Symantec™ VirtualStore Release Notes

Solaris

6.0 Platform Release 1

Symantec™ VirtualStore Release Notes

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

Product version: 6.0 PR1

Document version: 6.0PR1.3

Legal Notice

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization

- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information

- Upgrade assurance that delivers software upgrades

- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis

- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information

- Available memory, disk space, and NIC information

- Operating system

- Version and patch level

- Network topology

- Router, gateway, and IP address information

- Problem description:

  - Error messages and log files

  - Troubleshooting that was performed before contacting Symantec

  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization

- Product registration updates, such as address or name changes

- General product information (features, language availability, local dealers)

- Latest information about product updates and upgrades

- Information about upgrade assurance and support contracts

- Information about the Symantec Buying Programs

- Advice about Symantec's technical support options

- Nontechnical presales questions

- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

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

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

About Symantec 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 VirtualStore Release Notes

This document includes the following topics:

- About this document
- Component product release notes
- About Symantec VirtualStore
- Important release information
- Changes introduced in 6.0 PR1
- Changes related to installation
- Changes introduced in 6.0
- System requirements
- Known issues
- Software limitations
- Documentation errata
- Documentation

About this document

This document provides important information about Symantec VirtualStore (SVS) version 6.0 PR1 for Solaris. Review this entire document before you install or upgrade SVS.

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

This is Document version: 6.0PR1.3 of the *Symantec VirtualStore 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

For the latest information on updates, patches, and known issues regarding this release, see the following TechNote on the Symantec Technical Support website:

http://www.symantec.com/docs/TECH141448

Component product release notes

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

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

/product_name/docs

Symantec recommends copying the docs directory on the software media that contains the product guides to the /opt/VRTS directory on your system.

This release includes the following component product release notes:

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

■ *Veritas Cluster Server Release Notes* (6.0 PR1)

■ *Veritas Storage Foundation Cluster File System High Availability Release Notes* (6.0 PR1)

About Symantec VirtualStore

Symantec VirtualStore (SVS) powered by Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) serves as a highly scalable, highly available NAS solution optimized for deploying and hosting virtual machine. VirtualStore is built on top of Cluster File System (CFS), which provides high availability and linear scalability across the cluster.

Important release information

- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:
  http://www.symantec.com/docs/TECH164885

- For the latest patches available for this release, go to:
  http://sort.symantec.com/

- The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit the following URL:
  http://www.symantec.com/docs/TECH170013
  Before installing or upgrading Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

Changes introduced in 6.0 PR1

This section lists the changes in Symantec VirtualStore 6.0 PR1.

Changes related to installation

The product installer includes the following changes.

New packaging framework in Solaris 11

Solaris 11 introduces the new IPS packaging framework. All of the Symantec packages have been modified to IPS packages.

Changes introduced in 6.0

This section lists the changes in Symantec VirtualStore 6.0.

Changes related to installation and upgrades

The product installer includes the following changes in 6.0 PR1.

Support for product deployment using Flash Archives on Solaris 10

Use a Flash archive to install the Storage Foundation and High Availability Suite of products and the Solaris 10 operating system in conjunction with JumpStart.

See the *Installation Guide* for more information.

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

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

The installer can check product versions and hotfixes

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

You can discover the following information with these commands:

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

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

Using the installer's postcheck option

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

Rolling upgrade improvements

The rolling upgrade procedure has been streamlined and simplified.

Allow Response files to change tuning parameters

You can set non-default product and system tunable parameters using a tunables template file. With the file, you can set tunables such as the I/O policy or toggle native multi-pathing during or after the installation procedure.

See the *Installation Guide* for more information.

Using the installer for Symantec Virtual Store (SVS)

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

Packaging updates

The following lists the package changes in this release.

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

- New `VRTSfsadv` package for product data deduplication on Solaris SPARC
  The `VRTSfsadv` package is introduced in this release on Solaris SPARC. The `VRTSfsadv` package contains the libraries for the data deduplication feature.

For more information, see the *Installation Guide*.

Changes related to Symantec VirtualStore (SVS)

Symantec VirtualStore includes the following changes in 6.0 PR1:

Default disk layout Version is now 9

In this release, disk layout Version 9 is now the default version, which enables support for the following features:

- File compression
- Data deduplication

See the *Administrator's Guide*.

Enabled VMware View Integration

This allows you to import FileSnap cloned machines as a new Desktop Pool in VMware View.

