Symantec™ Storage Foundation for Sybase ASE CE 6.1 Release Notes - Solaris

February 2015

Symantec

Symantec™ Storage Foundation for Sybase ASE CE Release Notes

Product version: 6.1

Document version: 6.1 Rev 4

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our 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 Storage Foundation for Sybase ASE CE Release Notes

This document includes the following topics:

About this document

This document provides important information about Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE) version 6.1 for Solaris. Review this entire document before you install or upgrade SF Sybase CE.

The information in the Release Notes supersedes the information provided in the product documents for SF Sybase CE.

This is "Document version: 6.1 Rev 4" of the *Symantec Storage Foundation for Sybase ASE CE 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)
- *Symantec Storage Foundation Cluster File System High Availability Release Notes* (6.1)

About Symantec Storage Foundation for Sybase ASE CE

Symantec Storage Foundation™ for Sybase® Adaptive Server Enterprise Cluster Edition (SF Sybase CE) by Symantec leverages proprietary storage management and high availability technologies to enable robust, manageable, and scalable deployment of Sybase ASE CE on UNIX platforms. The solution uses cluster file system technology that provides the dual advantage of easy file system management as well as the use of familiar operating system tools and utilities in managing databases.

SF Sybase CE integrates existing Symantec storage management and clustering technologies into a flexible solution which administrators can use to:

- Create a standard toward application and database management in data centers. SF Sybase CE provides flexible support for many types of applications and databases.
- Set up an infrastructure for Sybase ASE CE that simplifies database management while fully integrating with Sybase ASE CE clustering solution.
- Apply existing expertise of Symantec technologies toward this product.

The solution stack comprises the Symantec Cluster Server (VCS), Veritas Cluster Volume Manager (CVM), Veritas Cluster File System (CFS), and Symnatec Storage Foundation, which includes the base Veritas Volume Manager (VxVM) and Veritas File System (VxFS).

Benefits of SF Sybase CE

SF Sybase CE provides the following benefits:

- Use of a generic clustered file system (CFS) technology or a local file system (VxFS) technology for storing and managing Sybase ASE CE installation binaries.
- Support for file system-based management. SF Sybase CE provides a generic clustered file system technology for storing and managing Sybase ASE CE data files as well as other application data.
- Use of Cluster File System (CFS) for the Sybase ASE CE quorum device.
- Support for a standardized approach toward application and database management. A single-vendor solution for the complete SF Sybase CE software stack lets you devise a standardized approach toward application and database management. Further, administrators can apply existing expertise of Veritas technologies toward SF Sybase CE.
- Easy administration and monitoring of SF Sybase CE clusters using Veritas Operations Manager.
- Enhanced scalability and availability with access to multiple Sybase ASE CE instances per database in a cluster.
- Prevention of data corruption in split-brain scenarios with robust SCSI-3 Persistent Reservation (PR) based I/O fencing.
- Support for sharing all types of files, in addition to Sybase ASE CE database files, across nodes.
- Increased availability and performance using Symantec Dynamic Multi-Pathing (DMP). DMP provides wide storage array support for protection from failures and performance bottlenecks in the Host Bus Adapters (HBAs) and Storage Area Network (SAN) switches.

- Fast disaster recovery with minimal downtime and interruption to users. Users can transition from a local high availability site to a wide-area disaster recovery environment with primary and secondary sites. If a node fails, clients that are attached to the failed node can reconnect to a surviving node and resume access to the shared database. Recovery after failure in the SF Sybase CE environment is far quicker than recovery for a failover database.
- Support for block-level replication using VVR.

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:

Prepare for your next installation or upgrade	■ List product installation and upgrade requirements, including operating system versions, memory, disk space, and architecture. ■ Analyze systems to determine if they are ready to install or upgrade Symantec products and generate an Installation and Upgrade custom report. ■ 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. ■ 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. ■ List VCS and ApplicationHA agents, documentation, and downloads based on the agent type, application, and platform.
Identify risks and get server-specific recommendations	■ 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. ■ Display descriptions and solutions for thousands of Symantec error codes.

