as part of a restart of the master node, internal storage may become disabled before network service. Any VxVM objects on the master node's internal storage may receive I/O errors and trigger an internal transaction. As part of this internal transaction, VxVM increments serial split brain (SSB) ids for remaining attached disks, to detect any SSB. If you then disable the network service, the master leaves the cluster and this results in a master takeover. In such a scenario, the master takeover (disk group re-import) may fail with a false split brain error and the `vxsplitlines` output displays 0 or 1 pools.

For example:

```
Syslog: "vxvm:vxconfigd: V-5-1-9576 Split Brain. da id is 0.2,
while dm id is 0.3 for dm disk5mirr
```

Workaround:

To recover from this situation

1 Retrieve the disk media identifier (dm_id) from the configuration copy:

```
# /etc/vx/diag.d/vxprivutil dumpconfig device-path
```

The dm_id is also the serial split brain id (ssbid)

2 Use the dm_id in the following command to recover from the situation:

```
# /etc/vx/diag.d/vxprivutil set device-path ssbid=dm_id
```

Symantec Storage Foundation for Databases (SFDB) tools known issues

This section describes the known issues in this release of Symantec Storage Foundation for Databases (SFDB) tools.

Upgrading Symantec Storage Foundation for Databases (SFDB) tools from 5.0.x to 6.2.1 (2184482)

The `sfua_rept_migrate`command results in an error message after upgrading SFHA or SF for Oracle RAC version 5.0 to SFHA or SF for Oracle RAC 6.2.1.

When upgrading from SF, SFCFSHA, SFHA or SFRAC version 5.0 to SF, SFCFSHA, SFHA or SFRAC 6.2.1, the S*vxdbms3 startup script is renamed to NO_S*vxdbms3. The S*vxdbms3 startup script is required by `sfua_rept_upgrade`. Thus when `sfua_rept_upgrade` is run, it is unable to find the S*vxdbms3 startup script and gives the error message:

```
/sbin/rc3.d/S*vxdbms3 not found
SFORA sfua_rept_migrate ERROR V-81-3558 File:  is missing.
SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.
```

Workaround: Before running `sfua_rept_migrate`, rename the startup script NO_S*vxdbms3 to S*vxdbms3.

Sometimes SFDB may report the following error message: SFDB remote or privileged command error (2869262)

While using SFDB tools, if you attempt to run commands, such as `dbed_update` then you may observe the following error:

```
$ /opt/VRTSdbed/bin/dbed_update
No repository found for database faildb, creating new one.
SFDB vxsfadm ERROR V-81-0450 A remote or privileged command could not
be executed on swpa04

Reason: This can be caused by the host being unreachable or the vxdbd
daemon not running on that host.

Action: Verify that the host swpa04 is reachable. If it is, verify
that the vxdbd daemon is running using the /opt/VRTS/bin/vxdbdctrl
status command, and start it using the /opt/VRTS/bin/vxdbdctrl start
command if it is not running.
```

Workaround: There is no workaround for this issue.

SFDB commands do not work in IPV6 environment (2619958)

In IPV6 environment, SFDB commands do not work for SF, SFCFSHA, SFHA or SFRAC.

Workaround:

There is no workaround at this point of time.

The dbdst_obj_move(1M) command moves all the extents of a database table (3277003)

The `dbdst_obj_move(1M)` command moves all the extents of a database table when:

- The `dbdst_obj_move(1M)` command is run from the CFS secondary node.
- The object is an Oracle database table (-t option)
- A range of extents is specified for movement to a target tier (-s and -e options). The `dbdst_obj_move(1M)` command moves all extents of the specified table to a target tier when the extent size is greater than or equal to 32768. However, the expectation is to move only a specified range of extents.

Workaround: Run the `dbdst_obj_move(1M)` command from the CFS primary node.

Use the `fsclustadm showprimary` *<mountpoint>* and `fsclustadm idtoname` *<nodeid>*commands to determine the mode of a CFS node.

When you attempt to move all the extents of a table, the `dbdst_obj_move`(1M) command fails with an error (3260289)

When you attempt to move all the extents of a database table, which is spread across multiple mount-points in a single operation, the `dbdst_obj_move(1M)` command fails. The following error is reported:

```
bash-2.05b$ dbdst_obj_move -S sdb -H $ORACLE_HOME -t test3 -c MEDIUM
FSPPADM err : UX:vxfs fsppadm: WARNING: V-3-26543: File handling failure
on /snap_datadb/test03.dbf with message -
SFORA dst_obj_adm ERROR V-81-6414 Internal Error at fsppadm_err
```

Note: To determine if the table is spread across multiple mount-points, run the dbdst_obj_view(1M) command

Workaround: In the `dbdst_obj_move(1M)` command, specify the range of extents that belong to a common mount-point. Additionally, if your table is spread across "n" mount-points, then you need to run the `dbdst_obj_move(1M)` command "n" times with a different range of extents.

The ReverseResyncBegin (RRBegin) operation with recovery option as AUTO fails (3076583)

The RRBegin operation with the recovery option as AUTO fails when you perform the following sequence of operations:

1. Validate the FlashSnap setup using the validate operation.
2. In the database, take the tablespace offline.
3. Perform a snapshot operation.
4. Bring the tablespace online which was taken offline in 2.
5. Perform the Reverse Resync Begin operation.

Note: This issue is encountered only with Oracle version 10gR2.

Workaround: Perform one of the following:

- Make sure to bring the tablespace online only after performing the RRBegin and RRCommit operations. Otherwise, perform the Reverse Resync Begin operation while the tablespace is in the offline mode.
- To recover a database, specify the recovery option as **AUTO_UNTIL_SCN** in the RRBegin operation.

The ReverseResyncBegin (RRBegin) operation fails when performed on multiple snapshot configurations (3066532)

When you perform a Reverse Resync operation on multiple snapshot configurations, SFDB reports the following error message:

```
$ vxsfadm -a oracle -s flashsnap --name \
man -o rrbegin
```

```
SFDB vxsfadm ERROR V-81-0943 Repository already relocated to alternate
location.
```

As per the Reverse Resync design, the first RRBegin operation relocates the SFDB repository to a backup location, and the ReverseResyncAbort and ReverseResyncCommit operations restore it to the original location. When the second RRBegin operation attempts to relocate the same repository which is already relocated, SFDB reports the error message.

Workaround: Make sure to perform the RRAbort or RRCommit operation using the snapshot configuration that is in the RRBegin state.

Note: You must complete Reverse Resync operations for a particular configuration before you start with another configuration.

The ReverseResyncBegin (RRBegin) operation fails and reports an error message due to a missing binary control file (3157314)

When the RRBegin operation cannot find the binary control file that is used to recover a database instance, it reports the following error message:

```
[oracle@testbox ~]$ vxsfadm -a oracle -s flashsnap -name man -o rrbegin
```

```
SFDB vxsfadm ERROR V-81-0949 Binary Control file is not available for
recovery purposes
```

This issue is observed in the third-mirror break-off type (FlashSnap) snapshots that are created using the older SFDB version, which did not include the binary control file in the snapshot images.

Workaround: There is no workaround for this issue.

Attempt to use SmartTier commands fails (2332973)

The attempts to run SmartTier commands such as `dbdst_preset_policy` or`dbdst_file_move` fail with the following error:

```
fsppadm: ERROR: V-3-26551: VxFS failure on low level mechanism
with message - Device or resource busy
```

This error occurs if a sub-file SmartTier command such as `dbdst_obj_move` has been previously run on the file system.

Workaround: There is no workaround for this issue. You cannot use file-based SmartTier and sub-file SmartTier simultaneously.

Attempt to use certain names for tiers results in error (2581390)

If you attempt to use certain names for tiers, the following error message is displayed:

```
SFORA dbdst_classify ERROR V-81-6107 Invalid Classname BALANCE
```

This error occurs because the following names are reserved and are not permitted as tier names for SmartTier:

- BALANCE
- CHECKPOINT
- METADATA

Workaround: Use a name for SmartTier classes that is not a reserved name.

