

# Symantec™ Storage Foundation and High Availability 6.1 Release Notes - AIX

# Symantec™ Storage Foundation and High Availability Release Notes

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

Product version: 6.1

Document version: 6.1 Rev 5

## Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

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

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

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

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

# Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

[www.symantec.com/business/support/index.jsp](http://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](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportolutions@symantec.com</a>

## 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](mailto: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 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>

# Symantec Storage Foundation and High Availability Release Notes

This document includes the following topics:

- [About this document](#)
- [Component product release notes](#)
- [About the Symantec Storage Foundation and High Availability Solutions products](#)
- [About Symantec Operations Readiness Tools](#)
- [Important release information](#)
- [Changes introduced in 6.1](#)
- [No longer supported](#)
- [System requirements](#)
- [Fixed issues](#)
- [Known issues](#)
- [Software limitations](#)
- [Documentation](#)

## About this document

This document provides important information about Symantec Storage Foundation and High Availability (SFHA) version 6.1 for AIX. Review this entire document before you install or upgrade SFHA.

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

This is "Document version: 6.1 Rev 5" of the *Symantec Storage Foundation and High Availability Release Notes*. Before you start, make sure that you are using the latest version of this guide. The latest product documentation is available on the Symantec Web site at:

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

## Component product release notes

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

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

`/docs/product_name`

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

This release includes the following component product release notes:

- *Symantec Storage Foundation Release Notes* (6.1)
- *Symantec Cluster Server Release Notes* (6.1)

## About the Symantec Storage Foundation and High Availability Solutions products

Symantec Storage Foundation and High Availability (SFHA) Solutions is a set of products that provide storage administration and management in a heterogeneous storage environment.

This section can help you determine which product you need.

[Table 1-1](#) shows the benefits of each product and its components.

**Table 1-1** SFHA Solutions product comparisons

Product	Components	Benefits
Symantec Cluster Server (VCS) connects multiple, independent systems into a management framework for increased availability. Each system, or node, runs its own operating system and cooperates at the software level to form a cluster. VCS links commodity hardware with intelligent software to provide application failover and control. When a node or a monitored application fails, other nodes can take predefined actions to take over and bring up services elsewhere in the cluster.	VCS	<ul style="list-style-type: none"> <li>■ Minimizes downtime</li> <li>■ Facilitates the consolidation and the failover of servers</li> <li>■ Effectively manages a wide range of applications in heterogeneous environments</li> <li>■ Provides data integrity protection through I/O fencing</li> <li>■ Provides High Availability of applications</li> </ul>
Dynamic Multi-Pathing (DMP) provides multi-pathing functionality for the devices configured on the system. The product creates DMP metadevices (also known as DMP nodes) to represent all the device paths to the same physical LUN.	DMP	<ul style="list-style-type: none"> <li>■ Extends DMP metadevices to support OS native logical volume managers (LVM)</li> <li>■ Provides improved storage I/O performance with load balancing</li> <li>■ Provides storage path failure protection and fast failover</li> <li>■ Centralizes storage path management regardless of operating system or storage hardware</li> </ul>
Symantec Replicator Option enables cost-effective replication of data over IP networks, giving organizations an extremely flexible, storage hardware independent alternative to traditional array-based replication architectures.	VVR	<p>Volume Replicator (VVR)</p> <ul style="list-style-type: none"> <li>■ Provides block-based continuous replication</li> <li>■ Provides effective bandwidth management</li> <li>■ Supports cross-platform replication, and replication in a Portable Data Container (PDC) environment</li> </ul>
<p>Storage Foundation (SF) is a storage management offering that consists of Veritas Volume Manager (VxVM), Veritas File System (VxFS), and DMP.</p> <p>Veritas Volume Manager is a storage management subsystem that enables you to manage physical disks and logical unit numbers (LUNs) as logical devices called volumes.</p> <p>Veritas File System is an extent-based, intent logging file system.</p>	DMP, VxVM, VxFS	<ul style="list-style-type: none"> <li>■ Increased storage utilization across heterogeneous environments</li> <li>■ Deduplication and compression</li> <li>■ Automated storage tiering</li> <li>■ Centralized storage management</li> <li>■ Easy OS and storage migration with minimum downtime</li> <li>■ All benefits of DMP</li> </ul>
Storage Foundation High Availability (SFHA) includes all the functionality of SF plus the high availability of VCS.	DMP, VxVM, VxFS, VCS	<ul style="list-style-type: none"> <li>■ All benefits of DMP</li> <li>■ All benefits of SF</li> <li>■ All benefits of VCS</li> </ul>

**Table 1-1** SFHA Solutions product comparisons (*continued*)

Product	Components	Benefits
<p>Storage Foundation Cluster File System High Availability (SFCFSHA) extends Symantec Storage Foundation to support shared data in a storage area network (SAN) environment. Multiple servers can concurrently access shared storage and files transparently to applications.</p> <p>Cluster Volume Manager (CVM) extends VxVM to support shared disk groups. Cluster File System (CFS) extends VxFS to support parallel clusters.</p>	DMP, VxVM, VxFS, VCS, CVM, SFCFSHA	<ul style="list-style-type: none"> <li>■ All benefits of DMP</li> <li>■ All benefits of SF</li> <li>■ All benefits of VCS</li> <li>■ Increased automation and intelligent management of availability and performance across shared storage</li> </ul>
<p>Storage Foundation for Oracle RAC (SFRAC) is an integrated suite of Symantec storage management and high-availability software. The software is engineered to improve performance, availability, and manageability of Real Application Cluster (RAC) environments.</p>	DMP, VxVM, VxFS, VCS, CVM, SFCFSHA, plus support for Oracle RAC	<ul style="list-style-type: none"> <li>■ All benefits of DMP</li> <li>■ All benefits of SF</li> <li>■ All benefits of VCS</li> <li>■ All benefits of SFCFSHA</li> <li>■ Support for Oracle RAC that simplifies database management while fully integrating with the Oracle clustering solution</li> </ul>
<p>Storage Foundation foAr Sybase ASE CE is an integrated suite of Symantec storage management and high-availability software. The software is engineered to improve performance, availability, and manageability of Sybase ASE CE on UNIX platforms.</p>	DMP, VxVM, VxFS, VCS, CVM, SFCFSHA, plus support for Sybase ASE CE	<ul style="list-style-type: none"> <li>■ All benefits of DMP</li> <li>■ All benefits of SF</li> <li>■ All benefits of VCS</li> <li>■ All benefits of SFCFSHA</li> <li>■ Support for SF Sybase ASE CE that simplifies database management while fully integrating with the Sybase clustering solution</li> </ul>

**Table 1-1** SFHA Solutions product comparisons (*continued*)

Product	Components	Benefits
<p>Symantec ApplicationHA provides monitoring capabilities for applications running inside virtual machines in the virtualization environment. Symantec ApplicationHA adds a layer of application awareness to the core high availability functionality that is offered by Symantec Cluster Server (VCS) in the physical host. Symantec ApplicationHA is based on VCS, and uses similar concepts such as agents, resources, and service groups. However, Symantec ApplicationHA has a lightweight server footprint that enables faster installation and configuration in virtualization environments.</p>	<p>Symantec ApplicationHA, VCS</p>	<ul style="list-style-type: none"> <li>■ Out of the box integration with VCS</li> <li>■ Full visibility and control over applications with the ability to start, stop, and monitor applications running inside virtual machines</li> <li>■ High availability of the application as well as the virtual machine inside which the application runs</li> <li>■ A series of incremental fault management remedies that include application restart, graceful virtual machine reboot, forceful virtual machine reboot, and vMotion. ApplicationHA tries the first two remedies and upon failure prompts VMwareHA to try the next two remedies.</li> <li>■ Standardized way to manage applications using a single interface that is integrated with the Veritas Operations Manager console</li> <li>■ Specialized Application Maintenance mode, in which Symantec ApplicationHA enables you to intentionally take an application out of its purview for maintenance or troubleshooting</li> </ul>
<p>Veritas Operations Manager provides a centralized management console for Symantec Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports.</p>	<p>All</p>	<ul style="list-style-type: none"> <li>■ Centralized, standardized way to manage the various features in the Storage Foundation products</li> <li>■ Visual interface for managing individual hosts and their storage</li> <li>■ Visibility into all instances of Storage Foundation that are running in the datacenter, across multiple operating systems</li> </ul>

**Table 1-1** SFHA Solutions product comparisons (*continued*)

Product	Components	Benefits
<p>Symantec Cluster Server (VCS) agents provide high availability for specific resources and applications. Each agent manages resources of a particular type. Typically, agents start, stop, and monitor resources and report state changes.</p> <p>In addition to the agents that are provided in this release, other agents are available through an independent Symantec offering called the Symantec High Availability Agent Pack. The agent pack includes the currently shipping agents and is re-released quarterly to add the new agents that are now under development.</p> <p>You can download the latest agents from the Symantec Operations Readiness (SORT) website at:</p> <p><a href="https://sort.symantec.com/agents">https://sort.symantec.com/agents</a></p>	VCS, Symantec ApplicationHA	<ul style="list-style-type: none"><li>■ All benefits of VCS</li><li>■ All benefits of Symantec ApplicationHA</li></ul>

## About Symantec Operations Readiness Tools

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

SORT can help you do the following:

- |   |   |
|---|---|
| <p>Prepare for your next installation or upgrade</p>          | <ul style="list-style-type: none"> <li>■ List product installation and upgrade requirements, including operating system versions, memory, disk space, and architecture.</li> <li>■ Analyze systems to determine if they are ready to install or upgrade Symantec products and generate an Installation and Upgrade custom report.</li> <li>■ List patches by product or platform, and in the order they need to be installed. Display and download the most recent patches or historical patches.</li> <li>■ Display Array Support Library (ASL) details by vendor, platform, or Storage Foundation and High Availability (SFHA) version. ASLs make it easier to manage arrays that are connected to SFHA-based servers.</li> <li>■ List VCS and ApplicationHA agents, documentation, and downloads based on the agent type, application, and platform.</li> </ul>  |
| <p>Identify risks and get server-specific recommendations</p> | <ul style="list-style-type: none"> <li>■ Analyze your servers for potential environmental risks. Generate a Risk Assessment custom report with specific recommendations about system availability, storage use, performance, and best practices.</li> <li>■ Display descriptions and solutions for thousands of Symantec error codes.</li> </ul>  |
| <p>Improve efficiency</p>                                     | <ul style="list-style-type: none"> <li>■ Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDDs), documentation, product releases, Hardware Compatibility Lists (HCLs), and VCS/ApplicationHA agents.</li> <li>■ Quickly gather installed Symantec product and license key information from across your production environment. Generate a License/Deployment custom report that includes product names, versions, and platforms, server tiers, Symantec Performance Value Units (SPVUs), and End of Service Life dates.</li> <li>■ List and download Symantec product documentation including product guides, manual pages, compatibility lists, and support articles.</li> <li>■ Access links to important resources on a single page, including Symantec product support, SymConnect forums, customer care, Symantec training and education, Symantec FileConnect, the licensing portal, and my.symantec.com. The page also includes links to key vendor support sites.</li> <li>■ Use a subset of SORT features from your iOS device. Download the application at:<br/> <a href="https://sort.symantec.com/mobile">https://sort.symantec.com/mobile</a></li> </ul> |

---

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

---

To access SORT, go to:

<https://sort.symantec.com>

## Important release information

- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:  
<http://www.symantec.com/docs/TECH211540>
- 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/TECH213121>

---

**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 6.1

This section lists the changes in Symantec Storage Foundation and High Availability 6.1.

### Changes related to installation and upgrades

The product installer includes the following changes in 6.1.

## Support for SFHA 6.1 installations from any supported operating system to any other supported operating system

You can use the Deployment Server or the web-based installer to install your 6.1 Symantec products on a target system that runs any supported UNIX or Linux platform, even if the source system and target system are running on different UNIX or Linux platforms. Prior to 6.1, releases still require the same platform, architecture, distribution, and version of the operating system.

See the *Installation Guide* for more information.

## Improved patching and updating process

You can now download product maintenance releases and public hot fix releases directly from the Symantec Operations Readiness Tools (SORT) website using the installer. When you use the `installer` command with the `-version` option, the installer now lists the available GA releases, maintenance releases, and hot fix releases. If you have Internet access, you can follow the installer prompts to download available patches and hot fixes to your local system.

Downloading patches and hot fixes requires the installer to make outbound networking calls. If you know your systems are behind a firewall, or do not want the installer to make outbound networking calls, you can disable external network attempts by running the installer using the no Internet patch center (`-noipc`) option. When using the `-noipc` option, the installer does not try to connect to SORT website. For example:

```
# ./installer -version -noipc system1 system2
```

See the *Installation Guide* for more information.