Improve efficiency

- Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDLs), documentation, product releases, Hardware Compatibility Lists (HCLs), and VCS/ApplicationHA agents.
- 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.
- List and download Symantec product documentation including product guides, manual pages, compatibility lists, and support articles.
- 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.
- Use a subset of SORT features from your iOS device. Download the application at:
  https://sort.symantec.com/mobile

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 SF Sybase CE 6.1

This section lists the changes in Symantec Storage Foundation for Sybase ASE CE 6.1.

Changes related to installation and upgrades

The product installer includes the following changes in SF Sybase CE 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 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 1-1.

Table 1-1 Deployment Server functionality

Feature	Description
Manage release images	■ View available Storage Foundation releases. ■ Download maintenance and hot fix release images from the Symantec Operations Readiness Tools (SORT) website into a repository. ■ Load the downloaded release image files from FileConnect and SORT into the repository. ■ View and remove release image files stored in the repository.

Table 1-1 Deployment Server functionality *(continued)*

Feature	Description
Check versions	■ Discovers packages and patches installed on designated systems and informs you of the product and version installed, including installed hot fixes. ■ Identify base, maintenance, and hot fix level upgrades to your system and download maintenance and hot fix releases. ■ Query SORT for the most recent updates.

Install or upgrade systems	■ Install or upgrade a release stored in the repository on selected systems.
	■ In release 6.1 and later:
	  ■ Install hot fix level releases.
	  ■ Install SFHA from any supported UNIX or Linux operating system to any other supported UNIX or Linux operating system.
	  ■ Automatically load the script-based installer hot fixes that apply to that release.

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, packages, 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 to I/O fencing

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

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*.

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*.

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*.

New SMF services avoid race conditions when you add or remove I/O fencing driver on Solaris 11

On Solaris 11, Symantec has added two new SMF services, 'vxfen-postinstall', and 'vxfen-preremove' to manage addition and removal of I/O fencing driver. With the addition of these new SMF services, the I/O fencing driver is added only during package installation and removed on package removal. The new SMF services avoid failure to install the I/O fencing driver during system restart.

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`.

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*.

Changes related to product name branding

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

Table 1-2 lists the rebranded Storage Foundation and High Availability Solutions products.

Table 1-2 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

System requirements

This section describes the system requirements for this release.

Supported Oracle VM Server for SPARC

Supported Oracle VM Server for SPARC (OVM) versions are OVM 2.0, OVM 2.1, OVM 2.2, OVM 3.0 and OVM 3.1.

For supported OS version for Oracle VM Server for SPARC, refer to *Oracle VM server for SPARC Release Notes*.

The version of the Oracle Solaris operating system (OS) that runs on a guest domain is independent of the Oracle Solaris OS version that runs on the primary domain. Therefore, if you run the Oracle Solaris 10 OS in the primary domain, you can still run the Oracle Solaris 11 OS in a guest domain. Likewise if you run the Oracle Solaris 11 OS in the primary domain, you can still run the Oracle Solaris 10 OS in a guest domain.

The only difference between running the Oracle Solaris 10 OS or the Oracle Solaris 11 OS on the primary domain is the feature difference in each OS.

Important preinstallation information for SF Sybase CE

Before you install SF Sybase CE, make sure that you have reviewed the following information:

- Preinstallation checklist for your configuration. Go to the SORT installation checklist tool. From the drop-down lists, select the information for the Symantec product you want to install, and click **Generate Checklist**.
- Hardware compatibility list for information about supported hardware: http://www.symantec.com/docs/TECH211575
- For important updates regarding this release, review the Late-Breaking News Technote on the Symantec Technical Support website: http://www.symantec.com/docs/TECH211540
- Sybase ASE CE documentation for additional requirements pertaining to your version of Sybase ASE CE.

Hardware requirements

Table 1-3 lists the hardware requirements for SF Sybase CE.