Clone operation failure might leave clone database in unexpected state (2512664)

If the clone operation fails, it may leave the clone database in an unexpected state. Retrying the clone operation might not work.

Workaround:

If retrying does not work, perform one the following actions depending on the point-in-time copy method you are using:

- For FlashSnap, resync the snapshot and try the clone operation again.
- For FileSnap and Database Storage Checkpoint, destroy the clone and create the clone again.

- For space-optimized snapshots, destroy the snapshot and create a new snapshot.

Contact Symantec support if retrying using the workaround does not succeed.

Clone command fails if PFILE entries have their values spread across multiple lines (2844247)

If you have a parameter, such as `log_archive_dest_1`, in single line in the `init.ora` file, then `dbed_vmclonedb` works but `dbed_vmcloneb` fails if you put in multiple lines for parameter.

Workaround: Edit the PFILE to arrange the text so that the parameter values are on a single line. If the database uses a spfile and some parameter values are spread across multiple lines, then use the Oracle commands to edit the parameter values such as they fit in a single line.

Clone command errors in a Data Guard environment using the MEMORY_TARGET feature for Oracle 11g (1824713)

The `dbed_vmclonedb` command displays errors when attempting to take a clone on a STANDBY database in a dataguard environment when you are using the MEMORY_TARGET feature for Oracle 11g.

When you attempt to take a clone of a STANDBY database, the `dbed_vmclonedb` displays the following error messages:

```
Retrieving snapshot information ...                          Done
Importing snapshot diskgroups ...                            Done
Mounting snapshot volumes ...                                Done
Preparing parameter file for clone database ...              Done
Mounting clone database ...
ORA-00845: MEMORY_TARGET not supported on this system


SFDB vxsfadm ERROR V-81-0612 Script
/opt/VRTSdbed/applications/oracle/flashsnap/pre_preclone.pl failed.
```

This is Oracle 11g-specific issue known regarding the MEMORY_TARGET feature, and the issue has existed since the Oracle 11gr1 release. The MEMORY_TARGET feature requires the `/dev/shm` file system to be mounted and to have at least 1,660,944,384 bytes of available space. The issue occurs if the `/dev/shm`file system is not mounted or if the file system is mounted but has available space that is less than the required minimum size.

Workaround: To avoid the issue, remount the `/dev/shm` file system with sufficient available space.

To remount the /dev/shm file system with sufficient available space

1. Shut down the database.
2. Unmount the `/dev/shm` file system:

   ```
   # umount /dev/shm
   ```

3. Mount the `/dev/shm` file system with the following options:

   ```
   # mount -t tmpfs shmfs -o size=4096m /dev/shm
   ```

4. Start the database.

Clone fails with error "ORA-01513: invalid current time returned by operating system" with Oracle 11.2.0.3 (2804452)

While creating a clone database using any of the point-in-time copy services such as Flashsnap, SOS, Storage Checkpoint, or Filesnap, the clone fails. This problem appears to affect Oracle versions 11.2.0.2 as well as 11.2.0.3.

You might encounter an Oracle error such as the following:

```
/opt/VRTSdbed/bin/vxsfadm -s flashsnap -o clone
-a oracle -r dblxx64-16-v1 --flashsnap_name TEST11 --clone_path
/tmp/testRecoverdb --clone_name clone1
USERNAME:  oragrid
STDOUT:
Retrieving snapshot information ...                            Done
Importing snapshot diskgroups ...                              Done
Mounting snapshot volumes ...                                  Done

ORA-01513: invalid current time returned by operating system
```

This is a known Oracle bug documented in the following Oracle bug IDs:

- Bug 14102418: DATABASE DOESNT START DUE TO ORA-1513
- Bug 14036835: SEEING ORA-01513 INTERMITTENTLY

Workaround: Retry the cloning operation until it succeeds.

Data population fails after datafile corruption, rollback, and restore of offline checkpoint (2869259)

Sometimes when a datafile gets corrupted below its reservation size, the rollback may not pass and the file may not be rolled back correctly.

There is no workround at this point of time.

FileSnap detail listing does not display the details of a particular snap (2846382)

FileSnap does not support displaying a detailed listing of a snapshot or clone. FileSnap only supports displaying a summary of all the snapshots or clones. For example, for the CLI `vxsfadm -s filesnap -a oracle --name=snap1 -o list`, a summary listing all the snapshots is displayed, instead of a detailed listing of a particular snapshot.

Workaround: There is no workaround for this issue.

Flashsnap clone fails under some unusual archivelog configuration on RAC (2846399)

In a RAC environment, when using FlashSnap, the archive log destination to snapshot must be a shared path, and must be the same across all the nodes. Additionally, all nodes must use the same archive log configuration parameter to specify the archive log destination. Configurations similar to the following are not supported:

```
tpcc1.log_archive_dest_1='location=/tpcc_arch'
tpcc2.log_archive_dest_2='location=/tpcc_arch'
tpcc3.log_archive_dest_3='location=/tpcc_arch'
```

Where tpcc1, tpcc2, and tpcc3 are the names of the RAC instances and /tpcc_arch is the shared archive log destination.

Workaround: To use FlashSnap, modify the above configuration to *.log_archive_dest_1='location=/tpcc_arch'. For example,

```
tpcc1.log_archive_dest_1='location=/tpcc_arch'
tpcc2.log_archive_dest_1='location=/tpcc_arch'
tpcc3.log_archive_dest_1='location=/tpcc_arch'
```

In the cloned database, the seed PDB remains in the mounted state (3599920)

In Oracle database version 12.1.0.2, when a container database (CDB) is cloned, the **PDB$SEED** pluggable database (PDB) remains in the mounted state. This behavior is observed because of the missing datafiles in the cloned database for all point-in-time copies.

When you attempt to open the cloned seed database, the following error is reported:

```
"ORA-01173" oracle error.
...
SFDB vxsfadm ERROR V-81-0564 Oracle returned error.

Reason: ORA-01122: database file 15 failed verification check
ORA-01110: data file 15: '/tmp/test1/data/sfaedb/newtbs1.dbf'
ORA-01202: wrong incarnation of this file - wrong creation time
...
```

Workaround: There is no workaround for this issue.

Cloning of a container database may fail after a reverse resync commit operation is performed (3509778)

After a reverse resync operation is performed, the cloning of a container database may fail with the following error message:

```
SFDB vxsfadm ERROR V-81-0564 Oracle returned error.

Reason: ORA-01503: CREATE CONTROLFILE failed
ORA-01189: file is from a different RESETLOGS than previous files
ORA-01110: data file 6: '/tmp/testRecoverdb/data/sfaedb/users01.dbf'
```

Workaround: There is no workaround for this issue.

If one of the PDBs is in the read-write restricted state, then cloning of a CDB fails (3516634)

Cloning a container database (CDB) for point-in-time copies fails if some of the pluggable databases (PDBs) are open in the restricted mode. The failure occurs with the following error message:

```
SFDB vxsfadm ERROR V-81-0564 Oracle returned error.

Reason: ORA-65106: Pluggable database #3 (PDB1) is in an invalid state.
```

Workaround: There is no workaround for this issue.

Cloning of a CDB fails for point-in-time copies when one of the PDBs is in the read-only mode (3513432)

For Oracle version 12.1.0.1, cloning a container database (CDB) fails if one of the pluggable databases (PDBs) is in the read-only mode. The failure occurs with the following error message:

```
SFDB vxsfadm ERROR V-81-0564 Oracle returned error.

Reason: ORA-00376: file 9 cannot be read at this time
ORA-01111: name for data file 9 is unknown - rename to correct file
ORA-01110: data file 9: '/ora_base/db_home/dbs/MISSING00009'...
```

Workaround: There is no workaround for this issue.