See the *Symantec VirtualStore Installation and Configuration Guide* for more information on creating virtual machine clones using Symantec FileSnap.

Direct NFS support in Clustered NFS environments for Oracle

Added support for NFS coming from Clustered NFS. Symantec VirtualStore (SVS) can serve as the backend storage for Oracle databases.

Direct NFS (dNFS) is an optimized NFS client that provides faster and more scalable access to NFS storage located on NAS storage accessible over TCP/IP.

See the *Symantec VirtualStore Administrator's Guide* for more information on deploying Oracle with Clustered NFS and VirtualStore utilities for the Oracle database.

See the `svsdbsnap`(1M) manual page.

Enhancements to the vCenter Plug-in

These enhancements to the vCenter Plug-in allows you to:

- Sets up a failover Web Service to host the VMware vSphere Plug-ins.

- Registers the cluster to the VMware vCenter Server.

- Unregisters the cluster from the VMware vCenter Server.

- Verifies the registration to a particular VMware vCenter Server.

- Displays a list of VMware vCenter Server to which the cluster is registered.

See the *Symantec VirtualStore Installation and Configuration Guide* for more information on setting up VirtualStore.

See the `svsvmwadm`(1M) manual page.

Added nodes into the Clustered NFS cluster

The `cfsshare` command has the ability to add a node in the Clustered NFS (CNFS) cluster.

See the *Veritas Storage Foundation Cluster File System Administrator's High Availability Guide.*

See the `cfsshare`(1M) manual page.

Administering iSCSI with VirtualStore

The `svsiscsiadm` command provides a mechanism to simplify the administration of exporting iSCSI LUNs backed by files residing on the VirtualStore file system. This utilizes the iSCSI target driver implementation that is shipped with the operating system.

See the *Symantec VirtualStore Administrator's Guide.*

See the `svsiscsiadm`(1M) manual page.

Enhancements to the installation and configuration of VirtualStore

Added the following enhancements to the installation and configuration of VirtualStore:

■ Typical installation mode - automatically configures VirutalStore with typical default settings.

■ Custom installation mode - prompts you to customize your VirtualStore configuration.

See the *Symantec VirtualStore Installatation and Configuration Guide*.

Improved the cfsshare command

Provided the following improvements to the `cfsshare` command:

■ Added the `-D` option to the `cfsshare` manual page. The `-D` option is used to deep I/O monitor the volume used by the file system.

■ Error messages that are returned from the command are more meaningful.

See the `cfsshare`(1M) manual page.

See the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide*.

FileSnap creation over Network File System

You can create a FileSnap over Network File System (NFS) by creating a hard link from an existing file to a new file with the extension ":::snap:vxfs:".

See the *Administrator's Guide*.

File compression

You can compress files to reduce the space used, while retaining the accessibility of the files and having the compression be transparent to applications. Compressed files look and behave almost exactly like uncompressed files: the compressed files have the same name, and can be read and written as with uncompressed files.

See the *Administrator's Guide*.

Migrating a source file system to the VxFS file system over NFS v3

NFS is one of the most commonly used file systems in network-attached storage solutions and is one of the standard file sharing mechanisms used in UNIX

environments. This feature enables you to migrate a source file system to the VxFS file system over your existing NFS v3 solution.

See the *Veritas Storage Foundation and High Availability Solutions Solutions Guide*.

Data deduplication on Solaris SPARC

On Solaris SPARC, you can run post-process periodic deduplication in a file system, which eliminates duplicate data without any continuous cost. This feature requires an Enterprise license.

See the *Administrator's Guide*.

Changes to SVS clusters in secure mode

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

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

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

Changes to LLT

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

- Faster detection of LLT link failures
  LLT now has the capability to detect the LLT link failures immediately using the operating system's link-down notification feature.

- LLT now supports VLAN tagging (IEEE 802.1Q).

- The `lltconfig` command includes the following new options:

  - -Q
    You can use this option to configure a link as "hidden". LLT needs this type of link when you enable faster detection of link failure.

  - -j
    You can use this option to set the LLT link failure detection level.

  - The command also includes a new timer parameter `linkstable`. This parameter specifies the amount of time to wait before LLT processes the

link-down event for any link of the local node when you have enabled faster link failure detection. This `linkstable` prevents a flaky link from causing unnecessary membership changes.

- -N
  You can use this option to list all the used cluster IDs.

- -M
  You can use this option to display the currently loaded LLT module version information.