## Automatic download of installer hot fixes

If you are running the 6.1 product installer, and your system has Internet access, the installer automatically imports any needed installer hot fix, and begins using it.

If your system does not have Internet access, you can still download installer hot fixes manually using the [Symantec Operations Readiness Tools](#) patch finder tool.

Automatic downloading of installer hot fixes requires the installer to make outbound networking calls. If you know your systems are behind a firewall, or do not want the installer to make outbound networking calls, you can disable external network attempts by running the installer using the no Internet patch center (`-noipc`) option.

See the *Installation Guide* for more information.

## Support for centralized installations using the Deployment Server

The Deployment Server is a script that makes it easier to install or upgrade SFHA releases. The Deployment Server lets you store multiple release images in one central location and deploy them to systems of any supported UNIX or Linux operating system (6.1 or later). Prior to 6.1, releases still require the same platform, architecture, distribution, and version of the operating system. You can use the Deployment Server if you want to install or upgrade multiple releases and or multiple platforms.

The Deployment Server lets you do the following as described in [Table 1-2](#).

**Table 1-2** Deployment Server functionality

Feature	Description
Manage release images	<ul style="list-style-type: none"><li>■ View available Storage Foundation releases.</li><li>■ Download maintenance and hot fix release images from the Symantec Operations Readiness Tools (SORT) website into a repository.</li><li>■ Load the downloaded release image files from FileConnect and SORT into the repository.</li><li>■ View and remove release image files stored in the repository.</li></ul>
Check versions	<ul style="list-style-type: none"><li>■ Discovers filesets and patches installed on designated systems and informs you of the product and version installed, including installed hot fixes.</li><li>■ Identify base, maintenance, and hot fix level upgrades to your system and download maintenance and hot fix releases.</li><li>■ Query SORT for the most recent updates.</li></ul>
Install or upgrade systems	<ul style="list-style-type: none"><li>■ Install or upgrade a release stored in the repository on selected systems.</li><li>■ In release 6.1 and later:<ul style="list-style-type: none"><li>■ Install hot fix level releases.</li><li>■ Install SFHA from any supported UNIX or Linux operating system to any other supported UNIX or Linux operating system.</li><li>■ Automatically load the script-based installer hot fixes that apply to that release.</li></ul></li></ul>

---

**Note:** The Deployment Server is available only for the script-based installer, not the web-based installer.

---

See the *Installation Guide* for more information.

## Support for simultaneously installing or upgrading base releases, maintenance patches, and hot fixes

Beginning with version 6.1, Symantec offers you a method to easily install or upgrade your systems directly to a base, maintenance, or hot fix level in one step using Install Bundles. Install Bundles is the ability for installers to merge so customers can install or upgrade directly to maintenance or hot fix levels in one execution. Install Bundles consists of executing the installer from a GA release with a pointer to a higher maintenance or hot fix release. The installer installs them both as if they were combined in the same release image. The various scripts, filesets, and patch components are merged and multiple releases are installed together as if they are one install entity.

---

**Note:** This feature is not supported by the Deployment Server.

---

There are five possible methods of integration. All upgrades must be executed from the highest level script.

- Base + maintenance
- Base + hot fix
- Maintenance + hot fix
- Base + maintenance + hot fix
- Base or maintenance + multiple hot fixes

See the *Installation Guide* for more information.

## Changes related to Symantec Storage Foundation and High Availability (SFHA)

Storage Foundation and High Availability (SFHA) includes the following changes in 6.1.

### Changes related to Veritas Volume Manager

Veritas Volume Manager (VxVM) includes the following changes in 6.1:

#### DMP support for thin reclamation commands

In this release, Dynamic Multi-Pathing (DMP) adds support for the `UNMAP` command for thin reclamation. The Array Support Library (ASL) for each array uses the most suitable reclamation method supported for the array. In previous releases, DMP

performed reclamation with the WRITE\_SAME method for SCSI and the TRIM method for SSD devices. You can use the `vxdisk -p list` command to show the reclaim interface that is supported for a particular device.

For more information, see the *Administrator's Guide*.

## Enhancements to the disk cloning operations

In this release, the following enhancements are made to the VxVM support for hardware clone disks:

- When you import a disk group, the disks with the `udid_mismatch` flag display the `clone_disk` flag regardless of whether the system sees the original source disks. In previous releases, the `clone_disk` flag was hidden if the source disks were not visible to the system.
- By default, VxVM now prevents the import of a partial set of disks in a clone disk group when the `-o updateid` option is specified. This behavior prevents the missing disks from being permanently detached from the new disk group. You can specify the `-f` option to partially import the clone disk group with `-o updateid`.
- When you import a set of clone disks with the `-o updateid` option and specify a new disk group name, the disk group becomes a standard disk group with updated disk and disk group identifiers. This operation clears the `udid_mismatch` flag or the `clone_disk` flag from the disks.
- When you import a set of clone disks with the `-o updateid` option, you can use the `vxvg import` with the `-c` option to convert the existing disk group to a standard disk group with updated disk and disk group identifiers. This operation clears the `udid_mismatch` flag or the `clone_disk` flag from the disks. You cannot perform this operation if the source disk group is already imported on the same host.
- You can now update the UDID for a disk and remove the `udid_mismatch` flag and the `clone_disk` flag with a single operation. Updating the UDID aligns it with the UDID detected by the DDL.  
`vxdisk -c updateudid diskname`
- You cannot create disk groups on `udid_mismatch` or `clone_disk` disks.
- If disks are falsely marked as `udid_mismatch`, you can use `vxvg -c init` option to create disk groups on them.
- If the disk group has multiple clone copies, and you import the disk group with a tagname, the disks that have tags set will be selected. The tag-based import operation gives higher priority to disks with the tags set rather than the set of disks that were last imported. In previous releases, if multiple clone copies had

the same disk group id, the import operation gave preference to the last import time.

## Enhancements to the Dynamic Reconfiguration tool

This section describes enhancements to the Dynamic Reconfiguration tool in this release. The Dynamic Reconfiguration tool now:

- Prompts you to rename devices during a Dynamic Reconfiguration operation, if appropriate, and if `avid=no` in the naming scheme. If you agree, the tool renames the devices and refreshes the device list.  
For example, if you have removed the LUN named `xyz_8`, which leaves the entries `xyz_7` and `xyz_9`. The DR tool prompts you whether you want to rename the LUNs. If you agree, `xyz_9` is renamed to `xyz_8`.
- Logs messages for each use of the tool, in the format `dmpdr_yyyymmdd_HHMM.log`.
- Accepts a file containing a list of devices as input to the removal operation.
- Displays all LUNs that are not operating as candidates for removal.
- Supports pattern matching to select disks for removal. For example, you can use an asterisk (\*) to match multiple characters and a question mark (?) to match a single character. This functionality replaces the option to specify a range of devices.
- If you quit a disk removal operation without physically removing the disks, the Dynamic Reconfiguration tool prompts you to run `vxdisksetup` over the selected disks to avoid data corruption.

## Changes related to Veritas File System

Veritas File System (VxFS) includes the following changes in 6.1:

### Support for 64-bit quotas

Starting in release 6.1, 64-bit quotas are supported on disk layout Version 10. Users were earlier limited to set quota usage limits only up to 1 terabyte, restricting functionality in high data usage environments. With the support for 64-bit quotas, the quota usage limit can be set up to 4 exabytes.

As for 32-bit quotas, this continues to be supported on disk layout Version 9 or earlier. The same quota commands can be used for both 32-bit and 64-bit quotas.

As for 64-bit quotas, there are two new quotas files. For group quotas the file name is `quotas.grp.64` and for user quotas the file name is `quotas.64`. These files will be created on each file system after the disk layout version upgrade is completed.

See the *Administrator's Guide* for more information on quota files on Veritas File System.

See the *Installation Guide* for more information on upgrading disk layout versions.

### **maxlink support**

Added support for more than 64K sub-directories. If maxlink is disabled on a file system, the sub-directory limit will be 32K by default. If maxlink is enabled on a file system, this allows you to create up to  $4294967295(2^{32} - 1)$  sub-directories.

By default maxlink is disabled.

See the *Administrator's Guide*.

### **Disk layout Version 10**

In this release, disk layout Version 10 is now the default version.

Version 10 disk layout enables support for maxlink.

See the *Administrator's Guide*.

### **vxfssstat command can display per file system memory and VOP statistics**

The `vxfssstat` command can now display per file system memory and VOP statistics. The following options display the statistics:

- B Displays per file system metadata buffer cache statistics.
- I Displays per file system inode cache and DNLC statistics.
- x An already existing option that displays per file system statistics, and now additionally displays the newly added memory and VOP counters. VOP counters include VOP time and VOP count.

## **Changes related to SFDB tools**

The following sections describe the changes related to Storage Foundation for Databases (SFDB) tools in 6.1.

### **Reverse Resync for Oracle database recovery**

In this release, the SFDB tools reintroduce the Reverse Resync feature for Oracle database recovery.

Reverse Resynchronization or Reverse Resync process helps in recovering a database from its volume snapshots using FlashSnap service.

Storage Foundation Database FlashSnap service is used to reverse resynchronize an online point-in-time copies image of a database in an Oracle environment.

Reverse Resync feature was supported in 5.X release. This feature was discontinued for 6.0 and 6.0.1 releases. In the current release, Reverse Resync feature is reintroduced with the following changes:

- You can perform ReverseResyncBegin operation after ReverseResyncAbort operation
- You can control the database recovery in ReverseResyncBegin operation using the new (optional) parameters:

```
Reverse_Resync_Recovery
```

```
Reverse_Resync_Archive_Log
```

Use the following commands for reverse resynchronization of the snapshot volume:

- `vxsfadm -o rrbegin` to start the Reverse Resync operation
- `vxsfadm -o rrcommit` to commit the Reverse Resync changes
- `vxsfadm -o rrabort` to abort or cancel the Reverse Resync operation and to go back to the original data volumes

---

**Note:** Reverse resync is not supported for RAC databases.

---

### Supported DB2 configurations

In this release, SFDB tools are supported with DB2 10.1 release.

### Support for instant mode snapshots for Oracle RAC databases

In 6.1, the SFDB tools support instant mode snapshots for Oracle RAC databases.

### Changes related to replication

Symantec Storage Foundation and High Availability Solutions includes the following changes related to replication in 6.1:

#### VVR replication performance improvements using bulk transfer

To effectively use network bandwidth for replication, data is replicated to a disaster recovery (DR) site in bulk at 256 KB. This bulk data transfer reduces Volume Replicator (VVR) CPU overhead and increases the overall replication throughput. With compression enabled, bulk data transfer improves the compression ratio and reduces the primary side CPU usage. Bulk data transfer is not supported with bunker replication, and in cross-platform replication.

## VVR I/O throughput improvements using batched writes

Batched writing of multiple application writes to the SRL increases application I/O throughput and lowers VVR CPU utilization. This is achieved by allocating a log location for a set of application writes, and then batching the writes together to form a single write to the SRL, and therefore replacing the multiple writes to the SRL at the primary RVG.

## Changes to LLT, GAB, and I/O fencing

This section covers new features or enhancements made to LLT, GAB, and I/O fencing.

### Changes to LLT

Symantec Cluster Server includes the following changes to LLT in 6.1:

#### LLT command changes

The following command changes are introduced in this release.

Updates in `lltconfig`:

- A new option `lltconfig -l` is introduced. When you add a new link, you can use the `-l` option to specify that the link is a low priority link.

### Changes to I/O fencing

Symantec Cluster Server (VCS) includes the following changes to I/O fencing in 6.1:

#### Set the order of coordination points while configuring I/O fencing

You can use the `-fencing` option in the installer to set the order of coordination points.

Decide the order of coordination points (coordination disks or coordination point servers) in which they participate in a race during a network partition. The order of coordination points you set in the installer is updated to the `/etc/vxfenmode` file. I/O fencing approaches the coordination points based on the order listed in the `vxfenmode` file.

So, the order must be based on the possibility of I/O Fencing reaching a coordination point for membership arbitration.

For more information, refer to the *Symantec Cluster Server Installation Guide*.

## **Refresh keys or registrations on the existing coordination points using the install program**

You can use the `-fencing` option with the installer to refresh registrations on the existing coordination points.

Registration loss on the existing coordination points may happen because of an accidental array restart, corruption of keys, or some other reason. If the coordination points lose the registrations of the cluster nodes, the cluster may panic when a network partition occurs. You must refresh registrations on coordination points when the CoordPoint agent notifies VCS about the loss of registrations on any of the existing coordination points.

You can also perform a planned refresh of registrations on coordination points when the cluster is online without application downtime on the cluster.

For more information, refer to the *Symantec Cluster Server Installation Guide*.