If a CDB has a tablespace in the read-only mode, then the cloning fails (3512370)

For Oracle version 12.1.0.1, when a container database (CDB) has a tablespace in the read-only mode for all point-in-time copies, cloning of that CDB fails with the following error message:

```
SFDB vxsfadm ERROR V-81-0564 Oracle returned error.

Reason: ORA-01122: database file 15 failed verification check
ORA-01110: data file 15: '/tmp/test1/data/sfaedb/newtbs1.dbf'
ORA-01202: wrong incarnation of this file - wrong creation time
...
```

Workaround: There is no workaround for this issue.

If any SFDB installation with authentication setup is upgraded to 6.2, the commands fail with an error (3644030)

The commands fail with the error message similar to the following:

```
SFDB vxsfadm ERROR V-81-0450 A remote or privileged command could not be
executed on prodhost

Reason: This can be caused by the host being unreachable or the vxdbd daemon
not running on that host or because of insufficient privileges.

Action: Verify that the prodhost is reachable. If it is, verify
that
the vxdbd daemon is enabled and running using the [
/opt/VRTS/bin/sfae_config
status ] command, and enable/start vxdbd using the [
/opt/VRTS/bin/sfae_config
enable ] command if it is not enabled/running. Also make sure you are
authorized to run SFAE commands if running in secure mode.
```

Workaround: Set up the authentication for SFDB again. See *Storage and Availability Management for Oracle Databases* or *Storage and Availability Management for DB2 Databases*.

Symantec Storage Foundation for Sybase ASE CE known issues

This section lists the known issues in SF Sybase CE for this release.

Sybase Agent Monitor times out (1592996)

Problem: The Sybase Agent Monitor has issues of timing out, in cases where qrmutil reports delay.

The Sybase Agent monitor times out, if qrmutil fails to report the status to the agent within the defined MonitorTimeout for the agent.

Solution: If any of the following configuration parameters for Sybase Database is increased, it will require a change in its MonitorTimeout value:

- quorum heartbeat interval (in seconds)
- Number of retries

If the above two parameters are changed, Symantec recommends that the MonitorTimeout be set to a greater value than the following: ((number of retries + 1) * (quorum heartbeat interval)) + 5.

Installer warning (1515503)

Problem: During configuration of Sybase instance under VCS control, if the quorum device is on CFS and is not mounted, the following warning message appears on the installer screen:

```
Error: CPI WARNING V-9-40-5460 The quorum file /qrmmnt/qfile
cannot be accessed now. This may be due to a file system not being mounted.
```

The above warning may be safely ignored.

Unexpected node reboot while probing a Sybase resource in transition (1593605)

Problem: A node may reboot unexpectedly if the Sybase resource is probed while the resource is still in transition from an online to offline state.

Normally the monitor entry point for Sybase agent completes with 5-10 seconds. The monitor script for the Sybase agent uses the qrmutil binary provided by Sybase. During a monitor, if this utility takes longer time to respond, the monitor entry point will also execute for longer duration before returning status.

Resolution: During the transition time interval between online and offline, do not issue a probe for the Sybase resource, otherwise the node may reboot.

Unexpected node reboot when invalid attribute is given (2567507)

Problem: A node may reboot unexpectedly if the Home, Version, or Server attributes are modified to invalid values while the Sybase resources are online in VCS.

Resolution: Avoid setting invalid values for the Home, Version, or Server attributes while the Sybase resources are online in VCS, to avoid panic of the node.

Symantec ApplicationHA known issues

SFHA Solutions 6.2.1 doesn’t support VCS 6.2.1 on VCSVM and AppHA 6.0 on AppVM running at the same time

SFHA Solutions 6.2.1 doesn’t support VCS 6.2.1 on VCSVM and AppHA 6.0 on AppVM running at the same time(3746362)

Workaround: If you plan to upgrade VCSVM to VCS621, perform a full upgrade for both VCSVM and AppVM.

App.RestartAttempts setting does not take effect if value is set to 2 or more

App.RestartAttempts configuration option defines the number of times Symantec ApplicationHA tries to restart a failed application or its component. Its value can range from 1 to 6.

For certain application configurations, this setting fails to take effect if its value is set to 2 or more. After successfully configuring an application, if there is a fault in the application or its dependent component, ApplicationHA attempts to restart it once. If the application fails to start, ApplicationHA reports the application state as faulted. (2508392)

This issue is applicable only for the following applications/components:

On Linux

- Custom Application
- SAP Netweaver (only in VMware)
- SAP Web Application Server (only in VMware)
- WebLogic Server (only in VMware)
- JBoss Application Server
- WebSphere Application Server
- WebSphere MQ
- Apache HTTP Server
- DB2

Workaround

Currently there is no workaround to resolve this issue.

Symantec recommends that for applications mentioned earlier, you set the App.RestartAttempts value to 1.

This ensures that ApplicationHA makes at least one attempt to restart the failed component. If the component still fails to start, ApplicationHA then declares it as faulted and takes further action as per the configuration settings (for example, a graceful reboot of the virtual machine).

Compatibility with other clustering products

Symantec Storage Foundation and High Availability Solutions runs on Symantec Cluster Server (VCS). The version of VCS used by SFHA Solutions is a customized version of VCS. Many components have been removed in order to provide a lighter footprint inside the virtual machine. You cannot run both SFHA Solutions and VCS together inside the same virtual machine. There is no method to upgrade from SFHA Solutions to VCS.

Additionally SFHA Solutions does not co-exist with other clustering solutions offered by Symantec. These include, Symantec Storage Foundation High Availability, Clustered File System, Clustered File System High Availability and Clustered Volume Manager.

Symantec High Availability tab issue

This issue applies only to VMware environments.

If you install both Symantec Storage Foundation (SF) and SFHA Solutions on the same virtual machine, and then remove SF, the Symantec High Availability tab on the vSphere client stops working. (2136077)

Workaround

When you install SFHA Solutions on a virtual machine, and then try to install Symantec Storage Foundation (SF), you may notice errors in the SF installation.

When you remove SF, you automatically remove the VRTSsfmh rpm from the system. The vSphere client needs the VRTSsfmh rpm to communicate with the virtual machine.

To reinstate VRTSsfmh, perform the following steps:

1. Install VRTSspt and VRTSsfmh rpms from the SFHA Solutions install media.
2. Stop the xprtld service:

   ```
   # /etc/init.d/xprtld stop
   ```

3. Add following line to the `/etc/opt/VRTSsfmh/xprtld.conf` file, if not present:

   ```
   namespaces vcs=/opt/VRTSvcs/portal
   ```

4. Start the xprtld service:

   ```
   # /etc/init.d/xprtld start
   ```

Application monitoring configuration freezes

This issue occurs if you configure application monitoring on systems where host names start with a hyphen. (2038685)

The application monitoring configuration may freeze and the SFHA Solutions view in the vSphere Client may not display the status of the application. If the configured application fails, SFHA Solutions takes no action.

Symantec recommends that you rename systems whose host names start with a hyphen before installing SFHA Solutions and configuring application monitoring on those systems.

Symantec Storage Foundation and High Availability Solutions commands do not display the time as per the locale settings

This issue occurs with all the SFHA Solutions commands that display the date and time stamp in the output. The date and time stamp do not display as per the locale settings on the system. They are displayed only in English. (2142740)

ApplicationHA fails to work if Veritas Operations Manager is uninstalled

In a VMware environment, if you use the vCenter integrated method, the Managed Host components of Veritas Operations Manager (VOM) are installed on the Console Server and the guest virtual machines, during the ApplicationHA installation.

In a KVM environment, the Managed Host components of Veritas Operations Manager (VOM) are installed on the physical host and the virtual machine, during the ApplicationHA installation. (2361128, 2323516)

Uninstallation of VOM removes the VRTSsfmh RPM which breaks the ApplicationHA functionality. The VRTSsfmh RPM contains the 'Veritas Storage Foundation Messaging Service' (xprtld) that is used by both, ApplicationHA and VOM.

Note: This issue also occurs when you uninstall the Veritas Operations Manager Central Server.