See the `lltconfig` manual page for more information.

The llttab file includes the following changes:

- hidden
  The new keyword hidden indicates that the link is a hidden link which LLT uses when you enable faster detection of link failure.

- set-linkfaildetectlevel
  You can use this new command option in the `/etc/llttab` file to set the LLT link failure detection level.

- Link utilization statistics are enhanced that help in the root cause analysis of performance related issues.

- Periodic flushing of ARP cache is disabled.

See the *Symantec VirtualStore Installation and Configuration Guide* and the *Symantec VirtualStore Administrator's Guide* for more details.

Changes to GAB

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

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

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

With the GAB and I/O fencing integration in this release, if the I/O fencing module's decision is still pending before GAB initiates a join of the subcluster, GAB delays the iofence message. GAB wait depends on the value of the VxFEN

tunable parameter *panic_timeout_offst* based on which VxFEN computes the delay value and passes to GAB.

See the Symantec VirtualStore Administrator's Guide for more details.

GAB can now recognize clients with names in addition to ports

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

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

The gabconfig command has new -C option

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

Changes to I/O fencing

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

Support for Non-SCSI3 fencing

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

See the *Symantec VirtualStore Installation and Configuration Guide* and the *Symantec VirtualStore Administrator's Guide* for more details.

Installer support to migrate between fencing configurations in an online cluster

You can now use the installer to migrate between disk-based and server-based fencing configurations. You can also replace the coordination points for any I/O

fencing configuration in an online cluster using the same installer option. The installer uses the `vxfenswap` script internally.

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

See the *Symantec VirtualStore Administrator's Guide* for more details.

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

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

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

■ If the racer node is not able to reach a majority of coordination points, then the VxFEN module on the racer node sends a LOST_RACE message and all nodes in the subcluster also panic when they receive the LOST_RACE message.

■ If the racer node panics during the arbitration, then the spectator nodes in the sub-cluster assume that the racer node lost the race and the spectator nodes also panic.

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

See the *Symantec VirtualStore Administrator's Guide* for more details.

Support for multiple virtual IP addresses in CP servers

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

See the *Symantec VirtualStore Installation and Configuration Guide* and the *Symantec VirtualStore Administrator's Guide* for more details.

Support for Quorum agent in CP servers

With the support for multiple virtual IP addresses, you can now use the Quorum agent to configure CP server service group failover policies. You can specify the

minimum number of IP resources that must be online for the Quorum resource to remain online.

See the *Symantec VirtualStore Installation and Configuration Guide* and the *Symantec VirtualStore Administrator's Guide* for more details.

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

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

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

■ If a number of nodes in a cluster are not up, GAB port (port a) still comes up in all the member-nodes in the cluster.

■ If the coordination points do not have keys from any non-member nodes, I/O fencing (GAB port b) also comes up.

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

See the *Symantec VirtualStore Administrator's Guide* for more details.

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

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

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

In this release, this behavior has changed. When a node leaves gracefully, the CVM or other clients on that node are stopped before the VxFEN module is unconfigured. Hence, data disks are already clear of its keys. The remaining sub-cluster tries to clear the gracefully leaving node's keys from the coordination points but does not panic if it is not able to clear the keys.

Enhancements to collecting a VxExplorer troubleshooting archive

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

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

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

www.symantec.com/docs/HOWTO32575

Licensing changes in the SFHA Solutions 6.0 release

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

■ The Cluster File System license is deprecated. CFS customers are entitled to the Storage Foundation Cluster File System High Availability (SFCFS HA) functionality.

■ The VVR Option is renamed as Veritas Replicator Option. This option includes VVR (volume-based replication) and the new file-based replication solution.

■ The VVR Enterprise license is deprecated; you can use Storage Foundation Enterprise and add Veritas Replicator Option to get this functionality. VVR Enterprise customers are entitled to Storage Foundation Enterprise with Replicator Option.

■ The VCS license enables full cluster functionality as well as the limited start/stop functionality.

■ Storage Foundation Enterprise CFS for Oracle RAC (Linux/x64) customers are entitled to Storage Foundation Enterprise for Oracle RAC (Linux/x64.)

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

■ The Compression feature is available with the Standard license.

■ The SmartTier feature is now available with the Standard license.

■ The Deduplication feature is available with the Enterprise license on Solaris SPARC.