## **CPI automatically installs a CP server-specific license while configuring CP server on a single-node VCS cluster**

The installer automatically installs a CP server-specific license if you are configuring CP server on a single-node VCS cluster. It also ensures that Veritas Operations Manager (VOM) identifies the license on a single-node coordination point server as a CP server-specific license and not as a VCS license.

For more information, see the *Symantec Cluster Server Installation Guide*.

## **Site-based preferred fencing policy**

The fencing driver gives preference to the node with higher site priority during the race for coordination points. VCS uses the site-level attribute Preference to determine the node weight.

For more information, see the *Symantec Cluster Server Administrator's Guide*.

## **Support for HTTPS communication between CP server and application client cluster nodes**

CP server and its application client cluster nodes can communicate securely over HTTPS, an industry standard protocol. Prior to release 6.1, communication between the CP server and its clients happened over the Inter Process Messaging (IPM) protocol, which is a Symantec proprietary protocol. Secure communication over IPM-based communication uses Symantec Product Authentication Services (AT) to establish secure communication between CP server and client nodes. With secure communication using HTTPS, CP server functionality is backward-compatible with previous releases. To support client nodes on releases before 6.1, CP server supports IPM-based communication in addition to HTTP-based communication. However, client nodes from 6.1 onwards only support HTTPS-based communication.

For more information, refer to the Symantec Cluster Server Installation Guide and Symantec Cluster Server Administrator's Guide.

### **The security attribute in `/etc/vxfenmode` file is obsolete**

From VCS 6.1, the Coordination Point (CP) client will communicate with CP server using HTTPS protocol. The 'security' parameter in `/etc/vxfenmode` is therefore deprecated and setting it to 1 or 0 has no effect whatsoever.

### **Rolling upgrade of an application cluster to release version 6.1 requires CP server running release version 6.1**

The application clusters and CP servers running on release version 6.1 communicate over the HTTPS protocol. Hence, an application cluster which is using CP server as a fencing coordination point can no longer access the pre-6.1 CP server after the cluster is upgraded to 6.1. To ensure a smooth upgrade, either application cluster must use CP servers running release version 6.1 or the CP servers running an earlier release version must be upgraded to 6.1. Note that CP server running release version 6.1 can still work with pre-6.1 application clusters.

### **Checks introduced in `vxfentsthdw` utility for disk size and option to override errors**

The `vxfentsthdw` utility is enhanced to check the disks for size compatibility and new error messages are introduced for better error evaluation. The utility also provides the override option (`-o`) to override size-related errors and continue testing.

### **New command for `hacli` in `vxfenswap` utility**

A new option `-p` is introduced to specify a protocol value that `vxfenswap` utility can use to communicate with other nodes in the cluster. The supported values for the protocol can be `ssh`, `rsh`, or `hacli`.

## Changes related to product name branding

Beginning with the 6.1 release, Storage Foundation and High Availability Solutions product names are rebranded.

[Table 1-3](#) lists the rebranded Storage Foundation and High Availability Solutions products.

**Table 1-3** Rebranded Storage Foundation and High Availability Solutions products

Old product name	New product names with Symantec branding
Veritas Storage Foundation	Symantec Storage Foundation (SF)
Veritas Dynamic Multi-Pathing	Symantec Dynamic Multi-Pathing (DMP)
Veritas Replicator Option	Symantec Replicator Option
Veritas Volume Replicator	Symantec Volume Replicator (VVR)
Veritas Storage Foundation Cluster File System HA	Symantec Storage Foundation Cluster File System HA (SFCFSHA)
Veritas Storage Foundation for Oracle RAC	Symantec Storage Foundation for Oracle RAC (SFRAC)
Veritas Storage Foundation HA	Symantec Storage Foundation HA (SFHA)
Veritas Cluster Server	Symantec Cluster Server (VCS)
Veritas Disaster Recovery Advisor	Symantec Disaster Recovery Advisor (DRA)
Veritas Storage Foundation and High Availability Solutions	Symantec Storage Foundation and High Availability Solutions (SFHAS)
Veritas High Availability Agent Pack	Symantec High Availability Agent Pack
Veritas File System Software Development Kit	Symantec File System Software Development Kit

Symantec rebranding does not apply to the following:

- Product acronyms
- Command names
- Error messages
- Alert messages
- Modules and components
- Feature names
- License key description
- Veritas Operations Manager product branding

## No longer supported

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

- The `fsppmk` command is deprecated and can no longer be used to create SmartTier placement policies.

## Symantec Storage Foundation for Databases (SFDB) tools features which are no longer supported

The following Storage Foundation for Databases (SFDB) tools features are not supported in this release:

- Storage Checkpoint policy and Storage Checkpoint quotas
- Interactive modes in clone and rollback

## System requirements

This section describes the system requirements for this release.

### Supported AIX operating systems

This section lists the supported operating systems for this release of Symantec products. For current updates, visit the Symantec Operations Readiness Tools Installation and Upgrade page: [https://sort.symantec.com/land/install\\_and\\_upgrade](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	Levels	Chipsets
AIX 7.1	TL0, TL1, or TL2	Power 5, Power 6, or Power 7
AIX 6.1	TL6, TL7, or TL8	Power 5, Power 6, or Power 7

AIX 6.1 TL6, AIX 6.1 TL7, AIX 7.1 TL0 and AIX 7.1 TL1 require an additional IBM APAR to be installed. Contact IBM to get the necessary APAR for your level.

## Storage Foundation for Databases features supported in database environments

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

**Table 1-5** 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
Quick I/O	Yes	Yes	Yes	Yes
Cached Quick I/O	Yes	Yes	Yes	Yes
Concurrent I/O	Yes	Yes	Yes	Yes
Storage Checkpoints	Yes	Yes	Yes	Yes
Flashsnap	Yes	Yes	Yes	Yes
SmartTier	Yes	Yes	Yes	Yes
Database Storage Checkpoints <b>Note:</b> Requires Enterprise license	Yes	Yes	Yes	No
Database Flashsnap <b>Note:</b> Requires Enterprise license	Yes	Yes	Yes	No
SmartTier for Oracle <b>Note:</b> 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.

## Number of nodes supported

SFHA supports cluster configurations with up to 64 nodes.

## AIX APARs required for Virtual Memory Management chunking

[Table 1-6](#) lists the AIX APARs that you must install to use the Virtual Memory Management (VMM) chunking feature, as well as the default value for the `thrgio_npages` and `thrgio_inval` APAR tunables.

**Table 1-6** AIX APARs required for Virtual Memory Management chunking

Operating System	Required APARs	Default APAR tunable value
AIX 6 TL6	IV19024	0
AIX 6 TL7 SP4	IV16839 IV18742	0 1024
AIX 6 TL8	IV16685 IV18846	0 1024
AIX 7 TL0	IV16521	0
AIX 7 TL1 SP4	IV16765 IV18778	0 1024
AIX 7 TL2	IV17138 IV19372	0 1024

You must set `dchunk_enable=1` to enable Veritas File System (VxFS) to utilize the VMM chunking feature rather than the VxFS internal chunking feature.

For information about setting the `dchunk_enable` tunable, see the `vxtunefs(1M)` manual page.

## Required attributes of LUNs for DMP devices

When the `reserve_policy=single_path` and `reserve_lock=yes`, the SCSI-2 Reserve may be placed on the device, which affects I/O load balancing and performance. To prevent the impact to load balancing and performance, set the `reserve_policy=no_reserve` and `reserve_lock=no` for the devices that are managed by DMP.

These settings are also required for a cluster set-up.

### Set the following attributes for LUNs

#### 1 Set the following attributes:

- If the path has the `reserve_policy` attribute set, change the `reserve_policy` attribute to `no_reserve` for all the paths.

```
# lsattr -El hdisk557 | grep res
reserve_policy single_path
Reserve Policy True

# chdev -l hdisk557 -a reserve_policy=no_reserve -P
hdisk557 changed
```

- If the path has the `reserve_lock` attribute set, change the `reserve_lock` attribute to `no`.

```
# lsattr -El hdisk558 | grep reserve_lock
reserve_lock yes
Reserve Device on open True

# chdev -l hdisk558 -a reserve_lock=no -P
hdisk558 changed
```

#### 2 Reboot the system for the changes to take effect.

## Fixed issues

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

## Installation and upgrades fixed issues

There are no install and upgrade fixed issues in this release.

## Symantec Storage Foundation and High Availability fixed issues

Issues fixed for Symantec Storage Foundation and High Availability (SFHA) includes issues fixed for Veritas File System and Veritas Volume Manager.

See [“Veritas File System fixed issues”](#) on page 30.

See [“Veritas Volume Manager fixed issues”](#) on page 35.

## Symantec Storage Foundation for Databases (SFDB) tools fixed issues

[Table 1-7](#) describes the Symantec Storage Foundation for Databases (SFDB) tools issues fixed in this release.

**Table 1-7** SFDB tools fixed issues

Incident	Description
2591463	Database Storage Checkpoint unmount may fail with device busy.
2534422	FlashSnap validate reports snapshot unsplittable.
2580318	dbed_vmclonedb ignores new clone SID value after cloning once.
2579929	User authentication fails.
2479901	FlashSnap resync fails if there is an existing space-optimized snapshot.
2869268	Checkpoint clone fails in a CFS environment if cloned using same checkpoint and same clone name on both nodes.
2849540	Very long off-host cloning times for large number of data files.
2715323	SFDB commands do not work with the ZHS16GBK character set.

## Veritas File System fixed issues

This section describes the incidents that are fixed in Veritas File System (VxFS) in this release.

**Table 1-8** Veritas File System fixed issues

Incident	Description
3331134	File system hangs due to a race condition when inodes are re-used from the delicache list.

**Table 1-8** Veritas File System fixed issues (*continued*)

Incident	Description
3331125	Enhancement to handle partial compressed extents during dedupe operation.
3331109	Additional checks in <code>fsck</code> to prevent file system metadata corruption with <code>filesnap</code> .
3331105	The <code>fsck</code> command does not validate if multiple reorg inodes point to the same source inode.
3331095	The <code>fsppadm</code> utility dumps core when an incorrect policy is specified during enforcement.
3331071	The <code>fsppadm</code> query and enforcement should honor the <code>-P</code> option to exclude private files.
3331045	The system panics in <code>vx_unlockmap</code> due to null pointer dereference.
3331010	File system full <code>fsck</code> fails as it erroneously accesses freed memory during RCT processing.
3310755	<code>fsck</code> fix to handle ZFOD extents while processing the <code>VX_RCQ_OP_DEC_ALL</code> operation.
3308673	A fragmented FS may get disabled when delayed allocations are enabled.
3298041	With the delayed allocation feature enabled on a locally mounted file system, observable performance degradation might be experienced when writing to a file and extending the file size.
3291635	The file system hangs when RCQ is full.
3265538	The system panics because VxFS calls the <code>lock_done</code> kernel service at <code>intpri=A</code> instead of <code>intpri=B</code> .
3261462	Mapbad corruption due to buffer overrun of <code>VX_TYPED_4</code> to <code>VX_TYPED_DEV8</code> conversion.
3253210	The file system hangs when it has reached the space limit.
3252983	During the test after having ported from 2486597, you see a dead loop situation where CPU is taken 100%, and the system barely responds.

**Table 1-8** Veritas File System fixed issues (*continued*)

Incident	Description
3249958	When /usr is mounted as a separate file system, the VxFS fails to load.
3233284	The <code>fsck (1M)</code> command hangs while checking Reference Count Table (RCT).
3228955	Some <code>fsck</code> enhancements to check that invalid extops are not present in older file system layouts.
3224101	After the optimization is enabled for updating the <code>i_size</code> across the cluster nodes lazily, the system panics.
3214816	With the DELICACHE feature enabled, frequent creation and deletion of the inodes of a user may result in corruption of the user quota file.
3194635	File system metadata corruption involving ZFOD extents and filesnap or compression.
3189562	Oracle daemons get hang with the <code>vx_growfile()</code> kernel function.
3164418	Data corruption happens due to the ZFOD split during ENOSPC conditions.
3153919	The <code>fsadm shrink</code> may hang, waiting for the hlock ownership while structural file set reorg is in progress.
3152313	With the Partitioned Directories feature enabled, removing a file may panic the system.
3150368	The <code>vx_writesuper()</code> function causes the system to panic in <code>evfsevol_strategy()</code> .
3142045	With Oracle 12c version, Veritas ODM library gives a version mismatch error.
3140990	Requirement for the ability to turn off VxFS's invalidation of pages for some Network File System (NFS) workloads.
3137886	Thin Provisioning Logging does not work for reclaim operations triggered via <code>fsadm</code> .
3101418	The current time returned by the operating system (Oracle error code ORA-01513) during Oracle startup is invalid.