Workaround

Perform the following steps

1 Insert the ApplicationHA software disc into your system drive and navigate to the directory that contains the RPM for the required operating system:

In a VMware environment:

Operating system	Directory
Oracle Linux 6	rhel6_x86_64
Red Hat Enterprise Linux 6	rhel6_x86_64
SUSE Linux Enterprise Server 11	sles11_x86_64

In a KVM environment:

Operating system	Directory
Red Hat Enterprise Linux 6	rhel6_x86_64
Red Hat Enterprise Linux 7	rhel7_x86_64

For example, to install ApplicationHA on a machine running the RHEL 6 operating system,

```
# cd cdrom_root/applicationha/rhel6_x86_64/rpms
```

2 Run the following command:

```
# rpm -ivh VRTSsfmh-*.rpm
```

Where * is the version of the Linux rpm. For example, version 4.1.119.0 for ApplicationHA 6.0 and 6.0.0.0 for ApplicationHA 6.1.

3 Stop the `xprtld` service.

```
# /etc/init.d/xprtld stop
```

4 Ensure that the file `/etc/opt/VRTSsfmh/xprtld.conf` contains the following text:

```
namespaces vcs=/opt/VRTSvcs/portal
```

5 Start the `xprtld` service.

```
# /etc/init.d/xprtld start
```

6 In a VMware environment, from the Symantec High Availability tab on the vSphere client, configure single sign-on (SSO).

For more information on configuring SSO, refer to the *Symantec ApplicationHA User's Guide*

Refreshing the Symantec High Availability view tab multiple times displays a network connectivity error

This issue is typically observed in case of IE7 browser.

Symantec High Availability tab of vSphere Client orSymantec High Availability view of Veritas Operations Manager refreshes the application status every 60 seconds. However, in case of network failure if you manually refresh the ApplicationHA view multiple times, IE displays a network connectivity error. (2379946, 2379707)

If you click **Ok** on the error message and then click another virtual machine on the VOM Management Server console, then the Symantec High Availability view displays the application status of an unknown application.

In the vSphere Client, you click **Ok** on the error message and then click another virtual machine, then the Symantec High Availability tab displays the application status of an unknown application.

This issue also occurs if you refresh the Symantec High Availability view or tab, and simultaneously reset the virtual machine.

Workaround

For details, refer to the following knowledge base article from Microsoft.

http://support.microsoft.com/kb/927917#more_information

VCS configuration incorrectly retains read-write mode

This issue occurs only in a KVM environment.

When you execute the enable_applicationha script on the physical host, if an error occurs, the script exits. However, the VCS configuration remains in the read-write mode. In this mode, the configuration is vulnerable to unintentional editing. (2607134)

Workaround

Revert the VCS configuration to the read-only mode by using the following command:

```
# haconf -dump -makero
```

Configuration option of SFHA Solutions installer malfunctions

When you run the Symantec Storage Foundation and High Availability Solutions installer, it displays the following option to configure SFHA Solutions: **Configure an Installed Product**.

If you specify this option, the installer fails to configure SFHA Solutions. Instead, the installer starts stopping certain SFHA Solutions processes. (2621468)

Workaround

Do not use the installer option to configure an application. Instead, to configure Symantec Storage Foundation and High Availability Solutions for monitoring an application, use one of the following methods:

- If you have already installed SFHA Solutions, navigate to the following URL, and use the **Configure Application Monitoring** link to launch the Symantec Storage Foundation and High Availability Solutions Application Monitoring Configuration Wizard:

  ```
  https://<virtualmachineNameorIPaddress>:5634/vcs/admin/
  application_health.html?priv=ADMIN
  ```

- You can launch the wizard from the Symantec High Availability view of the Veritas Operations Manager Management Server Console.
  For more information on working with VOM and accessing the SFHA Solutions, see the *Symantec ApplicationHA User's Guide*.
  You can launch the Symantec Storage Foundation and High Availability Solutions Configuration Wizard from the Symantec High Availability tab of the VMware vSphere client GUI.
  For more information, see the *Symantec ApplicationHA User's Guide*

Heartbeat service group may fail to come online

This issue occurs only in KVM environments.

If the high availability daemon (HAD) on the virtual machine is restarted, the configured heartbeat service group (VCSAppMonHBSG) does not automatically come online. (2605506)

Workaround

To continue application monitoring, you must manually bring the VCSAppMonHBSG online by using the following command:

```
# /opt/VRTSvcs/bin/hagrp -online VCSAppMonHBSG -sys System
```

Where *System* is name of the virtual machine.

Attributes of a virtual machine may retain stale values

This issue applies only to the KVM environment.

If the ESX/ESXi host crashes, the virtual machines may indicate stale values for attributes such as ConnectionState and SysState. The settings are updated after a virtual machine fails over to a new ESX/ESXi host. (2611726)

Application monitoring may not resume on exiting maintenance mode

If you suspend application monitoring from the Symantec High Availability view, and later resume it by clicking **Exit Maintenance Mode**, application monitoring may not resume as expected.

If you then refresh the tab/view, the Configure Application Monitoring link may appear. This issue may occasionally occur in any setup because of variations in the time taken by internal commands to complete, after you click **Exit Maintenance Mode**. In some cases, before the internal commands are complete, the High Availability Daemon (HAD) module may shut down and stop application monitoring. (3640282)

Workaround

Perform the following steps:

1. From the command line, execute the following command:

   ```
   # /opt/VRTSvcs/bin/hastart -onenode
   ```

2. From the Symantec High Availability view, try to resume application monitoring by clicking **Exit Maintenance Mode**.

Issues while working with VMware snapshots and migrating virtual machines

The following issues may occur while you are performing virtual machine administration on systems where Symantec ApplicationHA is actively monitoring applications:

- While working with virtual machine snapshots
  This issue occurs if you have installed vCenter Server version 4.0, 4.1, and 4.1 Update 1 only. This issue does not occur if you have installed vCenter Server version 5.0.
  While taking a virtual machine snapshot, the SFHA Solutions view may freeze momentarily and may not display the current state of the applications being monitored. Also, after you revert a snapshot, the virtual machine may reboot after the operation completes.

The Events view on the Tasks & Events tab in the vSphere Client displays the following warning messages:

Application heartbeat **failed** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

Application heartbeat status changed to **appStatusRed** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

Application heartbeat status changed to **appStatusGreen** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

- While migrating virtual machines to an alternate ESX host

  When you initiate a virtual machine migration, the ApplicationHA view may freeze momentarily and may not display the current state of the applications that is being monitored.

  The Events view on the Tasks & Events tab in the vSphere Client displays multiple instances of the following warning messages:

  Application heartbeat status changed to **appStatusGray** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

  Application heartbeat status changed to **appStatusGreen** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

Workaround

This is a known issue with VMware HA. Check the following VMware knowledge base article for more information about the patch for this issue:

http://kb.vmware.com/kb/1027413

Symantec recommends that you disable the application heartbeat (Disable Application Heartbeat button in the ApplicationHA view) on the virtual machine before working with snapshots or migrating the virtual machine. After the virtual machine administration activity is complete, enable the application heartbeat (Enable Application Heartbeat button in the ApplicationHA view) again.

Symantec High Availability tab may freeze

This issue occurs only in VMware environments.

The Symantec High Availability tab in the vSphere Client may freeze if SFHA Solutions is unable to establish a connection with the virtual machine. The application status in the Symantec High Availability view appears to be in a hung state and does not refresh. (2125902)

Workaround

This may occur if the virtual machine fails to respond to SFHA Solutions http requests. Either the virtual machine has moved to a suspended state or is in the process of migrating to an alternate ESX host.

Perform the following actions:

- Verify that the virtual machine is powered on and accessible over the network.
- Close the Symantec High Availability tab and open it again.
  In the vSphere Client, click another virtual machine, then click the original virtual machine again and then select the Symantec High Availability tab, or exit the vSphere Client and launch it again.

Symantec High Availability Console installation gives an error and the plugin registration fails if the installation directory contains multiple "%" characters

This issue occurs only in VMware environments.