The following products are included in this release:

■ Dynamic Multi-Pathing

■ VirtualStore

- Storage Foundation Basic

- Storage Foundation Standard

- Storage Foundation Enterprise

- Veritas Cluster Server

- Veritas Cluster Server HA/DR

- Storage Foundation Standard HA: Storage Foundation Standard plus Veritas Cluster Server

- Storage Foundation Enterprise HA: Storage Foundation Enterprise plus Veritas Cluster Server

- Storage Foundation Enterprise HA/DR

- Storage Foundation Enterprise Cluster File System HA

- Storage Foundation Enterprise Cluster File System HA/DR

- Storage Foundation Enterprise for Oracle RAC

- Storage Foundation Enterprise HA/DR for Oracle RAC

- Storage Foundation Enterprise for Sybase ASE CE

- Storage Foundation Enterprise HA/DR for Sybase CE

HA: High Availability

HA/DR: High Availability and Disaster Recovery

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

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

Changes related to product documentation

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

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

Table 1-1   New documents

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

Table 1-1   New documents *(continued)*

New documents	Notes
Veritas Storage Foundation Administrator's Guide	Administration information for Veritas Storage Foundation.
Veritas Storage Foundation and High Availability Release Notes	Release-specific information for Veritas Storage Foundation and High Availability users.
Veritas Storage Foundation and High Availability Solutions Solutions Guide	Solutions and use cases for Veritas Storage Foundation and High Availability Solutions.
Veritas Storage Foundation and High Availability Solutions Troubleshooting Guide	Troubleshooting information for Veritas Storage Foundation and High Availability Solutions.
Symantec VirtualStore Release Notes	Release-specific information Symantec VirtualStore.
Veritas Storage Foundation for Sybase ASE CE Release Notes	Release-specific information for Veritas Storage Foundation for Sybase ASE CE.
Veritas Storage Foundation for Sybase ASE CE Installation Guide	Installation information for Veritas Storage Foundation for Sybase ASE CE.
Veritas Storage Foundation for Sybase ASE CE Administrator's Guide	Administration information for Veritas Storage Foundation for Sybase ASE CE.
Virtual Business Services–Availability User's Guide	Information about Virtual Business Services. This document is available online.

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

Table 1-2   Deprecated documents

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

Table 1-2 Deprecated documents *(continued)*

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

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

Table 1-3 Online documents

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

System requirements

The topics in this section describe the system requirements for this release.

■ Supported operating systems

Supported operating systems

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

Table 1-4   Supported operating systems

Operating systems	Levels	Chipsets
Solaris 11	SRU 11.0.x.y.z	SPARC
Solaris 11	SRU 11.0.x.y.z	x64

Note: Supported Repository Update (SRU) digits in the table represent
Release.Update.SRU.Build.Respin.

Supported VMware software version

■ VMware vSphere 4 (ESX 4.0 Update 1 and later with vCenter Server 4.0 Update 1 and later)

■ VMware vSphere 4.1 (ESX 4.1 and later with vCenter Server 4.1 and later)

Supported guest operating system for guest operating system customization while cloning

■ Windows XP

■ Windows Server 2003

■ Windows 7

■ Windows Server 2008

■ Red Hat Enterprise Linux (RHEL 5)

■ Red Hat Enterprise Linux (RHEL 6)

■ SUSE Linux Enterprise Server (SLES 10)

■ SUSE Linux Enterprise Server (SLES 11)

Note: Customization of some guest operating systems and versions requires vCenter Server to be of sufficient version. Refer to
http://www.vmware.com/pdf/vsphere4/r40/vsp_compatibility_matrix.pdf for details.

Supported guest operating system for VMware View Integration while cloning

■ Windows XP

■ Windows 7

Veritas File System requirements

Veritas File System requires that the values of the Solaris variables `lwp_default_stksize` and `svc_default_stksize` are at least 0x8000. When you install the Veritas File System package, `VRTSvxfs`, the VRTSvxfs packaging scripts check the values of these variables in the kernel. If the values are less than the required values, the installer gives a warning. You need to set the values and reboot the system.

To avoid an unexpected need for a reboot, verify the values of the variables before installing Veritas File System.

Use the following commands to check the values of the variables:

```
# echo "lwp_default_stksize/X" | mdb -k
lwp_default_stksize:
lwp_default_stksize:            8000


# echo "svc_default_stksize/X" | mdb -k
svc_default_stksize:
svc_default_stksize:            8000
```

If the values shown are less than 8000, you can expect a reboot after installation.