**Table 1-8** Veritas File System fixed issues (*continued*)

Incident	Description
3096834	Intermittent <code>vx_disable</code> messages display in the system log.
3089314	AIX Workload partitions (WPARs) hang when you run the <code>pwdck</code> command.
3089211	When you add or remove CPUs, Veritas File System (VxFS) may crash with the Data Storage Interrupt (DSI) stack trace.
3069695	Default Access Control Lists (ACLs) are handled on named attributes.
3068902	In case of stale NFS mounts, the <code>statfs()</code> function calls on non-VxFS file systems may cause <code>df</code> commands to hang.
3066116	The system panics due to the NULL pointer dereference at the <code>vx_worklist_process()</code> function.
3042485	The fix to address file system metadata corruption involves named attribute directories.
3040944	The file system hangs due to a deadlock between the <code>dalloc</code> flusher thread and <code>dalloc</code> freeze under ENOSPC conditions.
3031360	The <code>vxfsconvert</code> command fails on a JFS filesystem with error message V-3-27051.
3029093	The <code>fsck</code> command fails to repair a file system with inconsistencies in RCT/RCQ records.
3022673	VxFS hangs when it changes the memory using Dynamic Logical Partitioning (DLPAR).
3011959	The system may panic because of the file system locking or unlocking using the <code>fsadm(1M)</code> or the <code>vxumount(1M)</code> command.
3003679	When you run the <code>fsppadm(1M)</code> command and remove a file with the named stream attributes ( <code>nattr</code> ) at the same time, the file system does not respond.
2999493	The file system check validation fails after a successful full <code>fsck</code> during the internal testing with the following message: <code>run_fsck : First full fsck pass failed, exiting.</code>

**Table 1-8** Veritas File System fixed issues (*continued*)

Incident	Description
2983248	The <code>vxrepquota(1M)</code> command dumps core.
2977697	A core dump is generated while the clone is being removed.
2966277	The high file system activities like read, write, open and lookup may panic the system.
2926684	In rare cases, the system may panic while performing a logged write.
2924447	Full <code>fsck</code> performance needs to be improved to reduce the amount of disk I/O.
2923105	Removal of the VxFS module from the kernel takes a longer time.
2916691	The <code>fsdedup</code> command hangs with an infinite loop in <code>vx_dedup_extents</code> .
2908391	It takes a long time to remove checkpoints from the VxFS file system, when there are a large number of files present.
2906018	The <code>vx_iread</code> errors are displayed after successful log replay and mount of the file system.
2905820	If the file is being read via the NFSv4 client, then removing the same file on the NFSv4 server may hang if the file system is VxFS.
2887423	Spin-lock contention on <code>vx_sched_lk</code> can result in slow I/O.
2885592	The <code>vxdump</code> operation is aborted on file systems which are compressed using the <code>vxcompress</code> command.
2881211	File ACLs are not preserved in checkpoints properly if the file has a hardlink.
2878164	VxFS consumes too much pinned heap.
2864471	The file system hangs during clone removal with Partition directory turned on.
2858683	For files greater than 8192 bytes, the <code>reserve-extent</code> attribute is changed after you run the command <code>vxrestore</code> .

**Table 1-8** Veritas File System fixed issues (*continued*)

Incident	Description
2857568	Performance issues occur during backup operations reading larges files sequentially.
2848948	VxFS buff cache consumption increased significantly after running over 248 days.
2841059	The file system is marked for a full <code>fsck</code> operation and the attribute inode is marked as <code>bad ondisk</code> .
2839871	On a system with DELICACHE enabled, several file system operations may hang.
2825125	VxFS does not support for sub-directories larger than 64K.
2781552	Mount detects the file system not being clean and hence sets the <code>fullfsck</code> flag. <code>fsck</code> is not able to clean the system.
2750860	Performance of the write operation with small request size may degrade on a large file system.
2720034	The <code>vxfsckd</code> daemon does not restart after being manually killed.
2667658	The <code>fsddsconv_endian</code> conversion operation fails because of a macro overflow.
2624262	System panics while executing dedup operation.
2444146	The Oracle Disk Manager read returns EINTR while running unspecified Oracle jobs.
2417858	VxFS quotas do not support 64 bit limits.

## Veritas Volume Manager fixed issues

This section describes the incidents that are fixed in Veritas Volume Manager (VxVM) in this release. This list includes Volume Replicator and Cluster Volume Manager (CVM) fixed issues.

**Table 1-9** Veritas Volume Manager fixed issues

Incident	Description
2787713	CVM fails to start if the first node joining the cluster has no connectivity to the storage.

**Table 1-9** Veritas Volume Manager fixed issues (*continued*)

Incident	Description
2866299	The vxrecover command does not automatically recover layered volumes in an RVG
3325371	When using snapshots, there is a panic in <code>vol_multistepsio_read_source</code> .
3312162	VVR:DV: Verification of the remote volumes found differences with <code>vradmin verifydata</code> .
3331765	Failed to create a create boot image while restoring <code>mksysb</code> on a disk with multiple paths with <code>AIX61TL8SP3</code> because AIX did not save the <code>reserve_policy</code> attribute.
3283525	Data Change Object (DCO) corruption after volume resize leads to <code>vxconfigd</code> hang.
3271595	VxVM should not allow turning off disk reclaim flag when there are pending reclaims on the disk.
3263095	The following error message is seen on the console, even with a non-MPIO disk while enabling the DMP path:  <code>VxVM vxdmp V-5-3-0 dmp_indirect_ioctl: Ioctl Failed for 19/0x49 with error 22</code>
3261601	<code>dmp_destroy_dmpnode</code> trying to free an already freed address.
3254311	The system panics when reattaching the site to a site-consistent disk group having a volume larger than 1 TB.
3249264	Disks get into the <code>ERROR</code> state after being destroyed with the command <code>vx dg destroy dg-name</code> .
3240858	The <code>/etc/vx/vxesd/.udev_lock</code> file may have different permissions at different instances.
3237503	System hang may happen after creating space-optimized snapshot with large size cache volume.
3236773	Multiple error messages of format <code>vxdmp V-5-3-0 dmp_indirect_ioctl: Ioctl Failed</code> can be seen during <code>set/get failover-mode</code> for EMC ALUA disk array.
3235350	System panic by <code>vxiod</code> process.

**Table 1-9** Veritas Volume Manager fixed issues (*continued*)

Incident	Description
3218013	Dynamic Reconfiguration (DR) Tool does not delete stale OS (operating system) device handles.
3205490	OS hangs at bootup when the boot LUN is shared across multiple nodes.
3199398	Output of the command <code>vxdmpadm pgrereg</code> depends on the order of DMP node list where the terminal output depends on the last LUN (DMP node).
3199056	Veritas Volume Replicator (VVR) primary system panics in the <code>vol_cmn_err</code> function due to the VVR corrupted queue.
3194358	Continuous I/O error messages on OS device and DMP node can be seen in the syslog associated with the EMC Symmetrix not-ready (NR) LUNs.
3188154	<code>vxconfigd</code> is down after enabling native support on and reboot.
3185199	Failed to restore <code>mksysb</code> when the target disk has multiple paths.
3182350	If there are more than 8192 paths in the system, the <code>vxassist(1M)</code> command hangs when you create a new VxVM volume or increase the existing volume's size.
3182175	The <code>vxdisk -o thin,fssize list</code> command can report incorrect file system usage data.
3178029	The value of "different blocks" is more than 100% while syncing the <code>rvg</code> .
3162418	The <code>vxconfigd(1M)</code> command dumps core due to an incorrect check in the <code>ddl_find_cdevno()</code> function.
3146715	Rlinks do not connect with Network Address Translation (NAT) configurations on Little Endian Architecture.
3130379	The <code>vxplex</code> command core dumped under random memory allocation failures.
3126204	[VVR] : machine panics when SRL is full.
3125631	With latest train snapshot fails for <code>dbdset</code> setup with error <code>vxsnap ERROR V-5-1-6433 Component volume has changed</code> .
3114134	Smart(sync) Autosync fails to work and instead replicates the entire volume size for larger sized volumes.
3111062	Make the <code>vxrsync</code> socket connection mechanism more robust.
3107741	<code>vxrvg snapdestroy</code> fails with a <code>Transaction aborted waiting for io drain error</code> and <code>vxconfigd</code> hangs for about 45 minutes.

**Table 1-9** Veritas Volume Manager fixed issues (*continued*)

Incident	Description
3090667	System panics/hangs while executing <code>vxdisk -o thin,fssize list</code> as part of VOM SF discovery.
3086627	The VxVM <code>vxdisk ERROR V-5-1-16282 Cannot retrieve stats: Bad address</code> error message displays while using <code>vxdisk -o thin,fssize list</code> for hitachi_osp-vm0 enclosure on the array configured for truecopy P-VOLs.
3076093	The patch upgrade script <code>installrp</code> can panic the system while doing a patch upgrade.
3063378	Some VxVM commands run slowly when EMC PowerPath presents and manages "read only" devices such as EMC SRDF-WD or BCV-NR.
3041014	Beautify error messages which are seen on the execution of <code>relayout</code> command.
3020015	With the OS naming scheme, the procedure of putting root disk under DMP control does not work properly.
3012929	<code>vxconfigbackup</code> keeps old disk names in its files and gives errors, when disk names are changed.
3011405	The <code>vxtune -o export</code> command failed with V-5-1-8826 (EXDEV).
3010191	Previously excluded paths are not excluded after upgrade to VxVM 5.1SP1RP3.
3002770	While issuing a SCSI inquiry command, NULL pointer dereference in DMP causes system panic.
2994976	BAD TRAP panic in <code>vxio:vol_mv_pldet_callback</code> .
2992667	When new disks are added to the SAN framework of the Virtual Intelligent System (VIS) appliance and the Fibre Channel (FC) switcher is changed to the direct connection, the <code>vxdisk list</code> command does not show the newly added disks even after the <code>vxdisk scandisks</code> command is executed.
2979824	The <code>vxdiskadm(1M)</code> utility bug results in the exclusion of the unintended paths.
2970368	Enhance handling of SRDF-R2 Write-Disabled devices in DMP.
2969844	The device discovery failure should not cause the DMP database to be destroyed completely.

**Table 1-9** Veritas Volume Manager fixed issues (*continued*)

Incident	Description
2959733	Handling the device path reconfiguration in case the device paths are moved across LUNs or enclosures to prevent the <code>vxconfigd(1M)</code> daemon core dump.
2959325	The <code>vxconfigd(1M)</code> daemon dumps core while performing the disk group move operation.
2948172	Executing the <code>vxdisk -o thin, fssize list</code> command can result in panic.
2946440	Add back the support for "INF" for LSI and ENGENIO VIDs to the LSI ASL.
2940446	A full file system check (fsck) hangs on I/O in Veritas Volume Manager (VxVM) when the cache object size is very large.
2925893	Make changes to Huawei APM to skip re-registering the keys on Secondary during failover.
2919714	On a thin Logical Unit Number (LUN), the <code>vxevac(1M)</code> command returns 0 without migrating the unmounted-VxFS volumes.
2915836	<code>vxnotify</code> does not report volume enabled message.
2911040	The restore operation from a cascaded snapshot leaves the volume in unusable state if any cascaded snapshot is in the detached state.
2899173	The <code>vxconfigd(1M)</code> daemon hangs after executing the <code>vradmind stopprep</code> command.
2898547	The <code>vradmind</code> process dumps core on the Veritas Volume Replicator (VVR) secondary site in a Clustered Volume Replicator (CVR) environment, when Logowner Service Group on VVR Primary Site is shuffled across its CVM (Clustered Volume Manager) nodes
2898324	UMR errors reported by Purify tool in <code>vradmind migrate</code> command.
2884225	The <code>vxconvert</code> command fails to convert 1.5TB AIX LVM volume group to VxVM disk group
2884122	VIOS:unwanted event messages seen on console.
2882908	Machine failed to bootup with error "PreP-BOOT : Unable to load full PreP image".
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.

**Table 1-9** Veritas Volume Manager fixed issues (*continued*)

Incident	Description
2880981	Thin Reclamation of EMC Symmetrix array with Microcode 5876 could fail with error EIO.
2878876	The <code>vxconfigd</code> daemon dumps core in <code>vol_cbr_dolog()</code> due to race between two threads processing requests from the same client.
2876706	VxVM commands hang when a LUN is changed to <code>not_ready</code> state from the array.
2869514	Issue with a configuration with large number of disks when the joining node is missing disks.
2866299	The <code>vxrecover</code> command does not automatically recover layered volumes in an RVG.
2859470	The Symmetrix Remote Data Facility R2 (SRDF-R2) with the Extensible Firmware Interface (EFI) label is not recognized by Veritas Volume Manager (VxVM) and goes in an error state
2857044	System crashes while resizing a volume with Data Change Object (DCO) version 30.
2851403	System panics while unloading <code>vxio</code> module when SmartMove feature is used and the <code>vxportal</code> module is reloaded (for example, during VxFS fileset upgrade).
2815517	The <code>vxdbg adddisk</code> command allows mixing of clone and non-clone disks in a disk group.
2779580	The <code>vradmin repstatus</code> operation may display a configuration error after cluster reconfiguration in a CVR environment.
2762147	I/O hangs on the primary node when running the <code>vxrvvg snapstore</code> operation.
2753954	At cable disconnect on port1 of dual-port FC HBA, paths via port2 marked SUSPECT.
2751423	<code>vxconfigd</code> core dumps in <code>ddl_migration_devlist_removed</code> during execution of internal testing.
2737686	The <code>vxddladm list [devices hbas ports targets]</code> command shows invalid output in some platforms and in some platforms the output fields are empty.
2715124	The <code>vxrecover</code> command does not handle RAID 5 volumes correctly.