This issue occurs while installing Symantec High Availability Console using the Symantec High Availability Console Installer. On the System Validation panel, if you customize the installation directory to a path that contains consecutive multiple "%" characters, the wizard successfully completes the verification checks and allows you to proceed further. However, when you click **Next** on the Post-install Summary panel the wizard displays a "Failed to create private domain. The system cannot find the path specified" error. You can click **Ok** on the error message and proceed with the installation. However, after the installation workflow is complete the wizard fails to register the ApplicationHA plugin on the vCenter Server.

If you verify the plugin registration using the PluginMgmt.bat utility available on the Console server, the plugin status reflects that the plugin is already registered. However, if you verify the plugin status on the Plug-in Manager available on the vCenter Server, the plugin status reflects "Download & Install".

Workaround

Launch the Symantec High Availability Console installation wizard again and provide a valid path that does not contain multiple "%" characters.

ApplicationHA guest components installation using the vSphere Client integrated menu may fail with "Failed to log-on..." error

While installing the ApplicationHA guest components using the vCenter integrated menu, the installation workflow completes successfully. However, the installation may fail with the "Failed to log-on" error on some virtual machines after the tasks are queued for installation. (2361891)

Also, a "MKS error..." may appear if you try to connect to these virtual machines using the vSphere client.

Workaround

- Refer to the VMware KB at the following location:

  ```
  http://kb.vmware.com/selfservice/microsites/search.do?
  language=en_US&cmd=displayKC&externalId=749640
  ```

- Restart the virtual machines on which the installation has failed.
- If the problem continues, contact your network administrator.

vMotion causes delay in health view and dashboard refresh

If you have configured application monitoring on a virtual machine with VMware vMotion enabled, the vMotion process gets triggered if the application faults and the virtual machine reboots. (2363462)

Due to vMotion, after a reboot the virtual machine starts and the application comes online on a failover virtual machine on a new ESX host. Even if the application is online, the ApplicationHA health view and the dashboard reflects the application status after a slight delay.

After a vMotion application heartbeat status shows "appStatusGreen" even if the application is faulted

After the application faults if you trigger VMware vMotion instead of VM reboot, the Tasks and Events of a virtual machine reflects the application status as "appStatusGreen", even if the application is faulted. (2363487)

This issue is observed if you are using the VMware vSphere 4.0 and 4.1.

During a test recovery ApplicationHA dashboard at both the sites show the updates

This issue occurs only in VMware environments.

If your VMware cluster network settings for test recovery are such that the failed over virtual machines are able to communicate with the protected site Symantec High Availability Console (due to the MAC address being the same as that of the protected site), then the updates due to the administrative tasks performed for application monitoring are reflected on the ApplicationHA dashboard at both the sites. (2363496)

Guest installation fails with an error "Failed to launch the guest installer process"

This issue is observed while installing the ApplicationHA guest components using the vSphere Client menu.

After the installation workflow is complete the virtual machine is queued for installation. However, the installation process may fail to start with a "Failed to launch the guest installer process" error in the vSphere Client tasks.

Workaround

On the virtual machine where the installation has failed run the installation wizard again.

Field selection using the Tab key may not work on the vCenter Server User Details panel

This issue occurs on the vCenter Server User Details panel during the ApplicationHA guest components installation, using the vSphere Client menu. The issue is typically observed if you have Adobe FlashPlayer version 10.1 installed on your system. (2362878)

Workaround

You have to click each field to specify the inputs.

Single sign-on with Symantec High Availability console on recovery site fails

This issue occurs only in VMware environments.

An SFHA Solutions configuration in an SRM environment involves a single sign-on (SSO) configuration between the virtual machines at the protected site and the Symantec High Availability Console at the recovery site.

If the Symantec High Availability Console server is installed on a virtual machine or a physical system that runs a Japanese locale operating system, the single sign-on configuration between the sites fails.

For a workaround, contact Symantec support.

Dashboard does not work

This issue occurs only in a VMware environment.

If you upgrade a virtual machine from Symantec Storage Foundation and High Availability Solutions 5.1, then after the upgrade, the SFHA Solutions dashboard may not display the virtual machine, if the following condition occurs:

- At the time of the upgrade, SFHA Solutions guest components are not running. (2581676)

Workaround

Perform the following steps:

1. `# /etc/init.d/vcs start`
2. Wait for VCS to start (approximately two minutes)
3. `#/opt/VRTSvcs/portal/admin/synchronize_guest_config.pl`

Storage Foundation uninstallation leads to warning

This issue occurs only in VMware environments.

If you uninstall Storage Foundation 6.0 from a virtual machine where you have unconfigured and uninstalled SFHA Solutions, the following CPI warning appears:

```
CPI WARNING V-9-40-3866 The VRTSsfmh rpm on <system_name> will be
uninstalled. Note that the system <system_name >is reporting to
the following management servers: appha://192.168.10.140
```

You can safely ignore this warning.

Users unable to copy-paste Symantec High Availability logs

This issue occurs only in VMware environments

If you click the View Logs link in the Symantec High Availability tab from the vSphere Client, you may be unable to copy-paste the log content. This issue occurs if you access the Symantec High Availability tab from the vSphere 5.5 Web Client.

This issue does not occur with vSphere 5.1 Web Client. (3504113)

Data abruptly disappears from Status and System columns of dashboard

This issue applies only to VMware environments.

When you access the Symantec High Availability Dashboard from the vSphere Web Client, data from the Status and System columns may abruptly disappear. This issue occurs only with VMware vSphere 5.1. (3509084)

Workaround

- Clear the web browser cache and then restart VMware vSphere Web Client.

- Click a tab other than Symantec High Availability tab in the VMware vSphere Web Client (for example, Storage, Reports), refresh the web browser, and then go to the Symantec High Availability tab.

Symantec High Availability tab persists even after unregistering Symantec HA plug-in from vCenter

When you add a vCenter Server to Veritas Operations Manager, the Symantec HA plug-in is registered with the vCenter Server. For virtual machines associated with that vCenter, the Symantec High Availability tab appears in the vSphere Web Client. If you unregister the plug-in, the tab should also disappear. Presently the Symantec High Availability tab erroneously persists in the vSphere Web Client. (3498886)

Workaround

Based on your configuration, perform the steps listed below.

If multiple vCenter servers are configured to support the Symantec HA Plug-in, and if you want to unregister the plug-in from all the vCenter servers, perform both the steps.

If multiple vCenter servers are configured, and if you do not need to unregister the plug-in from all the vCenter servers, then you must only restart the vSphere Web Client service.

Note: To remove the Symantec HA Plug-in add-on from the VOM Management Server, you must unregister the plug-in from all the vCenter servers, and then perform both the steps:

---

1. Delete the cached plug-in data from the following location on the VMware vSphere Web Client host:

   ```
   C:\ProgramData\VMware\vSphere Web
   Client\vc-packages\vsphere-client-serenity\com.symantec.applicationhaweb-6.1
   ```

2. Restart the VMware vSphere Web Client service.

LLT known issues

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

LLT may fail to detect when bonded NICs come up (2604437)

When LLT is configured over a bonded NIC and that bonded NIC is DOWN with the `ifconfig` command, LLT marks the corresponding link down. When the bonded

NIC is UP again using the `ifconfig` command, LLT fails to detect this change and marks the link up.

Workaround: Close all the ports and restart LLT, then open the ports again.

LLT connections are not formed when a vlan is configured on a NIC (2484856)

LLT connections are not formed when a vlan is configured on a NIC that is already used to configure an LLT link.

Workaround: Do not specify the MAC address of a NIC in the `llttab` file while configuring LLT if you want to configure a vlan later. If you have already specified the MAC address of a NIC, then delete the MAC address from the `llttab` file, and update the file before you restart LLT.

LLT port stats sometimes shows recvcnt larger than recvbytes (1907228)

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 [1810217]

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.

If you manually re-plumb (change) the IP address on a network interface card (NIC) which is used by LLT, then LLT may experience heartbeat loss and the node may panic (3188950)

With the LLT interfaces up, if you manually re-plumb the IP address on the NIC, then the LLT link goes down and LLT may experience heartbeat loss. This situation may cause the node to panic.