Note: The default value of the `svc_default_stksize` variable is 0 (zero), which indicates that the value is set to the value of the `lwp_default_stksize` variable. In this case, no reboot is required, unless the value of the `lwp_default_stksize` variable is too small.

To avoid a reboot after installation, you can modify the `/etc/system` file with the appropriate values. Reboot the system prior to installing the packages. Add the following lines to the `/etc/system` file:

```
set lwp_default_stksize=0x8000
set rpcmod:svc_default_stksize=0x8000
```

Known issues

This section covers the known issues in this release.

See the corresponding Release Notes for a complete list of known issues related to that product.

Symantec VirtualStore issues

LUNs are seen as "unregistered" after reboot of a node (2725256)

After the node is rebooted, the LUNs added as part of online of iSCSITarget resources are shown as "unregistered".

To view if the LUNs are unregistered

◆   Enter the following command:

   # **stmfadm list-lu -v**

Workaround:

To resolve this issue

◆   Restart the stmf and the target service:

   # **svcadm restart stmf target**

The svsiscsiadm create lun command fails if you create a LUN greater than the available space on the file system (2567517)

The svsiscsiadm create lun command fails if you create a LUN of a size greater than the total amount of space available on the file system. The underlying iscsitadm command fails with the following error message:

iscsitadm: Error Requested size is too large for system

The report of this error is logged in the /var/VRTSvcs/log/engine_A.log file.

If you then try to create a LUN on the same target, the LUN creation call fails again with the following error message:

iscsitadm: Error Failed to create a symbolic link to the backing store

The report of this error is logged in the /var/VRTSvcs/log/engine_A.log file.

This makes the target unusable.

Workaround

To resolve this issue

1   Note the TargetID and LunID on which the `svsiscsiadm create lun`
    command failed. To find the failed LunID, note the last LunID for the target
    on which `svsiscsiadm create lun` command failed with the use of the
    `svsiscsiadm list` command. To calculate the failed LunID, add 1 to last
    LunID seen by the `svsiscsiadm list` command.

2   Go to the configuration directory for the TargetID:

    # **cd /etc/iscsi/*TargetID* .**

3   Delete the symlink pointing to path of LUN backing file which failed to get
    added. The below LunID is the failed LunID, which is a result of calculation
    in point 1:

    # **rm -f /etc/iscsi/*TargetID*/lun.($lunid + 1)**

After removal of the symlink you should be able to add LUNs on the unusable
target.

CFS commands might hang when run by non-root (2403263)

The CFS commands might hang when run by non-root.

Workaround

To resolve this issue

◆   Use `halogin` command to save the authentication information before running
    any CFS commands on a non-root sessions.

    When you run the `halogin`command, VCS stores encrypted authentication
    information in the user's home directory.

VirtualStore machine clones created while the VirtualStore cluster reboots will probably not start (2164664)

In some cases when you clone while rebooting the SVS nodes, you may receive
several of the following error messages:

```
clone vms could not start X server
```

Workaround

Delete all the clones that got created while the node crashed and redo the cloning
operation.

Cloning may not work (2348628)

If you cannot clone and you are using the VMware vAPP and OVF templates, then you must disable the vApp.

Workaround

To disable the vAPP

1 In VI Client, right-click on the virtual machine > **Edit Settings** > **Options** > **vApp Options**.

2 Click **Disable**.

Need intelligent NDMP/NBU backups for virtual machines (2378396)

When using NDMP or the NBU client to backup a virtual machine, the space consumed by the backup is equivalent to the size of the disks in the virtual machine, even though not all of the disk space in the virtual machine is used.

If a VMDK (Virtual Machine Disk) file is 10GB in size, but only consumes 1GB of disk space, an backup done by NDMP or the NBU client generates 10GB of backup data, even though the original VMDK file contains 9GB of unassigned disk space.

Workaround

Use VMware-specific backup applications (such as NetBackup for VMware) to create space-efficient backups.

The Symantec Quick Clone Virtual Machine Wizard may not behave as expected when multiple instances are open (2309702)

The wizard may not behave as expected, if you invoke multiple parallel session of the wizard from a single vSphere Client at the same time.

For example, if you do the following:

■ Right-click wingoldvm1 and invoke the wizard.

■ Then soon after, right-click slesgoldvm1 and invoke the wizard.

This causes you to have two instances of the wizard running from the same vSphere Client and can cause unexpected behavior.