**Table 1-9** Veritas Volume Manager fixed issues (*continued*)

Incident	Description
2643506	<code>vxconfigd</code> core dumps when different LUNs of same enclosure are configured with different array modes.
2567618	The VRTSexplorer dumps core in <code>vxcheckhbaapi/print_target_map_entry</code> .
2510928	The extended attributes reported by <code>vxdisk -e list</code> for the EMC SRDF luns are reported as <code>tdev mirror</code> , instead of <code>tdev srdf-r1</code> .
2398954	The system panics while performing I/O on a VxFS mounted instant snapshot with the Oracle Disk Manager (ODM) SmartSync enabled.
2366066	The VxVM (Veritas Volume Manager) <code>vxstat</code> command displays absurd statistics for READ & WRITE operations on VxVM objects.
2354560	The <code>vx dg listclone</code> command output may not list all the disks with <code>clone_disk</code> or <code>udid_mismatch</code> flag set
2152830	In a multilevel clone disks environment, a regular disk group import should be handled properly. In the case of a disk group import failure, it should report the correct error message.
2149922	Importing a disk group using clone disks fails with a "wrong usage" or "invalid attribute" error.
2000585	<code>vxrecover</code> does not start remaining volumes if one of the volumes is removed during <code>vxrecover</code> command run.
1973983	The <code>vxunreloc(1M)</code> command fails when the Data Change Object (DCO) plex is in DISABLED state.
1953257	Panic in <code>voldiodone</code> , because a disk with hung IO is moved out of the disk group.
1952197	Running <code>vxtrace</code> against a volume shows response times as negative.
1942051	I/O hangs on master node after disabling secondary paths from slave node and rebooting slave node.
1903700	Removing mirror using <code>vxassist</code> does not work.
1902483	Unique PGR key per group is not needed.
1765916	VxVM socket files do not have proper write protection.
1289985	<code>vxconfigd</code> core dumps upon running the <code>vx dctl enable</code> command.

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

Table 1-10 lists the fixed issues for LLT, GAB, and I/O fencing.

**Table 1-10** LLT, GAB, and I/O fencing fixed issues

Incident	Description
2619600	After you execute Live Partition Mobility (LPM) on an SFHA or SFCFSHA node with SCSI-3 fencing enabled for data disks, I/O fails on devices or disks with reservation conflict.
2869763	When you run the <code>addnode -responsefile</code> command, if the cluster is using LLT over UDP, then the <code>/etc/llttab</code> file generated on new nodes is not correct. So, the procedure fails and you cannot add nodes to a cluster using CPI response files.
2991093	The preferred fencing node weight does not get reset to the default value when HAD is terminated. In spite of lack of high availability on that node, fencing may give preference to that node in a network partition scenario.
2995937	The default value of preferred fencing node weight that <code>vxfen</code> uses is 1 (one). However, when HAD starts without any service group or if HAD is stopped or terminated, the node weight is reset to 0 (zero). Since <code>vxfen</code> resets the preferred fencing weight to its default value when HAD gets terminated, stopping HAD and killing HAD shows different preferred fencing weight.
2802682	Server-based fencing may fail to start if you use the existing configuration files after reinstalling the stack.
2858190	If <code>VRTSvxfen</code> fileset is not installed on the system, then certain script files that are needed for the <code>vxfsthdw</code> utility to function are not available. So, without the <code>VRTSvxfen</code> fileset installed on the system you cannot run the utility from the install media.
3101262	GAB queue is overloaded causing memory pressure during I/O shipping.
3218714	GAB does not log messages about changing tunable values.
2858076	Changing the module parameter <code>gab_conn_wait</code> had no effect.

## Known issues

This section covers the known issues in this release.

### Installation known issues

This section describes the known issues during installation and upgrade.

## Stopping the installer during an upgrade and then resuming the upgrade might freeze the service groups [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:

```
# hagrps -list Frozen=1
```

- 2 Unfreeze all the frozen service groups:

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

## 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) 6.1, if you unmount all VxFS file systems including the one that hosts the NetBackup binaries (`/usr/opensv`), then while upgrading to SF 6.1, the installer fails to check if NetBackup is installed on the same machine and uninstalls the shared infrastructure filesets `VRTSspbx`, `VRTSat`, and `VRTSicisco`. This causes NetBackup to stop working.

**Workaround:** Before you unmount the VxFS file system that hosts NetBackup, copy the `/usr/opensv/netbackup/bin/version` file and `/usr/opensv/netbackup/version` file to the `/tmp` directory. If you have clustered NetBackup installed, you must also copy the `/usr/opensv/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/opensv/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/opensv/netbackup/bin  
# mkdir -p /usr/opensv/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 `VRTSicisco` filesets after the upgrade process completes.

## The VRTSvxvm fileset fails to install on a few cluster nodes because the template file is corrupted (2348780)

The installer debug log displays the failure of the `errupdate` command as following:  
`errupdate -f /usr/lpp/VRTSvxvm/inst_root/VRTSvxvm.err`. The `errupdate` command gets invoked through `/usr/lib/install/install` by the operating system. The command also fails for the `VRTSvxfs`, `VRTSglm`, and `VRTSgms` filesets.

The `errupdate` command generally creates a `*.undo.err` file to remove entries from the Error Record Template Repository in case of failed installation or cleanup. However, in this case the `*.undo.err` file does not get generated as the `errupdate` command fails. Also, it is not possible to manually remove entries from the Error Record Template Repository in order to undo the changes made by the failed installation, because the file is corrupted.

**Workaround:** Save a copy of the `/var/adm/ras/errtmpl` and `/etc/trcfmt` files before you install the product. Replace `/var/adm/ras/errtmpl` and `/etc/trcfmt` files with the ones that you saved, when the installation fails because the template file is corrupted. Uninstall all the filesets you installed and reinstall.

## After a locale change, you need to restart the vxconfig daemon (2417547)

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, "vxconfig daemon recovery."

## Web installer does not ask for authentication after the first session if the browser is still open (2509330)

If you install or configure SFHA 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.

## Erroneous resstatechange trigger warning [2277819]

You may encounter the following warning when you restart resources:

```
CPI WARNING V-9-40-4317 The installer has detected that resstatechange trigger is configured by setting TriggerResStateChange attributes.
```

**Workaround:** In future releases, the resstatechange trigger will not be invoked when a resource is restarted. Instead, the resrestart trigger will be invoked if you set the TriggerResRestart attribute. The resrestart trigger is available in the current release. Refer to the VCS documentation for details.

## The VRTSsfcp<oldversion> fileset is retained after you upgrade to 6.1 on an alternate disk (2811749)

On AIX, if you run the command `alt_disk_scenario` to perform a disk clone and upgrade from 6.0 or later to 6.1, the older version of the VRTSsfcp fileset is retained.

**Workaround:** Optionally uninstall the older VRTSsfcp<oldversion> fileset after upgrading. Retaining the older version will not cause any harm.

## If you have a non-shared (detached) WPAR configured, when you install, upgrade, or install any Symantec product, the filesets in the WPAR cannot be installed, upgraded, or uninstalled correspondingly (3313690)

On AIX, if you have a non-shared (detached) workload partition (WPAR) configured, when you perform an install, upgrade, or uninstall task on any Symantec product by the Symantec product installer, the filesets cannot be installed, upgraded, or uninstalled inside the WPAR correspondingly.

**Workaround:** There is no workaround for this issue.

## **If you have a shared (system) WPAR configured, when you install, upgrade, or uninstall any Symantec product, the filesets in the WPAR are not synchronized correspondingly (3313690)**

On AIX, if you have a shared (system) workload partition (WPAR) configured, when you perform an install, upgrade, or uninstall task on any Symantec product by the Symantec product installer, the filesets may not be installed, upgraded, or uninstalled correspondingly.

**Workaround:** After an install, upgrade, or uninstall task, execute the following command to synchronize your WPAR with global systems:

```
# /usr/sbin/syncwpar -A
```

## **Rolling upgrade may encounter a problem if open volumes from different disk groups have the same name (3326196)**

When you perform a rolling upgrade, the installer may block the rolling upgrade even if all the open volumes are under VCS control. This may occur if there are volumes with the same name under different disk groups although they are not mounted.

**Workaround:** Avoid creating volumes from different disk groups with the same name. If they already exist, unmount all the VxFS mount points. After the upgrade is finished, remount the volumes.

## **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 `vxcpse` 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.

## **If you select rolling upgrade task from the Install Bundles menu, the CPI exits with an error (3442070)**

If you try to perform rolling upgrade using Install Bundles and select the rolling upgrade task from the Install Bundle menu, the CPI exits with an error.

**Workaround:** Run the installer with `-rolling_upgrade` option instead of choosing the task from the menu.

```
# ./installer -hotfix_path /path/to/hotfix -rolling_upgrade
```

## LLT known issues

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

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

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

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

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

```
# lsattr -El SEA
```

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

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

### The node may panic after you stop the LLT service and LLT unload is in progress [3333290]

LLT uses the `xmfree()` function of the AIX operating system to free network messages. This function takes a heap as an argument. The heap is created before allocating memory in AIX. In rare cases, during LLT unload, it may happen that LLT destroys this heap while LLT frees messages using the `xmfree()` function. This issue causes LLT to panic the node.

No workaround. You can restart the node and resume normal operations.

## 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 deinitd 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.

## I/O fencing known issues

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

### CP server repetitively logs unavailable IP addresses (2530864)

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

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

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

See the *Symantec Storage Foundation and High Availability 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.

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

When you configure fencing in customized mode and do not 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 `vxcpsserv` 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.

## 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 fileset is not removed from the system, the `cpsadm` command loads the old security libraries present on the system. As the installer runs the `cpsadm` command on the CP server to add or upgrade the SFHA cluster (application cluster), the installer also fails.

**Workaround:** To resolve this issue, perform the following procedure on all of the nodes of the CP server:

- 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
```

## 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.

## 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.

## 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 coordinator disk group

**Workaround:** There is no workaround for this issue.

## 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 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 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*.

## Fencing configuration fails if SysDownPolicy is set to AutoDisableNoOffline in online service groups [3335137]

If SysDownPolicy of one or more online service groups is configured to AutoDisableNoOffline, fencing configurations such as server-based, disk-based and disable mode fail. Since the service groups is configured with `SysDownPolicy = { AutoDisableNoOffline }`, stopping VCS fails which leads to the failure of fencing configuration.

**Workaround:** When configuring fencing and before stopping VCS, you must offline the service groups configured with `SysDownPolicy = { AutoDisableNoOffline }` manually.

## 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*.

## The `vxfsentsthdw` utility may not run on systems installed with partial SFHA stack [3333914]

The `vxfsentsthdw` 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 VRTSvxfen package, then run the utility from either the install media or from the `/opt/VRTSvcs/vxfsentsthdw/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, `vxfsd`, 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.

## Symantec Storage Foundation and High Availability known issues

This section describes the known issues in this release of Symantec Storage Foundation and High Availability (SFHA).

### 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.

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

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

Running AIX 6.1, you may receive the following error message when using sqlplus:

```
$ sqlplus " / as sysdba"
SQL> startup nomount
SQL> ORA 0-0-0-0
```

**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 environment, but it has not been tested or released yet.

## Not all the objects are visible in the VOM GUI (1791063, 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 Departed 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 [1922388, 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/racl1g1/.DB_NAME
(No such file or directory).
SFORA vxreptadm ERROR V-81-8847 Cannot get filename from sid
for 'racl1g1', rc=-1.
SFORA vxreptadm ERROR V-81-6550 Could not connect to repository
database.
VxVM vxdg ERROR V-5-1-582 Disk group SNAP_racl1dg1: No such disk
group SFORA
vxsnapadm ERROR V-81-5623 Could not get CVM information for
SNAP_racl1dg1.
SFORA dbed_vmclonedb ERROR V-81-5578 Import SNAP_racl1dg1 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.

**DB2 databases are not visible from the VOM Web console (1850100)**

If you upgraded to SF 5.1, DB2 databases will be not visible from the VOM web console.

This will be fixed in the SF 5.1 Patch 1 release.

**Workaround:** Reinstall is required for VOM DB2-Hotfix (HF020008500-06.sfa), if the host is upgraded to SF 5.1. Use the deployment framework and reinstall the hotfix for DB2 (HF020008500-06.sfa) on the managed host.

**To resolve this issue**

- 1 In the Web GUI, go to **Settings > Deployment**.
- 2 Select **HF020008500-06 hotfix**.
- 3 Click **Install**.
- 4 Check the **force** option while reinstalling the hotfix.

**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.

**Upgrading operating system Technology Levels along with Storage Foundation using an alternate disk fails (2162945)**

Upgrading the operating system Technology Levels (TL) along with Storage Foundation using an alternate disk fails occasionally with the following error:

```
alt_disk_copy: 0505-224 ATTENTION:
An error occurred during installation of
one or more software components.
Modifying ODM on cloned disk.
Building boot image on cloned disk.
forced unmount of /alt_inst/var/adm/ras/platform
forced unmount of /alt_inst/var
umount: error unmounting /dev/alt_hd2: Device busy
0505-144 alt_disk_install: Unable to unmount alt_inst filesystems.
```

No issues have been observed with Storage Foundation in the cause of the failure.

**CP server service group fails to come online with the default database path after the CP server is upgraded from 6.0 to 6.1 on a multi-node cluster [3326639]**

If the CP server is configured on a multi-node cluster before the upgrade with security enabled, you must reconfigure the CP server after the CP server upgrade.

If you reuse the old credentials with the old database path, the CP server service group does not come online. Since the default database paths of CP server in 6.0 and 6.1 are different, reusing the old credentials and default database path prevents the CP server service group from coming online.

**Workaround:**

If the CP server multi-node cluster is configured with security enabled and if the old credentials such as database path are expected to be reused in reconfiguration of the CP server after the upgrade of the CP server, use the same database path before and after the upgrade.

## Veritas Volume Manager known issues

The following are the Veritas Volume Manager known issues for this release.

### **DMP does not support disks from SEAGATE which do not give unique NAA IDs (3343009)**

DMP does not support disks from SEAGATE which do not give unique NAA IDs.

**Workaround:**

There is no workaround for this issue.

### **Creating a disk group with a large number of objects or splitting, joining, or moving such a disk group reports an out of kernel memory error (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.

### **For HP 3PAR array with firmware 3.1.2, all subpaths are not enabled after the reboot of the array controller (3049401)**

This issue occurs on the AIX platform with the HP 3PAR array with firmware 3.1.2. After an array controller is rebooted, some of the paths through that controller remain in disabled state even after the controller is up.

#### **Workaround:**

After the controller is rebooted, use the following command to enable all of the paths:

```
# vxdisk scandisks
```

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

This issue occurs on A/P arrays. If the voting disk loses connectivity 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 than 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
```

### **Cascaded failure of nodes with ioship enabled may cause the vxconfigd daemon to hang (2865771)**

In a shared disk group environment with `ioship` enabled, the `vxconfigd` daemon may hang in certain cases. When the I/O is initiated from the slave node that has lost connectivity to the disks locally, the I/O is shipped to other nodes. If the node processing the shipped I/O also leaves the cluster shortly after the first node, and tries to rejoin the cluster as a slave, the cascaded failures may cause the `vxconfigd` daemon to hang.

## 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 multiple enclosures. The rebalancing process takes time, during which time the `vxconfigd` daemon is busy and does not respond to commands.

## The `vxconvert` utility fails if PowerPath disks are formatted as simple disks (857504)

If a PowerPath disk is formatted as a simple disk (a foreign device), then the `vxconvert` utility may fail during conversion of LVM to VxVM. To view the format of the disk, use the `vxdisk list` command. This issue may also occur if the `/etc/vx/darecs` file contains an `hdiskpower` disk entry. This entry may be present if PowerPath disks were configured as foreign disks in Storage Foundation 4.0, and the entry was not changed after subsequent upgrades.

## 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
```

## Co-existence check might fail for CDS disks

In Veritas Volume Manager (VxVM) 5.1 SP1, VxVM introduces the ability to support Cross-platform Data Sharing (CDS) on disks larger than 1TB. VxVM uses the Solaris VTOC Table to initialize the cdsdisk layout on devices up to 1TB. VxVM uses the GUID Partition Table (GPT) to initialize the cdsdisk layout on devices larger than 1TB.

In layouts where Solaris VTOC Table is used for initialization (typically, when the disk size has never exceeded 1TB), the AIX co-existence label can be found at sector 7 and the VxVM ID block (also known as HP co-existence label) can be found at sector 16.

In layouts where GPT is used for initialization (typically, when the disk size is currently greater than or had earlier exceeded 1TB), the AIX co-existence label is placed at sector 55 and VxVM ID block (also known as HP co-existence label) is placed at sector 64. Consequently, AIX utilities would not be able to recognize a cdsdisk initialized using GPT to be a valid VxVM disk. Symantec is working with IBM and third party OEMs to enhance the co-existence check in these utilities.

**Workaround:** There is no workaround for this issue.

## I/O fails on some paths after array connectivity is restored, due to high restore daemon interval (2091619)

If a path loses connectivity to the array, the path is marked as suspected to fail and hence is not used for I/O. After the connectivity is restored, the restore daemon detects that the path is restored when the restore daemon probes the paths. The restore daemon makes the path available for I/O. The restore daemon probes the paths at the interval set with the tunable parameter `dmp_restore_interval`. If you set the `dmp_restore_interval` parameter to a high value, the paths are not available for I/O until the next interval.

## vxconfigd hang with path removal operation while IO is in-progress (1932829)

In AIX with HBA firmware version SF240\_320, `vxdisk scandisks` (device discovery) takes a long time when a path is disabled from the switch or from the array.

**Workaround:**

To resolve this issue, upgrade the HBA firmware version to SF240\_382.

## 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.

### Work-arounds:

Use one of the following work-arounds:

- 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.

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

During online migration from LVM to VxVM volumes, if there is a system reboot when the migration setup is in partial state, that is, the start operation has not

completed successfully, then the recover and abort operations might not be able to recover and rollback the configuration.

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

## Issues 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.

### Workaround:

#### To work around this issue

- 1 Restore storage connectivity.
- 2 Deport the disk group.
- 3 Import the disk group.

## 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:

```
# vxddmpadm setattr enclosure enc11 recoveryoption=throttle \  
iotimeout=600
```

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

```
# vxddctl enable
```

## Upgrading from Symantec Storage Foundation and High Availability 5.x to 6.1 may fail for IBM XIV Series arrays (2715119)

Starting in the Symantec Storage Foundation and High Availability 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 from a release prior to that release to the current 6.1 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`.

## Upgrading SFHA to version 6.1 marks vSCSI disks as cloned disks (2434444)

This issue is seen when you upgrade from a pre-51SP1 version of SFHA which has vSCSI disks included in a disk group. After upgrading SFHA to 6.1, the vSCSI disks that were included in a disk group are marked as cloned disks.

### Workaround:

Use the following procedure to clear the clone disk flag:

#### To clear the clone disk flag:

- 1 Remove the vSCSI devices that are in error state (`ibm_vscsi#_#`) using the following command:

```
# vxdisk rm device_name
```

- 2 Deport the disk group.

```
# vxdg deport dg_name
```

- 3 Re-import the disk group with a new udid.

```
# vxdg -o updateid import dg_name
```

- 4 Display the devices that are part of the disk group.

```
# vxdisk -g dg_name list
```

- 5 Clear the clone\_disk tag from these devices.

```
# vxdisk set device_name clone=off
```

### **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
```

### **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.

## **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.

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

In an environment 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.

## **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.

## **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 dname
```

### **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.

**Disk group deport operation reports messages in the syslog for remote disks (3283518)**

During the **vx dg deport** operation, the following messages may be seen in the syslog for remote disks:

```
Aug 12 14:51:57 swlx87 vxvm:vxconfigd: V-5-1-12708 vold_pgr_unregister(): failed to get key (Error 9).
```

**Workaround:**

These messages can be ignored for all the remote disks.

**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 `vx disk scandisks` or `vx dctl 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 `vx disk scandisks` command again. This cycle causes continuous I/O error messages. This problem can also other commands to run slowly because the VxVM configuration daemon (`vxconfigd`) is busy servicing `vx disk scandisks`.

**Workaround: Stop the vxattachd script and:**

- 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:

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

## LUNs from any EMC CLARiiON arrays that have Not Ready state are shown in "online invalid" state by Veritas Volume Manager (VxVM) (3287940)

LUNs from any EMC CLARiiON arrays that have Not Ready state are shown in "online invalid" state by Veritas Volume Manager (VxVM). They should be shown in "error" state. The EMC CLARiiON arrays do not have a mechanism to communicate the NR (Not Ready) state of the LUNs, so VxVM cannot recognize it. However, the read operation on these LUNs fails and due to defect in disk online operation this read failure is ignored causing disk online to succeed. Thus, these LUNs are shown as "online invalid".

### Workaround:

There is no workaround.

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

The Veritas Volume Manager (VxVM) 6.1 includes several array names that differ from the array names in releases 5.1SP1 or prior. Therefore, if you upgrade to VxVM 6.1 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 6.1. Manually reconfigure the enclosure attributes to resolve the issue.

[Table 1-11](#) shows the Hitachi arrays that have new array names.

**Table 1-11** Hitachi arrays with new array names

Previous name	New name
TagmaStore-USP	Hitachi_USP
TagmaStore-NSC	Hitachi_NSC
TagmaStoreUSPV	Hitachi_USP-V

**Table 1-11** Hitachi arrays with new array names (*continued*)

Previous name	New name
TagmaStoreUSPVM	Hitachi_USP-VM
<New Addition>	Hitachi_R700
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 6.1. 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

### **MPIO device names shown in error state (3169587)**

In this release, DMP does not support extended attributes like AVID for AIX MPIO devices. In the 5.1SP1 release, DMP used to support AVID for the MPIO devices. When you upgrade from 5.1SP1 or prior release to a release 6.0 or later, DMP assigns new names to the MPIO devices.

The MPIO device may go into an error state after the upgrade, if a persistent disk access record (entry in `/etc/vx/darecs`) exists with the old name, and the device was assigned a new name.

The same issue may occur if the MPIO device name changes for another reason, such as the changed cabinet serial numbers for 3PAR or XIV devices.

#### **Workaround:**

Use the following procedure to remove the persistent disk access record and resolve the issue.

**To resolve the issue with MPIIO devices in error state**

- 1 Remove the following file:

```
# rm /etc/vx/darecs
```

- 2 Reset the `vxconfigd` daemon:

```
# vxconfigd -kr reset
```

## Veritas File System known issues

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

### Cannot use some commands from inside an automounted Storage Checkpoint (2490709)

If your current work directory is inside an automounted Storage Checkpoint, for example `/mnt1/.checkpoint/clone1`, some commands display the following error:

```
can't find current directory
```

This issue is verified with the following commands:

- `cp -r`
- `du`

However, this issue might occur with other commands.

**Workaround:** Run the command from a different directory.

### Enabling delayed allocation on a small file system sometimes disables the file system (2389318)

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

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

**Workaround:** Use the `vxtune fs` command to turn off delayed allocation for the file system.

## Delayed allocation sometimes gets turned off automatically when one of the volumes in a multi-volume file system nears 100% usage even if other volumes have free space (2438368)

Delayed allocation sometimes gets turned off automatically when one of the volumes in a multi-volume file system is nearing 100% usage even if other volumes in the file system have free space.

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

## Deduplication can fail with error 110 (2591473)

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.

## Unable to unmount the NFS exported file system on the server if you run the fsmigadm command on the client (2355258)

Unmounting the NFS-exported file system on the server fails with the "Device busy" error when you use the `fsmigadm` command on the NFS client.

**Workaround:** Unexport the file system prior to unmounting.

## vxresize fails while shrinking a file system with the "blocks are currently in use" error (2437138)

The `vxresize` shrink operation may fail when active I/Os are in progress on the file system and the file system is being shrunk to a size closer to its current usage. You see a message similar to the following example:

```
UX:vxfs fsadm: ERROR: V-3-20343: cannot shrink /dev/vx/rdsk/dg1/vol1 -
blocks are currently in use.
```

VxVM vxresize ERROR V-5-1-7514 Problem running fsadm command for volume voll, in diskgroup dg1

**Workaround:** Rerun the shrink operation after stopping the I/Os.

### **In a VxFS file system that has compression enabled, the file system may get disabled due to the ENOSPC error (3301716)**

In a VxFS file system that has compression enabled, the file system may get disabled due to the ENOSPC error. This occurs because of a defect in the delayed allocation feature.

**Workaround:** Turn off the delayed allocation.

### **Two VxFS parameters are deprecated (3260671)**

The `read_unit_io` and `write_unit_io` parameters have been deprecated. If you specify values for these parameters, they do not affect system behavior. The parameters will be removed in a future release.

**Workaround:** Not applicable.

### **When in-place and relocate compression rules are in the same policy file, file relocation is unpredictable (3278193)**

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.

### **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.

### **The file system may hang due to file system full conditions when file level snapshots are present (2746259)**

In the presence of file level snapshots, file system full conditions may lead to the file system hang. Following a reboot, a mount may hang as well.

**Workaround:**

There is no workaround for this issue.

**The file system may be marked for full fsck during a clone removal (2977828)**

Under low memory conditions, a clone removal may lead to file system being marked for full fsck.

**Workaround:**

A full fsck of the file system will be required to recover the file system.

**Unaligned large reads may lead to performance issues (3064877)**

On AIX, when there are unaligned large reads, there may be a performance degradation.

**Workaround:**

There is no workaround for this issue.

**NFSv4 server panics in unlock path (3228646)**

In a CFS configuration, if `fcntl(1m)` fails, some NFS specific structures (`I_pid`) are not updated correctly and may point to stale information. This causes the NFSv4 server to panic.

**Workaround:**

There is no workaround for this issue.

**I/O errors on the file system may lead to data inconsistency (3331282)**

If there are writable clones on the file system, I/O errors may lead to data inconsistency.

**Workaround:**

Run a full `fsck` to recover the file system.

**Forcing the system to unmount during heavy I/O load may result in system panic in `vx_is_fs_disabled_impl` (3331284)**

Forcing the system to unmount during heavy I/O load may result in system panic in `vx_is_fs_disabled_impl`.

**Workaround:**

There is no workaround for this issue.

**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.

**In case of scenarios where updates to writable clones are frequent, the clone operation may hang (3348553)**

In case of scenarios where updates to writable clones are frequent, the clone operation may hang when a large directory hash is enabled, and inodes are reused aggressively.

**Workaround:** There is no workaround for this issue.

## Replication known issues

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

**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 vradmnr 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.

**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 `vxxvrg -g dg -P snap_prefix snapdestroy vvg` 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 -V 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 -V vxfs /dev/vx/dsk/dg/data_volume
```

## 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.

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

## **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
```

## **vxassist and vxresize operations do not work with layered volumes that are associated to an RVG (2162579)**

This issue occurs when you try a resize operation on a volume that is associated to an RVG and has a striped-mirror layout.

### **Workaround:**

To resize layered volumes that are associated to an RVG:

- 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 Resize the volumes. In this example, the volume is increased to 10 GB. Enter the following:  

```
# vxassist -g diskgroup growto vol 10G
```
- 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.

## 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 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.

## 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.

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

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 `newIPM_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
```

## The `vradmin repstatus` command does not show that the SmartSync feature is running (3345984)

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
```

## 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: None

## 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 6.1 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.

## 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*.

## Symantec Storage Foundation for Databases (SFDB) tools known issues

The following are known issues in this release of Symantec Storage Foundation for Databases (SFDB) tools.

### SFDB commands do not work in IPV6 environment (2619958)

In IPV6 environment, SFDB commands do not work for SFHA. There is no workaround at this point of time.

### 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.

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 of 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.

## Upgrading Symantec Storage Foundation for Databases (SFDB) tools from 5.0.x to 6.1 (2184482)

The `sfua_rept_migrate` command results in an error message after upgrading SFHA or SF for Oracle RAC version 5.0 or 5.0MP3 to SFHA or SF for Oracle RAC 6.1.

When upgrading from SFHA version 5.0 or 5.0MP3 to SFHA 6.1 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`.

## 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 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 workaround at this point of time.

## Checkpoint clone fails if the archive log destination is same as the datafiles destination (2869266)

Checkpoint cloning fails if the archive log destination is the same as the datafiles destination. The error is similar to:

```
Use of uninitialized value $path in hash element
at /opt/VRTSdbed/lib/perl/DBED/CkptOracle.pm line 121.
Use of uninitialized value $path in concatenation (.) or string
at /opt/VRTSdbed/lib/perl/DBED/CkptOracle.pm line 124.
Use of uninitialized value $path in pattern match (m//)
at /opt/VRTSdbed/lib/perl/DBED/CkptOracle.pm line 126.
```

```
SFDB vxsfadm ERROR V-81-0564 Oracle returned error.
```

```
Reason: ORA-02236: invalid file name (DBD ERROR: error possibly near
<*> indicator at char 172 in 'CREATE CONTROLFILE REUSE SET DATABASE
'TClone03' RESETLOGS NOARCHIVELOG
```

**Workaround:** For the 6.1 release, create distinct archive and datafile mounts for the checkpoint service.

## 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.

## sfua\_rept\_migrate fails after phased SF Oracle RAC upgrade from 5.0MP3RP5 to 6.0.1 (2874322)

Command `sfua_rept_migrate` sometimes gives an error when upgrading to 6.0.1, and fails to unmount the repository volume. The error message is similar to:

```
# ./sfua_rept_migrate
Mounting SFUA Sybase ASA repository.
Unmounting SFUA Sybase ASA repository.
UX:vxfs umount: ERROR: V-3-26388: file system /rep has been mount
locked
SFORA sfua_rept_migrate ERROR V-81-5550 umount /dev/vx/dsk/repdg/repvol
```

```
failed.  
SFORA sfua_rept_migrate ERROR V-81-9162 Failed to umount repository.
```

**Workaround:** The error does not hamper the upgrade. The repository migration works fine, but the old repository volume does not get unmounted. Unmount the mount using the manual option.

For example, use `/opt/VRTS/bin/umount -o mntunlock=VCS /rep`.

For more information, see [TECH64812](#).

## 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:

```
[oracle@dblxx64-3-vip3 ~]$ 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 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 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.

### The information file that is generated after a DBED data collector operation reports an error (2795490)

When the VRTSexplorer DBED scripts use the old VRTSdbms3-specific scripts that are removed from the products, the information file reports the following error:

```
/opt/VRTSdbms3/vxdbms_env.sh: cannot open [No such file or directory]
```

**Workaround:**

- 1 Run the `cd /opt/VRTSspt/DataCollector/sort` command. If this directory does not exist, run `sh /opt/VRTSspt/DataCollector/*.sh`.
- 2 Run the `cd advanced/lib/VOS/v10/Collector/VxExpCollector/explorer_scripts` command.
- 3 In `dbed_rept_sql`, comment

```
$VXDBMS_DIR/vxdbms_env.sh
```

Or

Replace `$VXDBMS_DIR/vxdbms_env.sh` with

```
[[ -f $VXDBMS_DIR/vxdbms_env.sh ]] &&
{
    . $VXDBMS_DIR/vxdbms_env.sh
}
```

**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.

## 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.

## In an off-host scenario, a clone operation may fail with an error message (3313572)

A clone operation may fail with the following error due to restricted process resource limits in effect for the root user.

```
ORA-00283: recovery session canceled due to errors
ORA-01110: data file 5: '/flash_snap/oracle/oradata/run/soe.dbf'
ORA-01157: cannot identify/lock data file 5 - see DBWR trace file
ORA-01110: data file 5: '/flash_snap/oracle/oradata/run/soe.dbf'
```

All off-host operations especially the clone operations are routed through the `vxdbd` daemon, which is currently unable to support the per-user process resource limits that are set for the non-root users. Thus, all operations that are routed through `vxdbd`, inherit the resource limits set for the root user. If these limits are restrictive, then the operation may fail.

**Workaround:** Set the resource limit for the root user to a maximum range such that it is close to the Oracle database's requirement.

## The database clone operation using the `vxsfadm -o clone(1M)` command fails (3313715)

In an Oracle RAC environment, while you try to bring up a cloned database instance on a remote RAC node using the `SECONDARY_HOST` parameter in snapshot configuration, the database clone operation fails. Additionally, the following error message occurs:

```
[oracle@rac-v01 ~]$ vxsfadm -s flashsnap -a oracle -o clone
--flashsnap_name sn115 --clone_path /cloneoracle --clone_name cln709
--secondary_host rac-v02
```

```
SFDB vxsfadm ERROR V-81-0602 Remote execution failed:
SFDB vxsfadm ERROR V-81-0000 Another instance of vxsfadm is running
```

**Workaround:** Avoid using the `SECONDARY_HOST` parameter in a snapshot configuration. Additionally, perform the cloning operation locally on the RAC node where you need the cloned instance to be brought up.

## Flashsnap clone fails under some unusual archive log 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'
```

## Database Storage Checkpoints created by using `dbed_ckptcreate` may not be visible after upgrading to 6.1 (2626248)

After upgrading from a 5.0 release to 6.1, the Database Storage Checkpoints created earlier using `dbed_ckptcreate` may not be migrated.

### Workaround

Perform the following steps to make the old Database Storage Checkpoints visible.

To resolve the issue:

- 1 Remove the new repository.
  - Examine the contents of the `/var/vx/vxdba/rep_locfile` to determine the location of the 6.1 repository.
  - Remove the `.sfae` directory specified as the `location` attribute.
- 2 Remove the repository location file: `/var/vx/vxdba/rep_loc`.
- 3 Create a symlink `/var/vx/vxdba/<SID>/sfdb_rept` pointing to the `.sfdb_rept` directory created in the same location as the `.sfae` directory removed earlier.

```
$ ln -s <location>/sfdb_rept /var/vx/vxdba/<SID>/sfdb_rept
```

This step creates a symlink to the old repository.

- 4 Import repository data by running the `dbed_update` command.

This step imports the data from the old repository.

The old Database Storage Checkpoints are now visible.

## Instant mode clone fails in RAC environment for all FSMs with data loading (3517782)

When you use the instant clone mode for RAC databases, the clone operation may fail during Oracle recovery. The issue is more likely to be seen when there is load activity on some of the RAC nodes.

**Workaround:** Use either online or offline snapshot mode.

## Virtualization known issues

There are no new virtualization known issues in this release of Symantec Storage Foundation and High Availability (SFHA).

## Software limitations

This section covers the software limitations of this release.

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

See [“Documentation”](#) on page 101.

## Veritas Volume Manager software limitations

The following are software limitations in this release of Veritas Volume Manager.

### **SFHA does not support thin reclamation of space on a linked mirror volume (2729563)**

The thin reclamation feature does not support thin reclamation for a linked mirror volume.

### **Thin reclamation requests are not redirected even when the ioship policy is enabled (2755982)**

Reclamation requests fail from nodes that do not have local connectivity to the disks, even when the ioship policy is enabled. Reclamation I/Os are not redirected to another node.

### **Veritas Operations Manager does not support disk, disk group, and volume state information related to CVM I/O shipping feature (2781126)**

The Veritas Operations Manager (VOM) does not support disk, disk group, and volume state information related to the I/O shipping feature introduced in this release of Cluster Volume Manager. New states such as Ifailed, lmissing or LDISABLED are introduced when I/O shipping is active because of storage disconnectivity.

### **Limitation with device renaming on AIX 6.1TL6**

If you rename an operating system (OS) path with the `rendev` command on AIX 6.1TL6, the operation might remove the paths from DMP control. DMP cannot discover these paths.

## DMP settings for NetApp storage attached environment

To minimize the path restoration window and maximize high availability in the NetApp storage attached environment, change the default values for the DMP tunable parameters.

[Table 1-12](#) describes the DMP tunable parameters and the new values.

**Table 1-12** DMP settings for NetApp storage attached environment

Parameter name	Definition	New value	Default value
dmp_restore_interval	DMP restore daemon cycle	60 seconds.	300 seconds.
dmp_path_age	DMP path aging tunable	120 seconds.	300 seconds.

The change is persistent across reboots.

### To change the tunable parameters

1 Issue the following commands:

```
# vxddmpadm settune dmp_restore_interval=60
```

```
# vxddmpadm settune dmp_path_age=120
```

2 To verify the new settings, use the following commands:

```
# vxddmpadm gettune dmp_restore_interval
```

```
# vxddmpadm gettune dmp_path_age
```

## DMP support in AIX virtualization environment (2138060)

DMP does not support exporting paths to the same LUN through both vSCSI and NPIV interfaces.

DMP treats the same LUN seen through vSCSI and NPIV interfaces as two separate LUNs, because the behavior of the LUN at the VIOC level is different due to the intermediate SCSI interface at the VIOS level for vSCSI devices.

## Snapshot configuration with volumes in shared disk groups and private disk groups is not supported

A snapshot configuration with volumes in the shared disk groups and private disk groups is not a recommended configuration. In this release, this configuration is not supported.

## Storage reclamation does not happen on volumes with break-off snapshot (2798523)

In this release, storage reclamation on a volume is prevented when it has a break-off type snapshot. If storage reclamation is allowed on such volumes, it can lead to the following undesired situation. Instant snapshot operations, including `vxsnap refresh` and `vxsnap restore` operations, lead to full synchronization of either the snapshot or the primary volume depending on the operation.

In this release, if the volume has a snapshot, the storage reclamation is silently prevented. The physical storage is not reduced. The reclaim command reports that the reclamation is done on the disks but the actual storage is not reclaimed for volumes with snapshots:

```
# vxdisk -o full reclaim dg1
```

```
Reclaiming storage on:
```

```
Disk xiv0_617 : Done.
```

```
Disk xiv0_616 : Done.
```

```
Disk xiv0_618 : Done.
```

```
Disk xiv0_612 : Done.
```

```
Disk xiv0_613 : Done.
```

```
Disk xiv0_614 : Done.
```

```
Disk xiv0_615 : Done
```

As shown in the following example output, the storage is not actually reclaimed.