Table 1-3 Hardware requirements for basic clusters

Item	Description
SF Sybase CE systems	Two to four systems with two or more CPUs. For details on the additional requirements for Sybase ASE CE, see the Sybase ASE CE documentation.
DVD drive	A DVD drive on one of the nodes in the cluster.
Disk space	You can evaluate your systems for available disk space by running the product installation program. Navigate to the product directory on the product disc and run the following command: `# ./installsfsybasece -precheck node_name` For details on the additional space that is required for Sybase ASE CE, see the Sybase ASE CE documentation.
RAM	Each SF Sybase CE system requires at least 2 GB.
Network	Two or more private links and one public link. Links must be 100BaseT or gigabit Ethernet directly linking each node to the other node to form a private network that handles direct inter-system communication. These links must be of the same type; you cannot mix 100BaseT and gigabit. Symantec recommends gigabit Ethernet using enterprise-class switches for the private links. You can also configure aggregated interfaces.
Fiber Channel or SCSI host bus adapters	At least one additional SCSI or Fibre Channel Host Bus Adapter per system for shared data disks.

Supported Solaris 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.

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

Table 1-4 Supported operating systems

Operating systems	Levels	Chipsets
Solaris 10	Update 9, 10, and 11	SPARC

Supported Sybase ASE CE releases

SF Sybase CE supports Sybase ASE CE 15.5 only at time of publication.

For the latest information on the supported Sybase ASE CE database versions, see the following Technical Support TechNote:

http://www.symantec.com/docs/DOC4848

See the Sybase ASE CE documentation for more information.

Supported SF Sybase CE configurations

The following Sybase configuration options are required in an SF Sybase CE environment:

- Set SF Sybase CE fencing to "sybase" mode.
- Configure Sybase private networks on LLT links
- Set Sybase cluster membership to "vcs" mode.
- Configure Sybase instances under VCS control.

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 0x6000. 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, VRTSvxfs increases the values and modifies the `/etc/system` file with the required values. If the VRTSvxfs scripts increase the values, the installation proceeds as usual except that you must reboot and restart the installation program. A message displays if a reboot is required.

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:

For Solaris 10:
```
# echo "lwp_default_stksize/X" | mdb -k
lwp_default_stksize:
lwp_default_stksize:            6000

# echo "svc_default_stksize/X" | mdb -k
svc_default_stksize:
svc_default_stksize:            6000
```

If the values shown are less than 6000, 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:

For Solaris 10:
```
set lwp_default_stksize=0x6000
set rpcmod:svc_default_stksize=0x6000
```

Supported replication technologies for global clusters

SF Sybase CE supports the software replication technology Veritas Volume Replicator (VVR) for global cluster configurations.

Fixed issues

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

Issues fixed in SF Sybase CE 6.1

Table 1-5 lists the issues fixed in SF Sybase CE 6.1.

Table 1-5 Issues fixed in SF Sybase CE 6.1

Incident Number	Description
2615341	AutoFailOver = 0 attribute absent in the sample files at `/etc/VRTSagents/ha/conf/Sybase`.

I/O fencing fixed issues

Table 1-6 lists the issues fixed for I/O fencing

Table 1-6 I/O fencing fixed issues

Incident Number	Description
2858190	Cannot run the `vxfentsthdw` utility directly from the install media if the `VRTSvxfen` package is not installed on the system.

Known issues

This section covers the known issues in this release.

SF Sybase CE issues

This section lists the known issues in SF Sybase CE for this release.

Sybase Agent Monitor times out (1592996)

Problem: The Sybase Agent Monitor has issues of timing out, in cases where qrmutil reports delay.

The Sybase Agent monitor times out, if qrmutil fails to report the status to the agent within the defined MonitorTimeout for the agent.

Solution: If any of the following configuration parameters for Sybase Database is increased, it will require a change in its MonitorTimeout value:

- quorum heartbeat interval (in seconds)
- Number of retries

If the above two parameters are changed, Symantec recommends that the MonitorTimeout be set to a greater value than the following: ((number of retries + 1) * (quorum heartbeat interval)) + 5.