Workaround

To resolve this issue:

■ Close both instances of the wizard.

■ Reopen a new instance of the wizard.

Virtual machines created by the Symantec Quick Clone Virtual Machine Wizard might not boot correctly if during the process the FileStore cluster node, the ESX Server, or the vCenter Server reboots (2164664, 2374229)

In some cases when you clone using the wizard, and one of the following servers crashes or reboots while the clone process is in progress, the clones might not get created correctly:

■ FileStore nodes

■ ESX host on which the clones are being created

■ vCenter Server

Even if the clones appear in the vCenter inventory as created, the clones GuestOS might not be able to boot.

Workaround

Delete all of the clones that were created when the servers crashed or were rebooted, and redo the wizard operation.

Error message does not always display when you select an incorrect cluster to clone (2372713)

In cases where multiple FileStore clusters are registered with the same Virtual Center, the Symantec Quick Clone Virtual Machine Wizard might not provide a warning that you selected an incorrect cluster to clone a golden image. This could happen if all of the FileStore clusters are exporting the same file system path, such as /mnt. Instead of an advanced warning that you selected the wrong cluster, you instead see an error on the final page of the wizard when the wizard attempts to clone the disks (vmdks) of the golden image. The error that displays is similar to the following example:

```
/mnt/goldvm/goldvm.vmdk no such file or directory...
```

Workaround

There is no workaround for this issue.

The installer output states, "Registering SVS license," even if you enabled keyless licensing

When installing, if you enable keyless licensing, the installer's output includes the following message:

```
Registering SVS license
```

Workaround: This message is harmless and can be ignored. The product will successfully install without a license key.

Cloning issue in a Japanese environment (2623471)

You might be unable to clone with Guest OS Customization or VMware View integration. While using the FileSnap wizard, options may be missing or in an error state.

Workaround

The workaround involves temporarily running the vCenter Server in the English locale.

To resolve this issue

1   From the vCenter Server, stop the following services using the Task Manager or services.msc:

    ```
    VMware VCMDS
    VMware VirtualCenter Server
    VMware VirtualCenter Management Webservices
    VMware vCenter Update Manager Services
    ```

2   Rename the following language directories `ja` to `ja-x`:

    ```
    C:\Program Files\VMware\Infrastructure\VirtualCenter Server\ja
    C:\Program Files\VMware\Infrastructure\VirtualCenter Server\locale\ja
    C:\Program Files\VMware\Infrastructure\VirtualCenter Server\imgres\ja
    ```

3   Restart the services from step 1.

4   Take FileSnap clones with customization and/or View integration using the FileSnap wizard.

5   To return the vCenter Server to the Japanese locale, reverse steps 1-3.

Issues related to I/O fencing

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

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

Solaris 10 SMF marks the service status based on the exit code of the start method for that service. The VxFEN start method executes the vxfen-startup script in the

background and exits with code 0. Hence, if the vxfen-startup script subsequently exits with failure then this change is not propagated to SMF. This behavior causes the `svcs` command to show incorrect status for VxFEN.

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

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

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

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

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

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

```
operation failed.
CPS ERROR V-97-1400-446 Un-authorized user cpsclient@system01,
domaintype vx; not allowing action
```

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

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

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

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

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

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

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

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

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

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

Workaround: Start VxFEN again after some time.

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 VirtualStore Administrator's Guide* for more details.

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

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

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

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

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

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

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

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

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

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

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

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

Unable to customize the 30-second duration (2551621)

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

Workaround: No workaround.

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

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

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

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

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

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

Workaround: You can use any of the following options:

- Before running the `configure_cps.pl` utility, change the default shell for root user to either KSH or bash.

- Perform the following steps after running the `configure_cps.pl` utility on each node of the cluster:

  - Manually remove the old credential directory or softlink. For example:

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

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

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

■ Start the CPSSG service group:

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

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

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

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

■ Rename cpsadm to cpsadmbin.

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

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

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

■ Provide the following permissions to the new file:

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

Issues related to installation

This section describes the known issues during installation and upgrade.

On Solaris 11, uninstalling an IPS package does not always remove the package's SMF services from the SMF database

On Solaris 11, after uninstalling an IPS package, some of the SMF services owned by the package that was uninstalled continue to exist in the SMF database. This issue is due to a defect in the Solaris 11 operating system.

For more information, refer to the Oracle bug ID#7104300 (Removing an external dependency manifest and its manifest the instance is masked).