```
# vxdisk -o thin list
```

DEVICE	SIZE (MB)	PHYS_ALLOC (MB)	GROUP	TYPE
xiv0_612	19313	2101	dg1	thinrclm
xiv0_613	19313	2108	dg1	thinrclm
xiv0_614	19313	35	dg1	thinrclm
xiv0_615	19313	32	dg1	thinrclm
xiv0_616	19313	31	dg1	thinrclm
xiv0_617	19313	31	dg1	thinrclm
xiv0_618	19313	31	dg1	thinrclm

## Veritas File System software limitations

The following are software limitations in this release of Veritas File System.

### **Recommended limit of number of files in a directory**

To maximize VxFS performance, do not exceed 100,000 files in the same directory. Use multiple directories instead.

### **The `vxlist` command cannot correctly display numbers greater than or equal to 1 EB**

The `vxlist` command and all of the other commands that use the same library as the `vxlist` command cannot correctly display numbers greater than or equal to 1 EB.

### **Limitations with delayed allocation for extending writes feature**

The following limitations apply to the delayed allocation for extending writes feature:

- In the cases where the file data must be written to disk immediately, delayed allocation is disabled on that file. Examples of such cases include Direct I/O, concurrent I/O, FDD/ODM access, and synchronous I/O.
- Delayed allocation is not supported on memory mapped files.
- Delayed allocation is not supported with BSD quotas. When BSD quotas are enabled on a file system, delayed allocation is turned off automatically for that file system.
- Delayed allocation is not supported for shared mounts in a cluster file system.

### **FlashBackup feature of NetBackup 7.5 (or earlier) does not support disk layout Version 8, 9, or 10**

The FlashBackup feature of NetBackup 7.5 (or earlier) does not support disk layout Version 8, 9, or 10.

## Replication software limitations

The following are replication software limitations in this release of Symantec Storage Foundation and High Availability.

### **VVR Replication in a shared environment**

Currently, replication support is limited to 8-node cluster applications.

## VVR IPv6 software limitations

VVR does not support the following Internet Protocol configurations:

- A replication configuration from an IPv4-only node to an IPv6-only node and from an IPv6-only node to an IPv4-only node is not supported, because the IPv6-only node has no IPv4 address configured on it and therefore VVR cannot establish communication between the two nodes.
- A replication configuration in which an IPv4 address is specified for the `local_host` attribute of a primary RLINK and an IPv6 address is specified for the `remote_host` attribute of the same RLINK.
- A replication configuration in which an IPv6 address is specified for the `local_host` attribute of a primary RLINK and an IPv4 address is specified for the `remote_host` attribute of the same RLINK.
- IPv6 is not supported in a CVM and VVR cluster where some nodes in the cluster are IPv4-only and other nodes in the same cluster are IPv6-only, or all nodes of a cluster are IPv4-only and all nodes of a remote cluster are IPv6-only.
- VVR does not support Edge and NAT-PT routers that facilitate IPv4 and IPv6 address translation.

## VVR support for replicating across Storage Foundation versions

VVR supports replication between Storage Foundation 6.1 and the prior major releases of Storage Foundation (6.0 and 6.0.1). Replication between versions is supported for disk group versions 170, 180, and 190 only. Both the Primary and Secondary hosts must be using a supported disk group version.

## Limitations related to I/O fencing

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

### Preferred fencing limitation when VxFEN activates RACER node re-election

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

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

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

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

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

## Stopping systems in clusters with I/O fencing configured

The I/O fencing feature protects against data corruption resulting from a failed cluster interconnect, or “split brain.” See the *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 fileset, the DMP module will no longer be

loaded in memory. On a system where VRTSvxvm fileset is uninstalled, if VxFEN attempts to access DMP devices during shutdown or fencing arbitration, the system panics.

## Limitations related to LLT

This section covers LLT-related software limitations.

### **LLT over IPv6 UDP cannot detect other nodes while SFHA tries to form a cluster (1907223)**

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

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

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

### **LLT does not start automatically after system reboot (2058752)**

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

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

#### **Workaround: To resolve the LLT startup issue**

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

## Symantec Storage Foundation for Databases (SFDB) tools software limitations

The following are the SFDB tools software limitations in this release.

### Oracle Data Guard in an Oracle RAC environment

SFDB tools cannot be used with RAC standby databases. SFDB tools can still be used with the primary database, even in a Data Guard Oracle RAC environment.

### Upgrading to Oracle 10.2.0.5 is required if using SFDB tools

If you are running Oracle version 10.2.0.4 and upgrading a Storage Foundation product with SFDB tools to 6.1, you must upgrade the Oracle binaries and database to version 10.2.0.5, before upgrading to 6.1.

### Parallel execution of `vxsfadm` is not supported (2515442)

Only one instance of the `vxsfadm` command can be run at a time. Running multiple instances of `vxsfadm` at a time is not supported.

### Creating point-in-time copies during database structural changes is not supported (2496178)

SFDB tools do not support creating point-in-time copies while structural changes to the database are in progress, such as adding or dropping tablespaces and adding or dropping data files.

However, once a point-in-time copy is taken, you can create a clone at any time, regardless of the status of the database.

## Documentation

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

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

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

## Documentation set

Each product in the Storage Foundation and High Availability Solutions product line includes release notes, an installation guide, and additional documents such as administration and agent guides. In most cases, you may also need to refer to the documentation for the product's components.

The SFHA Solutions documents describe functionality and solutions that apply across the product line. These documents are relevant whichever SFHA Solutions product you use.

### Storage Foundation and High Availability

[Table 1-13](#) lists the documentation for Symantec Storage Foundation and High Availability.

For cluster administration, refer to the Symantec Cluster Server Administrator's Guide

See [the section called "Symantec Cluster Server documentation"](#) on page 102.

For storage administration, refer to the Symantec Storage Foundation Administrator's Guide.

See [the section called "Symantec Storage Foundation documentation"](#) on page 103.

The SFHA Solutions documents describe functionality and solutions relevant to the SFHA product.

See [Table 1-16](#) on page 104.

**Table 1-13** Symantec Storage Foundation and High Availability documentation

Document title	File name	Description
<i>Symantec Storage Foundation and High Availability Release Notes</i>	sfha_notes_61_aix.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
<i>Symantec Storage Foundation and High Availability Installation Guide</i>	sfha_install_61_aix.pdf	Provides information required to install the product.

### Symantec Cluster Server documentation

[Table 1-14](#) lists the documents for Symantec Cluster Server.

**Table 1-14** Symantec Cluster Server documentation

Title	File name	Description
<i>Symantec Cluster Server Release Notes</i>	vcs_notes_61_aix.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
<i>Symantec Cluster Server Installation Guide</i>	vcs_install_61_aix.pdf	Provides information required to install the product.
<i>Symantec Cluster Server Administrator's Guide</i>	vcs_admin_61_aix.pdf	Provides information required for administering the product.
<i>Symantec Cluster Server Bundled Agents Reference Guide</i>	vcs_bundled_agents_61_aix.pdf	Provides information about bundled agents, their resources and attributes, and more related information.
<i>Symantec Cluster Server Agent Developer's Guide</i> (This document is available online only.)	vcs_agent_dev_61_unix.pdf	Provides information about the various Symantec agents and procedures for developing custom agents.
<i>Symantec Cluster Server Agent for DB2 Installation and Configuration Guide</i>	vcs_db2_agent_61_aix.pdf	Provides notes for installing and configuring the DB2 agent.
<i>Symantec Cluster Server Agent for Oracle Installation and Configuration Guide</i>	vcs_oracle_agent_61_aix.pdf	Provides notes for installing and configuring the Oracle agent.
<i>Symantec Cluster Server Agent for Sybase Installation and Configuration Guide</i>	vcs_sybase_agent_61_aix.pdf	Provides notes for installing and configuring the Sybase agent.

## Symantec Storage Foundation documentation

[Table 1-15](#) lists the documentation for Symantec Storage Foundation.

**Table 1-15** Symantec Storage Foundation documentation

Document title	File name	Description
<i>Symantec Storage Foundation Release Notes</i>	sf_notes_61_aix.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.

**Table 1-15** Symantec Storage Foundation documentation (*continued*)

Document title	File name	Description
<i>Symantec Storage Foundation Installation Guide</i>	sf_install_61_aix.pdf	Provides information required to install the product.
<i>Symantec Storage Foundation Administrator's Guide</i>	sf_admin_61_aix.pdf	Provides information required for administering the product.
<i>Symantec Storage Foundation: Storage and Availability Management for DB2 Databases</i>	sfhas_db2_admin_61_unix.pdf	Provides information about the deployment and key use cases of the SFDB tools with Storage Foundation High Availability (SFHA) Solutions products in DB2 database environments. It is a supplemental guide to be used in conjunction with SFHA Solutions product guides.
<i>Symantec Storage Foundation: Storage and Availability Management for Oracle Databases</i>	sfhas_oracle_admin_61_unix.pdf	Provides information about the deployment and key use cases of the SFDB tools with Storage Foundation High Availability (SFHA) Solutions products in Oracle database environments. It is a supplemental guide to be used in conjunction with SFHA Solutions product guides.
<i>Veritas File System Programmer's Reference Guide</i> (This document is available online only.)	vxfs_ref_61_aix.pdf	Provides developers with the information necessary to use the application programming interfaces (APIs) to modify and tune various features and components of the Veritas File System.

## Symantec Storage Foundation and High Availability Solutions products documentation

[Table 1-16](#) lists the documentation for Symantec Storage Foundation and High Availability Solutions products.

**Table 1-16** Symantec Storage Foundation and High Availability Solutions products documentation

Document title	File name	Description
<i>Symantec Storage Foundation and High Availability Solutions—What's new in this release</i> (This document is available online.)	sfhas_whats_new_61_unix.pdf	Provides information about the new features and enhancements in the release.

**Table 1-16** Symantec Storage Foundation and High Availability Solutions products documentation (*continued*)

Document title	File name	Description
<i>Symantec Storage Foundation and High Availability Solutions Getting Started Guide</i>	getting_started.pdf	Provides a high-level overview of installing Symantec products using the Veritas script-based installer. The guide is useful for new users and returning users that want a quick refresher.
<i>Symantec Storage Foundation and High Availability Solutions Solutions Guide</i>	sfhas_solutions_61_aix.pdf	Provides information about how SFHA Solutions product components and features can be used individually and in concert to improve performance, resilience and ease of management for storage and applications.
<i>Symantec Storage Foundation and High Availability Solutions Virtualization Guide</i> (This document is available online.)	sfhas_virtualization_61_aix.pdf	Provides information about Symantec Storage Foundation and High Availability support for virtualization technologies. Review this entire document before you install virtualization software on systems running SFHA products.
<i>Symantec Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide</i> (This document is available online.)	sfhas_dr_impl_61_aix.pdf	Provides information on configuring campus clusters, global clusters, and replicated data clusters (RDC) for disaster recovery failover using Storage Foundation and High Availability Solutions products.
<i>Symantec Storage Foundation and High Availability Solutions Replication Administrator's Guide</i>	sfhas_replication_admin_61_aix.pdf	Provides information on using Volume Replicator (VVR) for setting up an effective disaster recovery plan by maintaining a consistent copy of application data at one or more remote locations.
<i>Symantec Storage Foundation and High Availability Solutions Troubleshooting Guide</i>	sfhas_tshoot_61_aix.pdf	Provides information on common issues that might be encountered when using Symantec Storage Foundation and High Availability Solutions and possible solutions for those issues.

Veritas Operations Manager (VOM) is a management tool that you can use to manage Symantec Storage Foundation and High Availability Solutions products. If you use VOM, refer to the VOM product documentation at:

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

## Manual pages

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

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

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

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

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

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

See the `man(1)` manual page.

The latest manual pages are available online in HTML format on the Symantec website at:

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