Workaround: Do not re-plumb the IP address on the NIC that is currently used for LLT operations. Take down the stack before you re-plumb the IP address for the LLT interface.

A network restart of the network interfaces may cause heartbeat loss for the NIC interfaces used by LLT

A network restart may cause heartbeat loss of the network interfaces configured LLT. LLT configured for UDP or LLT configured for RDMA may experience loss of heartbeat between the interfaces, which may cause the node to panic.

Workaround: Recommendations before you restart the network:

- Assess the effect of a network restart on a running cluster that is using LLT over RDMA or LLT over UDP.
- Do not use the network restart functionality to add or configure a new NIC to the system.
- If you are using the network restart functionality, make sure that the LLT interfaces are not affected.
- Increase the `llt-peerinact` time to a higher value to allow network restart to complete within that time.
  Run the `# lltconfig -T peerinact:6000` command to increase the peerinact time to 1 minute.

When you execute the /etc/init.d/llt start script to load the LLT module, the syslog file may record messages related to kernel symbols associated with Infiniband (3136418)

When you execute /etc/init.d/llt start to start the LLT module on some Linux kernel versions, the syslog file may display the following messages for multiple such symbols:

```
kernel: llt: disagrees about version of symbol ib_create_cq
kernel: llt: Unknown symbol ib_create_cq
```

The LLT module is shipped with multiple module *.ko files, which are built against different kernel versions. If the kernel version on the node does not match the kernel version against which the LLT module is built, the LLT module fails to load and logs RDMA-related messages in the syslog file. In this case, the kernel logs these messages. The modinst script loads the compatible module on the system and starts LLT without any issues.

Workaround: Rearrange the kernel versions in the `/opt/VRTSllt/kvers.lst` file such that the first line displays the kernel version that is most likely to be compatible with the kernel version on the node. This rearrangement allows the modinst script to load the best possible kernel module first. Therefore, the warning message is less likely to appear.

I/O fencing known issues

This section describes the known issues in this release of I/O fencing.

One or more nodes in a cluster panic when a node in the cluster is ungracefully shutdown or rebooted [3750577]

This happens when you forcefully stop VCS on the system, which leaves all the applications, file systems, CVM etc. online. If a node is rebooted in the online state, fencing race occurs to avoid data corruption. Then, the nodes in the sub-cluster lose the race and panic.

Workaround: The only workaround is to always cleanly shutdown or reboot any node in the cluster.

The cpsadm command fails after upgrading CP server to 6.0 or above in secure mode (2846727)

The `cpsadm` command may fail after you upgrade coordination point server (CP server) to 6.0 in secure mode. If the old VRTSat RPM 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 SFCFSHA cluster (application cluster), the installer also fails.

Workaround: Perform the following procedure on all of the nodes of the CP server.

To resolve this issue

1 Rename `cpsadm` to `cpsadmbin`:

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

2 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 "$@"
```

3 Change the permissions of the new file to 775:

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

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 *Symantec Storage Foundation and High Availability Solutions 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 information to the CP server to resolve this issue. Alternatively, you can use installer as the installer adds cluster information to the CP server during configuration.

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

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

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

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

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

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

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

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

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

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

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

```
operation failed.
CPS ERROR V-97-1400-446 Un-authorized user cpsclient@sys1,
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 cluster, 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.

Common product installer cannot setup trust between a client system on release version 5.1SP1 and a server on release version 6.0 or later [3226290]

The issue exists because the VCS 5.1SP1 release version does not support separate directories for truststores. However, VCS version 6.0 and later support separate directories for truststores. Because of this mismatch in support for truststores, you cannot set up trust between client systems and servers.

Workaround: Set up trust manually between the coordination point server and client systems using the `cpsat` or `vcsat` command so that the servers and client systems can communicate in a secure mode.

Hostname and username are case sensitive in CP server (2846392)

The hostname and username on the CP server are case sensitive. The hostname and username used by fencing to communicate with CP server must be in same case as present in CP server database, else fencing fails to start.

Workaround: Make sure that the same case is used in the hostname and username on the CP server.

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 at least 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: There is no workaround for this issue.

CoordPoint agent does not report the addition of new disks to a Coordinator disk group [2727672]

The LevelTwo monitoring of the CoordPoint agent does not report a fault even if the constituent of a coordinator disk group changes due to addition of new disks in the cooridnator disk group

Workaround: There is no workaround for this issue.

Fencing may show the RFSM state as replaying for some nodes in the cluster (2555191)

Fencing based on coordination point clients in Campus cluster environment may show the RFSM state as replaying for some nodes in the cluster.

Workaround:

Restart fencing on the node that shows RFSM state as replaying.

The vxfenswap utility deletes comment lines from the `/etc/vxfemode` file, if you run the utility with hacli option (3318449)

The vxfenswap utility uses RSH, SSH, or hacli protocol to communicate with peer nodes in the cluster. When you use vxfenswap to replace coordination disk(s) in disk-based fencing, vxfenswap copies `/etc/vxfenmode` (local node) to `/etc/vxfenmode` (remote node).

With the hacli option, the utility removes the comment lines from the remote `/etc/vxfenmode` file, but, it retains comments in the local `/etc/vxfenmode` file.

Workaround: Copy the comments manually from local `/etc/vxfenmode` to remote nodes.

When you configure CP server only for HTTPS-based communication, the engine_A.log displays a misleading message (3321101)

The engine_A.log file displays the following message when you configure CP server only for HTTPS-based communication but not for IPM-based communication.

```
No VIP for IPM specified in /etc/vxcps.conf
```

Workaround: Ignore the message.

The vxfentsthdw utility may not run on systems installed with partial SFHA stack [3333914]

The vxfentsthdw utility runs if the SFHA stack and VCS are fully installed with properly configured SF and VxVM. It also runs if the entire SFHA stack and VCS are not installed. However, partial installs where SF is installed and configured but VCS is not installed is not supported. The utility will display an error with the -g or -c options.

Workaround: Install the VRTSvxfen RPM, then run the utility from either the install media or from the /opt/VRTSvcs/vxfen/bin/ location.

When a client node goes down, for reasons such as node panic, I/O fencing does not come up on that client node after node restart (3341322)

This issue happens when one of the following conditions is true:

- Any of the CP servers configured for HTTPS communication goes down.
- The CP server service group in any of the CP servers configured for HTTPS communication goes down.
- Any of the VIPs in any of the CP servers configured for HTTPS communication goes down.

When you restart the client node, fencing configuration starts on the node. The fencing daemon, vxfend, invokes some of the fencing scripts on the node. Each of these scripts has a timeout value of 120 seconds. If any of these scripts fails, fencing configuration fails on that node.

Some of these scripts use cpsadm commands to communicate with CP servers. When the node comes up, cpsadm commands try to connect to the CP server using VIPs for a timeout value of 60 seconds. So, if the multiple cpsadm commands that are run within a single script exceed the timeout value, then the total timeout value exceeds 120 seconds, which causes one of the scripts to time out. Hence, I/O fencing does not come up on the client node.

Note that this issue does not occur with IPM-based communication between CP server and client clusters.

Workaround: Fix the CP server.

VCS fails to take virtual machines offline while restarting a physical host in RHEV and KVM environments (3320988)

In RHEV and KVM environments, the virtualization daemons `vdsmd` and `libvirtd`required to operate virtual machines are stopped before VCS is stopped during a reboot of the physical host. In this scenario, VCS cannot take the virtual machine resource offline and therefore the resource fails to stop. As a result , LLT, GAB and fencing fail to stop. However, the virtual network bridge is removed leading to the loss of cluster interconnects and causing a split-brain situation.

Workaround: If the virtual network bridge is not assigned to any virtual machine, remove the virtual bridge and configure LLT to use the physical interface. Alternatively, before initiating a reboot of the physical host, stop VCS by issuing the `hastop -local` command. The `-evacuate` option can be used to evacuate the virtual machines to another physical host.