Installer warning (1515503)

Problem: During configuration of Sybase instance under VCS control, if the quorum device is on CFS and is not mounted, the following warning message appears on the installer screen:

```
Error: CPI WARNING V-9-40-5460 The quorum file /qrmmnt/qfile
cannot be accessed now. This may be due to a file system not being mounted.
```

The above warning may be safely ignored.

Unexpected node reboot while probing a Sybase resource in transition (1593605)

Problem: A node may reboot unexpectedly if the Sybase resource is probed while the resource is still in transition from an online to offline state.

Normally the monitor entry point for Sybase agent completes with 5-10 seconds. The monitor script for the Sybase agent uses the qrmutil binary provided by Sybase. During a monitor, if this utility takes longer time to respond, the monitor entry point will also execute for longer duration before returning status.

Resolution: During the transition time interval between online and offline, do not issue a probe for the Sybase resource, otherwise the node may reboot.

Unexpected node reboot when invalid attribute is given (2567507)

Problem: A node may reboot unexpectedly if the Home, Version, or Server attributes are modified to invalid values while the Sybase resources are online in VCS.

Resolution: Avoid setting invalid values for the Home, Version, or Server attributes while the Sybase resources are online in VCS, to avoid panic of the node.

Bus error while stopping the ports (2358568)

Problem: When the `hastop -local` command or the `hastop -all` command is issued, the `fuser -kill` command is issued on the mounted Sybase mount point. This results in bus error and a core dump, though the ports stop cleanly.

Resolution: Before issuing the `hastop -local` command or the `hastop -all` command, ensure that the `uafstartup.sh` script is stopped, so that the `fuser -kill` command is not issued on the mounted Sybase mount point.

Installation known issues

This section describes the known issues during installation and upgrade.

On Solaris 10 xprtld will not be started if user use jumpstart to install product (3325954)

If you install the operating system plus the Symantec product using the JumpStart method and after installation, reboot the machine then configure and start the product, all the processes will be started except for `xprtld` process.

Workaround:

After reboot, manually execute the following command to start `xprtld`:

```
# /opt/VRTSsfmh/adm/xprtldctrl start
```

Stopping the installer during an upgrade and then resuming the upgrade might freeze the service groups [2574731]

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

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

To unfreeze the service groups manually

1 List all the frozen service groups:

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

2 Unfreeze all the frozen service groups:

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

After Live Upgrade to Solaris 10 Update 10, boot from alternate boot environment may fail (2370250)

If your setup involves volumes in a shared disk group that are mounted as CFS in a cluster, then during Live Upgrade using the `vxlustart` command from any supported Solaris version to Solaris 10 Update 10, boot from an alternate boot environment may fail.

Workaround: Run the `vxlufinish` command. Before rebooting the system, manually delete the entries of all the volumes of shared disks that are mounted as CFS in the `/altroot.5.10/etc/vfstab` directory.

Flash Archive installation not supported if the target system's root disk is encapsulated

Symantec does not support SF Sybase CE installation using Flash Archive if the target system's root disk is encapsulated.

Make sure that the target system's root disk is unencapsulated before starting the installation.

On Solaris 10, a flash archive installed through JumpStart may cause a new system to go into maintenance mode on reboot (2379123)

If a Flash archive is created on a golden host with encapsulated root disks, when this Flash archive is installed onto another host through JumpStart, the new system may go to maintenance mode when you initially reboot it.

This problem is caused by the predefined root disk mirror in the Flash archive. When the archive is applied to a clone system, which may have different hard drives, the newly cloned system may get stuck at root disk mirroring during reboot.

Workaround: Create the Flash archive on a golden host with no encapsulated root disks. Run `vxunroot` to clean up the mirrored root disks before you create the Flash archive.

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

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

This issue will be resolved in a later release.

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.