This issue sometimes prevents you from reinstalling the same package. For example, if you uninstall the VRTSvxvm package, reinstalling the package completes, but some SMF services fail to get added to the repository, which leads to VxVM drivers not getting loaded, as well as vxconfigd and other VxVM daemons not starting.

Workaround: Update your Solaris 11 systems to Solaris 11 Support Repository Update 1.

On Solaris 11, uninstalling an IPS package moves some files to the $IMAGE_META/lost+found directory

After uninstalling an IPS package, some of the files related to the package get moved to the $IMAGE_META/lost+found directory. The value of $IMAGE_META generally is /var/pkg. These files are not part of the package, but reside in the directories created by the package.

One example is the log files. In the VRTSvxvm package, the CBR log files are kept in /var/adm/vx. During the uninstallation of the VRTSvxvm package, the following warning message displays:

```
The following unexpected or editable files and directories were
salvaged while executing the requested package operation; they
have been moved to the displayed location in the image:

var/adm/vx -> /var/pkg/lost+found/var/adm/vx-20120221T114835Z
usr/lib/vxvm/bin -> /var/pkg/lost+found/usr/lib/vxvm/bin-20120221T114835Z
etc/vx/vras -> /var/pkg/lost+found/etc/vx/vras-20120221T114835Z
```

Workaround: There is no workaround for this issue. This is Solaris 11 IPS behaviour.

Software limitations

VMware vSphere extension for VirtualStore limitations

The following are the software limitations for VMware vSphere extension for VirtualStore that are known in this release.

F5 usage is not supported for wizard refreshing (2362940)

F5 usage is not supported for wizard refreshing.

Workaround

To get new or refreshed data, it is important to restart the wizard and not use the F5 key.

Virtual machines with VMware Snapshots cannot be used as golden images (2514969)

Any virtual machine (or template) which has VMware Snapshots stored, cannot be used as a golden image for making clones with the FileSnap wizard. To use such virtual machines (or templates), first delete the Snapshots, then use the FileSnap wizard.

Limitations related to I/O fencing

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

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

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

Veritas Volume Manager software limitations

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

DMP and EMC PowerPath coexistence

EMC PowerPath (EMCPP) currently does not claim support for Solaris 11. Therefore, DMP and EMCPP coexistence is not supported in Solaris 11.

You cannot encapsulate the boot disk in Solaris 11

Encapsulation of the boot disk in Solaris 11 is not supported.

Documentation errata

The following sections cover additions or corrections for Document version: 6.0PR1.3 of the product documentation. These additions or corrections may be included in later versions of the product documentation that can be downloaded

from the Symantec Support website and the Symantec Operations Readiness Tools (SORT).

See the corresponding Release Notes for documentation errata related to that component or product.

See "Documentation" on page 37.

VirtualStore manual page

The following errata applies to the VirtualStore manual page.

The svsvmwadm -P and --vcport options are missing

The -P and --vcport options are missing from the svsvmwadm manual page. The following options and description should be present:

```
-P, --vcport     HTTPS port in the range 1-65535(443 default)
configured in VMware vCenter Server
```

Documentation

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

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

http://sort.symantec.com/documents

Documentation set

Table 1-5 lists the documentation for Veritas Storage Foundation Cluster File System High Availability.

Table 1-5　　　　Veritas Storage Foundation Cluster File System High Availability documentation

Document title	File name
Veritas Storage Foundation Cluster File System High Availability Release Notes	sfcfs_notes_60pr1_sol.pdf

Table 1-5 Veritas Storage Foundation Cluster File System High Availability documentation *(continued)*

Document title	File name
Veritas Storage Foundation Cluster File System High Availability Installation Guide	sfcfs_install_60pr1_sol.pdf
Veritas Storage Foundation Cluster File System High Availability Administrator's Guide	sfcfs_admin_60pr1_sol.pdf

Table 1-6 lists the documentation for Symantec VirtualStore.

Table 1-6 Symantec VirtualStore documentation

Document title	File name
Symantec VirtualStore Release Notes	virtualstore_notes_60pr1_sol.pdf
Symantec VirtualStore Installation and Configuration Guide	virtualstore_install_60pr1_sol.pdf
Symantec VirtualStore Administrator's Guide	virtualstore_admin_60pr1_sol.pdf

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

http://sort.symantec.com/documents

Manual pages

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

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

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

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

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

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

See the `man`(1) manual page.