Fencing may panic the node while shut down or restart when LLT network interfaces are under Network Manager control [3627749]

When the LLT network interfaces are under Network Manager control, then shutting down or restarting a node may cause fencing race resulting in a panic. On RHEL, VCS requires that LLT network interfaces are not put under Network Manager control, as it might cause problems when a node is shut down or restarted. During shutdown, the Network Manager service might stop before the VCS shutdown scripts are called. As a result, fencing race is triggered and the losing sub-cluster panics.

Workaround: Either exclude the network interfaces to be used by LLT from Network Manager control or disable the Network Manager service before configuring LLT. Please refer to the Red Hat documentation to do the same.

The `vxfenconfig -l` command output does not list Coordinator disks that are removed using the `vxdmpadm exclude dmpnodename=<dmp_disk/node>` command [3644431]

After you remove a Coordinator disk used by fencing or fencing disk group by running the `vxdmpadm exclude dmpnodename=<dmp_disk/node>` command, the removed disk is not listed in the `vxfenconfig -l` command output.

In case of a split brain, the `vxfen` program cannot use the removed disk as a coordination point in the subsequent fencing race.

Workaround: Run the `vxdmpadm include dmpnodename=<dmp_disk/node>` command to again enable the dmp disk. This disk will show up in subsequent `vxfencondig -l` output.

Stale .vxfendargs file lets hashadow restart vxfend in Sybase mode (2554886)

When I/O fencing is configured in customized mode, vxfend, the user mode daemon of I/O fencing, creates the `/opt/VRTSvcs/lock/.vxfendargs` file. VCS uses this file to restart the vxfend daemon when it gets killed. However, VCS does not use this file when I/O fencing is configured in Sybase mode. This file is not removed from the system when I/O fencing is unconfigured.

If user configures I/O fencing in Sybase mode and an old `/opt/VRTSvcs/lock/.vxfendargs` file is present in the system from an earlier configuration of I/O fencing in customized mode, then VCS attempts to restart the vxfend daemon every time it is killed. This interferes with the functioning of I/O fencing in the Sybase mode.

Workaround: Before you configure I/O fencing in Sybase mode, delete the `/opt/VRTSvcs/lock/.vxfendargs` file if it is present in the system.

Coordination point server-based fencing may fail if it is configured on 5.1SP1RP1 using 6.0.1 coordination point servers (2824472)

The 5.1SP1 installer (CPI) cannot set up trust between a 5.1SP1 client and a 6.0 or later server, because there are no separate directories for truststores in the 5.1SP1. When trust cannot be setup, the 5.1SP1 installer cannot configure 5.1SP1 clients to work with 6.0 or later CPS in secure mode.

Workaround:

Set up trust manually between the CPS and clients using the cpsat or the vcsat command. After that, CPS and client will be able to communicate properly in the secure mode.

The CoordPoint agent faults after you detach or reattach one or more coordination disks from a storage array (3317123)

After you detach or reattach a coordination disk from a storage array, the CoordPoint agent may fault because it reads an older value stored in the I/O fencing kernel module.

Workaround: Run the `vxfenswap` utility to refresh the registration keys on the coordination points for both server-based I/O fencing and disk-based I/O fencing. But, even if the registrations keys are not lost, you must run the `vxfenswap` utility to refresh the coordination point information stored in the I/O fencing kernel module.

For more information on refreshing registration keys on the coordination points for server-based and disk-based I/O fencing, refer to the *Symantec Cluster Server Administrator’s Guide*.

The upper bound value of FaultTolerance attribute of CoordPoint agent should be less than the majority of the coordination points. (2846389)

The upper bound value of `FaultTolerance` attribute of `CoordPoint` agent should be less than the majority of the coordination points. Currently this value is less than the number of coordination points.

GAB known issues

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.

Workaround: There is no workaround for this issue.

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.

Workaround: There is no workaround for this issue.

Software limitations

This section covers the software limitations of this release.

Note: For software limitations inherited from previous releases, see the 6.2 component product release notes. The latest product documentation is available on the Symantec website at:

https://sort.symantec.com/documents

Veritas Volume Manager software limitations

The following are software limitations in this release of Veritas Volume Manager.

It is not recommended to create a disk group with large number of objects, otherwise "Out of kernel memory" error may be reported while creating disk group or while splitting, joining or moving such a disk group (3069711)

When you create a disk group with an extremely large number of objects (volumes, snapshots, plexes, disks), you may see the following error:

```
ERROR-V-5-1-10128 Out of kernel memory
```

You may also see the error when you perform operations like split/join/move on such a disk group.

Each object has a record which is used for its description and state. These records are stored in the private region of every disk group. The default private region size is 32 MB which can accommodate a sufficient number of objects. If the private region of disk group does not have space to create a new record, the operation fails with the above error message. Typical use cases would not hit this condition.

Workaround:

The best practice is not to have an extremely large number of objects in the disk group. Instead, split the disk group into multiple disk groups.

Refer to the section "Reorganizing the contents of disk groups" in the *Administrator's Guide* for information about splitting disk groups.

After upgrade from VxVM version 5.1 SP1RP3 or version 6.0 with an encapsulated boot disk, the system fails to boot (2750782)

On Red Hat Enterprise Linux 6 (RHEL6), during the Veritas Volume Manager (VxVM) upgrade from version 5.1 SP1RP3 or version 6.0 to a higher version, the RPM runs the installation scripts of the VxVM higher version first. Then the RPM runs the uninstallation scripts of the existing VxVM version. Due to a defect in the 5.1 SP1RP3 or 6.0 uninstallation script, it corrupts the file installed by the higher version. This leads to boot failure.

Workaround:

1. Unroot the encapsulated root disk.
2. Uninstall the existing `VRTSvxvm` (5.1 SP1RP3 or 6.0) RPM.
3. Install `VRTSvxvm` of the higher version.

On RHEL 7 system, the `fstab` entries for VxFS filesystem on the VxVM volume does not mount during the boot-up phase (3587126)

On RHEL 7 when entries are added in the file systems table (`fstab`) for VxFS file system on the VxVM volume, the system enters an emergency mode during the system boot-up phase. This occurs because the `systemd` daemon is not able to find the VxVM volume while processing the `fstab`.

Note: This is not applicable to supported Linux distributions other than RHEL 7.

Workaround: As suggested in the `fstab` comment, use the `nofail mount` option for VxFS filesystem on the VxVM volume. The `nofail mount` option avoids the boot failure, if the `systemd` daemon fails to find the VxVM volume devices.

Root disk encapsulation and its dependent operations are not supported for enclosure-based naming scheme (3623681)

When the naming scheme for Veritas Volume Manager (VxVM) is set to enclosure-based naming (EBN), root disk encapsulation is not supported. Operations such as mirroring, splitting, or joining on encapsulated root disks are also not supported.

Root disk encapsulation is only supported if the device naming scheme is set to operating system-based naming (OSN) and the persistence attribute is set to yes.

Workaround:

Before encapsulating a root disk, use the following command to set the VxVM device naming scheme to OSN and the persistence attribute to yes.

```
# vxddladm set namingscheme=osn persistence=yes
```

RLINK name cannot exceed 31 characters

The `vradmin` utility truncates the RLINK name to 31 characters, as the `vxmake` utility does not support the creation of RLINK names that are longer than 31 characters.

Workarounds:

- Specify the `prlink` and `srlink` attributes using the `vradmin addsec` command, so you can choose the RLINK name in the `addsec` command line.
- If using IPv6 addresses, create host name aliases for the IPv6 addresses and specify the aliases in the `addsec` command line.

Replication software limitations

The following are replication software limitations in this release of Symantec Storage Foundation and High Availability Solutions.

The RVGPrimary agent may fail to bring the application service group online on the new Primary site because of a previous primary-elect operation not being run or not completing successfully (2043831)

In a primary-elect configuration, the RVGPrimary agent may fail to bring the application service groups online on the new Primary site, due to the existence of previously-created instant snapshots. This may happen if you do not run the `ElectPrimary` command to elect the new Primary or if the previous `ElectPrimary` command did not complete successfully.