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
```

I/O fencing known issues

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.

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.

Stale .vxfendargs file lets hashadow restart vxfend in Sybase mode (2554886)

When I/O fencing is configured in customized mode, vxfend, the user mode daemon of I/O fencing, creates the `/opt/VRTSvcs/lock/.vxfendargs` file. VCS uses this file to restart the vxfend daemon when it gets killed. However, VCS does not use this file when I/O fencing is configured in Sybase mode. This file is not removed from the system when I/O fencing is unconfigured.

If user configures I/O fencing in Sybase mode and an old `/opt/VRTSvcs/lock/.vxfendargs` file is present in the system from an earlier configuration of I/O fencing in customized mode, then VCS attempts to restart the vxfend daemon every time it is killed. This interferes with the functioning of I/O fencing in the Sybase mode.

Workaround: Before you configure I/O fencing in Sybase mode, delete the `/opt/VRTSvcs/lock/.vxfendargs` file if it is present in the system.

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.

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.

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 30.

Only one Sybase instance is supported per node

In a Sybase ASE CE cluster, SF Sybase CE supports only one Sybase instance per node.

SF Sybase CE is not supported in the Campus cluster environment

SF Sybase CE does not support the Campus cluster. SF Sybase CE supports the following cluster configurations. Depending on your business needs, you may choose from the following setup models:

- Basic setup
- Secure setup
- Central management setup
- Global cluster setup

See the *Installation Guide* for more information.

Hardware-based replication technologies are not supported for replication in the SF Sybase CE environment

You can use Veritas Volume Replicator (VVR), which provides host-based volume replication. Using VVR you can replicate data volumes on a shared disk group in SF Sybase CE. Hardware-based replication is not supported at this time.

SF Sybase CE installation is not supported by Web installer

SF Sybase CE does not support the Web-based installer at this time. You can use one of the following methods to install and configure SF Sybase CE.

- Interactive installation and configuration using the script-based installer
- Silent installation using the response file
- Installation using the JumpStart script file

See the *Installation Guide* for more information.

Limitations related to I/O fencing

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

Preferred fencing limitation when VxFEN activates RACER node re-election

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

Stopping systems in clusters with I/O fencing configured

The I/O fencing feature protects against data corruption resulting from a failed cluster interconnect, or “split brain.” See the *Symantec Cluster Server Administrator's Guide* for a description of the problems a failed interconnect can create and the protection I/O fencing provides.

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

placing the SCSI-3 PR keys on data disks and similar registrations on CP server. The VCS administrator must be aware of several operational changes needed when working with clusters protected by I/O fencing. Specific shutdown procedures ensure keys are removed from coordination points and data disks to prevent possible difficulties with subsequent cluster startup.

Using the reboot command rather than the shutdown command bypasses shutdown scripts and can leave keys on the coordination points and data disks. Depending on the order of reboot and subsequent startup events, the cluster may warn of a possible split brain condition and fail to start up.

Workaround: Use the shutdown -r command on one node at a time and wait for each node to complete shutdown.

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

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

Documentation

Product guides are available in the PDF format on the software media in the `/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.

Note: The GNOME PDF Viewer is unable to view Symantec documentation. You must use Adobe Acrobat to view the documentation.

Symantec Storage Foundation for Sybase ASE CE documentation

Table 1-7 lists the documentation for Symantec Storage Foundation for Sybase ASE CE.

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

See Table 1-11 on page 34.

Table 1-7 Symantec Storage Foundation for Sybase ASE CE documentation

Document title	File name	Description
Symantec Storage Foundation for Sybase ASE CE Release Notes	sfsybasece_notes_61_sol.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
Symantec Storage Foundation for Sybase ASE CE Installation and Configuration Guide	sfsybasece_install_61_sol.pdf	Provides information required to install and configure the product.
Symantec Storage Foundation for Sybase ASE CE Administrator's Guide	sfsybasece_admin_61_sol.pdf	Provides information required for administering the product.

Symantec Storage Foundation Cluster File System High Availability documentation

Table 1-8 lists the documentation for Symantec Storage Foundation Cluster File System High Availability.

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

See Table 1-11 on page 34.

Table 1-8 Symantec Storage Foundation Cluster File System High Availability documentation

Document title	File name	Description
Symantec Storage Foundation Cluster File System High Availability Release Notes	sfcfs_notes_61_sol.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
Symantec Storage Foundation Cluster File System High Availability Installation Guide	sfcfs_install_61_sol.pdf	Provides information required to install the product.
Symantec Storage Foundation Cluster File System High Availability Administrator's Guide	sfcfs_admin_61_sol.pdf	Provides information required for administering the product.

Table 1-9 lists the documents for Symantec Cluster Server.

Table 1-9 Symantec Cluster Server documentation

Title	File name	Description
Symantec Cluster Server Release Notes	vcs_notes_61_sol.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
Symantec Cluster Server Installation Guide	vcs_install_61_sol.pdf	Provides information required to install the product.
Symantec Cluster Server Administrator's Guide	vcs_admin_61_sol.pdf	Provides information required for administering the product.
Symantec Cluster Server Bundled Agents Reference Guide	vcs_bundled_agents_61_sol.pdf	Provides information about bundled agents, their resources and attributes, and more related information.
Symantec Cluster Server Agent Developer's Guide (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.

Table 1-9 Symantec Cluster Server documentation *(continued)*

Title	File name	Description
Symantec Cluster Server Application Note: Dynamic Reconfiguration for Oracle Servers (This document is available online only.)	vcs_dynamic_reconfig_61_sol.pdf	Provides information on how to perform dynamic reconfiguration operations on VCS clustered system domains of Oracle servers.
Symantec Cluster Server Agent for DB2 Installation and Configuration Guide	vcs_db2_agent_61_sol.pdf	Provides notes for installing and configuring the DB2 agent.
Symantec Cluster Server Agent for Oracle Installation and Configuration Guide	vcs_oracle_agent_61_sol.pdf	Provides notes for installing and configuring the Oracle agent.
Symantec Cluster Server Agent for Sybase Installation and Configuration Guide	vcs_sybase_agent_61_sol.pdf	Provides notes for installing and configuring the Sybase agent.

Table 1-10 lists the documentation for Symantec Storage Foundation.

Table 1-10 Symantec Storage Foundation documentation

Document title	File name	Description
Symantec Storage Foundation Release Notes	sf_notes_61_sol.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
Symantec Storage Foundation Installation Guide	sf_install_61_sol.pdf	Provides information required to install the product.
Symantec Storage Foundation Administrator's Guide	sf_admin_61_sol.pdf	Provides information required for administering the product.
Veritas File System Programmer's Reference Guide (This document is available online only.)	vxfs_ref_61_sol.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 1-11 lists the documentation for Symantec Storage Foundation and High Availability Solutions products.

Table 1-11 Symantec Storage Foundation and High Availability Solutions products documentation

Document title	File name	Description
Symantec Storage Foundation and High Availability Solutions—What's new in this release (This document is available online.)	sfhas_whats_new_61_unix.pdf	Provides information about the new features and enhancements in the release.
Symantec Storage Foundation and High Availability Solutions Getting Started Guide	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.
Symantec Storage Foundation and High Availability Solutions Solutions Guide	sfhas_solutions_61_sol.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.
Symantec Storage Foundation and High Availability Solutions Virtualization Guide (This document is available online.)	sfhas_virtualization_61_sol.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.
Symantec Storage Foundation and High Availability Solutions Disaster Recovery Implementation Guide (This document is available online.)	sfhas_dr_impl_61_sol.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.
Symantec Storage Foundation and High Availability Solutions Replication Administrator's Guide	sfhas_replication_admin_61_sol.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.
Symantec Storage Foundation and High Availability Solutions Troubleshooting Guide	sfhas_tshoot_61_sol.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