Workaround: Destroy the instant snapshots manually using the `vxrvg -g` *`dg`* `-P` *`snap_prefix`* `snapdestroy` *`rvg`* command. Clear the application service group and bring it back online manually.

While vradmin commands are running, vradmind may temporarily lose heart beats (2071568, 2275444)

This issue may occasionally occur when you use `vradmin` commands to administer VVR. While the `vradmin` commands run, `vradmind` may temporarily lose heartbeats, and the commands terminate with the following error message:

```
VxVM VVR vradmin ERROR V-5-52-803 Lost connection to host host;
terminating command execution.
```

Workaround:

To resolve this issue

1 Depending on the application I/O workload and network environment, uncomment and increase the value of the`IPM_HEARTBEAT_TIMEOUT`variable in the `/etc/vx/vras/vras_env`on all the hosts of the RDS to a higher value. The following example increases the timeout value to 120 seconds.

```
export IPM_HEARTBEAT_TIMEOUT
IPM_HEARTBEAT_TIMEOUT=120
```

2 Restart`vradmind`on all the hosts of the RDS to put the new `IPM_HEARTBEAT_TIMEOUT`value into affect. Enter the following on all the hosts of the RDS:

```
# /etc/init.d/vras-vradmind.sh restart
```

Running SUSE Linux and using Novell's YaST tool to configure an IPv6 address may result in an error (1679261)

When Novell's YaST tool is invoked to configure an IPv6 address on a different network interface and if:

- the host name, the DNS server name and domain name are specified to the YaST tool.
- IPv6 address is assigned by the Dynamic Host Configuration Protocol (DHCP).
- the "Write Hostname to /etc/hosts" option is selected (this is selected by default).

This results in the `vradmin` command returning the following error:

```
VxVM VVR vradmin ERROR V-5-52-488 RDS has configuration error related
to the master and logowner.
```

This happens because the YaST tool can replace the `/etc/hosts` entry containing `127.0.0.2` from the IPv4 host name to the specified new IPv6 host name. For example:

```
127.0.0.2 v6hostname.space.ipv6.com v6hostname
```

Workaround: The following procedure resolves this issue.

To resolve this issue

1. Edit the `/etc/hosts` file to specify the correct IPv6 address.
2. Restart the `vradmind` daemon on all VVR hosts:

   ```
   # /etc/init.d/vras-vradmind.sh restart
   ```

vradmin syncvol command compatibility with IPv6 addresses (2075307)

The `vradmin syncvol` command does not work with the compressed form of IPv6 addresses if the target disk group and volume names are not specified.

Workaround: In IPv6 environments, if you run the `vradmin syncvol` command and identify the target host using the compressed form of the IPv6 address, then you also need to specify the target disk group and volume names.

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

Node may panic if HAD process is stopped by force and then node is shut down or restarted [3640007]

A node may panic if the HAD process running on it is stopped by force and then it is shut down or restarted.This limitation is observed when you perform the following steps on a cluster node:

1. Stop the HAD process with the `force` flag.

   ```
   # hastop -local -force
   ```

   or

   ```
   # hastop -all -force
   ```

2. Restart or shut down the node.

The node panics because forcefully stopping VCS on the node leaves all the applications, file systems, CVM, and other process online on that node. If the same node is restarted in this starte, VCS triggers a fencing race to avoid data curruption. However, the restarted node loses the fencing race and panics.

Workaround: No workaround.

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.

Mount agent limitations

The Mount agent has the following limitations:

- The Mount agent mounts a block device at only one mount point on a system. After a block device is mounted, the agent cannot mount another device at the same mount point.
- Mount agent does not support:
  - ext4 filesystem on SLES 11, SLES 11SP2
  - ext4 filesystem configured on VxVM
  - xfs filesystem configured on VxVM

Share agent limitations

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

Driver requirements for DiskReservation agent

The VRTSvcsdr package ships the scsiutil utility. DiskReservation agent supports only those drivers supported by the scsiutil utility.

Volumes in a disk group start automatically irrespective of the value of the StartVolumes attribute in VCS [2162929]

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.

Application agent limitations

- ProPCV fails to prevent execution of script-based processes configured under MonitorProcesses.

Campus cluster fire drill does not work when DSM sites are used to mark site boundaries [3073907]

The campus cluster FireDrill agent currently uses the SystemZones attribute to identify site boundaries. Hence, campus cluster FireDrill is not supported in DSM enabled environment.

Workaround: Disable DSM and configure the SystemZones attribute on the application service group to perform the fire drill.

Mount agent reports resource state as OFFLINE if the configured mount point does not exist [3435266]

If a configured mount point does not exist on a node, then the Mount agent reports the resource state as OFFLINE instead of UNKNOWN on that particular node. If an attempt is made for onlining the resource, it fails on that node as the mount point does not exist.

Workaround: Make sure that configured mount point exists on all nodes of the cluster or alternatively set the CreateMntPt attribute value of Mount agent to 1. This will ensure that if a mount point does not exist then it will create while onlining the resource.

Limitation of VMwareDisks agent to communicate with the vCenter Server [3528649]

If VMHA is not enabled and the host ESX faults then even after the disks are attached to the target virtual machine, they remain attached to the failed virtual machine. This issue occurs because the request to detach the disks fails since the host ESX itself has faulted. The agent then sends the disk attach request to the vCenter Server and attaches the disks to the target virtual machine. Even though the application availability is not impacted, the subsequent restart of the faulted virtual machine fails. This issue occurs because of the stale link between the virtual machine and the disks attached. Even though the disks are now attached to the target virtual machine the stale link with the failed virtual machine still exists.

Workaround: Detach the disks from the failed virtual machine and then restart the virtual machine.

Limitations related to VCS engine

Loads fail to consolidate and optimize when multiple groups fault [3074299]

When multiple groups fault and fail over at the same time, the loads are not consolidated and optimized to choose the target systems.

Workaround: No workaround.

Preferred fencing ignores the forecasted available capacity [3077242]

Preferred fencing in VCS does not consider the forecasted available capacity for fencing decision. The fencing decision is based on the system weight configured.

Workaround: No workaround.

Failover occurs within the SystemZone or site when BiggestAvailable policy is set [3083757]

Failover always occurs within the SytemZone or site when the BiggestAvailable failover policy is configured. The target system for failover is always selected based on the biggest available system within the SystemZone.

Workaround: No workaround.

Load for Priority groups is ignored in groups with BiggestAvailable and Priority in the same group[3074314]

When there are groups with both BiggestAvailable and Priority as the failover policy in the same cluster, the load for Priority groups are not considered.

Workaround: No workaround.

Symantec cluster configuration wizard limitations

Wizard fails to configure VCS resources if storage resources have the same name [3024460]

Naming storage resources like disk group and volumes with the same name is not supported as the Symantec High Availability wizard fails to configure the VCS resources correctly.

Workaround: No workaround.

Environment variable used to change log directory cannot redefine the log path of the wizard [3609791]

By default, the Symantec cluster configuration wizard writes the logs in `/var/VRTSvcs/log` directory. VCS provides a way to change the log directory through environment variable VCS_LOG, but this does not apply to the logs of VCS wizards.

Workaround: No workaround.

Limitations related to the VCS database agents

DB2 RestartLimit value [1234959]

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

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

Sybase agent does not perform qrmutil based checks if Quorum_dev is not set (2724848)

If you do not set the Quorum_dev attribute for Sybase Cluster Edition, the Sybase agent does not perform the qrmutil-based checks. This error in configuration may lead to undesirable results. For example, if qrmutil returns failure pending, the agent does not panic the system. Thus, the Sybase agent does not perform qrmutil-based checks because the Quorum_dev attribute is not set.

Therefore, setting Quorum_Dev attribute is mandatory for Sybase cluster edition.

Pluggable database (PDB) online may timeout when started after container database (CDB) [3549506]

PDB may take long time to start when it is started for the first time after starting CDB. As a result, the PDB online initiated using VCS may cause ONLINE timeout and the PDB online process may get cancelled.

Workaround: Increase the OnlineTimeout attribute value of the Oracle type resource.

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.