Symantec™ Storage Foundation and High Availability Solutions 6.2 What's new in this release - AIX, Linux, Solaris

March 2015

Symantec

What's New In This Release

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

Product version: 6.2

Document version: 6.2 Rev 2

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_apj@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

What's new in this release

This document includes the following topics:

About this document

This document covers the major new features, enhancements, and changes that are introduced in 6.2 for the following Symantec Storage Foundation and High Availability Solutions products:

- Symantec Dynamic Multi-Pathing (DMP)
- Symantec Storage Foundation (SF)

- Symantec Storage Foundation and High Availability (SFHA)
- Symantec Storage Foundation Cluster File System High Availability (SFCFSHA)
- Symantec Cluster Server (VCS)
- Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)
- Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE)
- Symantec ApplicationHA
- Common Product Installer (CPI) – Installation and Upgrades

Review the following notes before you use the document:

Note: The new features and enhancements listed in this document apply to AIX, Linux, and Solaris unless mentioned otherwise. If a new feature or enhancement applies to a particular platform, it is indicated at the beginning of the section.

Note: The Administrator and Installation Guide references provided in this document pertain to the Symantec Storage Foundation and High Availability Solutions product installed in your environment.

For a complete list of changes, see the appropriate product Release Notes.

Featured product enhancements in 6.2

Symantec Storage Foundation and High Availability Solutions products 6.2 include the following major new features:

Caching on Solid-State Drives on AIX and Solaris	■ Storage Foundation SmartIO See "SmartIO: Support for caching on Solid-State Drives" on page 13.
Flexible Storage Sharing on AIX and Solaris	■ Cluster Volume Manager (CVM) in Storage Foundation Cluster File System High Availability (SFCFSHA) See "Support for Flexible Storage Sharing" on page 29.
Centralized installations using the Deployment Server	■ See "Support for centralized installations using the Deployment Server" on page 9.
Support for Atomic writes on Linux	■ Storage Foundation (SF) See "Support for atomic writes" on page 15.

Changes related to installation and upgrades

The product installer includes the following changes in 6.2.

Connecting to the SORT website through a proxy server

The product installer connects to the Symantec Operations Readiness Tools (SORT) website for several purposes, such as downloading the latest installer patches, and uploading installer logs. Deployment Server can connect to SORT to automatically download Maintenance or Patch release images. In this release, before running the product installer or Deployment Server, you can use the following proxy settings to connect to SORT through proxy servers:

```
# https_proxy=http://proxy_server:port
# export https_proxy
# ftp_proxy=http://proxy_server:port
# export ftp_proxy
```

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 platform (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
Install or Upgrade systems with Install Bundle and Install Template	■ Install or upgrade systems with an Install Bundle. ■ Install packages on systems based on the information stored in the Install Template.
Define or modify Install Bundles	Define or modify Install Bundles and save them using the Deployment Server.
Create Install Templates	Discover installed components on a running system that you want to replicate on new systems.

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

Feature	Description
Connecting the Deployment Server to SORT using a proxy server	Use a proxy server, a server that acts as an intermediary for requests from clients, for connecting the Deployment Server to the Symantec Operations Readiness Tools (SORT) website.
Platform Filtering	On the Set Preference menu, choose Selected Platforms to filter the platforms that are currently being used in the deployment environment.

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

See the *Installation Guide* for more information.

Symantec Storage Foundation and High Availability Solutions gets installed in secure mode by default

Symantec Storage Foundation and High Availability Solutions gets installed in secure mode by default. You are advised to install SFHA Solutions in secure mode to be able to control guest user access to secure clusters and encrypt communication between SFHA Solutions components. You can choose the non-secure mode during installation; however, the product installer warns you during the installation with the following message:

```
Symantec recommends that you install the cluster
in secure mode. This ensures that communication between
cluster components is encrypted and cluster information
is visible to specified users only.
```

The upgrade from non-secure mode continues to happen in non-secure mode. The upgrade from secure mode advises you to control user access to secure clusters.

Package updates

This topic applies to Linux.

The following lists the package changes in this release.

- The `VRTSlvmconv` package has been merged with the `VRTSvxvm` package.There is no separate package for `lvmconvert` now.

- The VRTSvxvm package adds dependency for bc -1.06.95-13.el7.x86_64, pcre-8.32-12.el7.i686 (pcre(x86-32)), and xz-libs-5.1.2-8alpha.el7.i686 (xz-libs(x86-32)) packages on RHEL 7 distribution. Newly required dependent package for VRTSvxvm is:

Package name	Version	Architecture
bc	Default version available with RHEL7	x86_64
pcre	Default version available with RHEL7	el7.i686
xz-libs	Default version available with RHEL7	el7.i686

For more information, see the *Installation Guide* for the complete list of packages for this release.

Support for installation using the Red Hat Satellite server

This topic applies to Linux.

You can install SFHA Solutions using the Red Hat Satellite server. Red Hat Satellite is supported for Red Hat Enterprise Linux 6 (RHEL6) and Red Hat Enterprise Linux 7 (RHEL7). You can install packages and rolling patches on the systems which the Red Hat Satellite server manages.

In a Red Hat Satellite server, you can manage the system by creating a channel. A Red Hat Satellite channel is a collection of software packages. Using channels, you can segregate the packages by defining some rules.

Behavioral changes in RHEL 7 as compared with previous releases

This topic applies to Linux.

Note the following behavioral changes in RHEL 7:

- The XFS file system is not supported for the Root Disk Encapsulation (RDE) feature.
  RDE is not supported if the root partition is mounted with the XFS file system.
- Enclosure-based naming (EBN) is not supported for RDE.
  RDE, mirroring, splitting, and joining operations on root disks are not supported if the naming scheme is set to EBN.

Support for upgrading SFHA Solutions using the web-based installer for Solaris 10 Live Upgrade

This topic applies to Solaris.

You can use the Symantec web-based installer to upgrade SFHA Solutions as part of the Live Upgrade.

On a node in the cluster, run the web-based installer on the DVD to upgrade SFHA Solutions on all the nodes in the cluster.

Run the web-based installer on the DVD to upgrade SFHA Solutions.

The program uninstalls the existing version of SFHA Solutions on the alternate boot disk during the process. At the end of the process, SFHA Solutions 6.2 is installed on the alternate boot disk.

Support for setting up ssh and rsh connection using the pwdutil.pl utility

The password utility, `pwdutil.pl`, is bundled in the 6.2 release under the scripts directory. The users can run the `pwdutil.pl` utility to set up the `ssh` and `rsh` connection automatically.

New `ProcessOnOnly` resource added to VCS configuration file during upgrades

During upgrade, the following new `ProcessOnOnly` resource is added to the VCS configuration file:

```
ProcessOnOnly vxattachd (
   Critical = 0
   Arguments = "- /usr/lib/vxvm/bin/vxattachd root"
   PathName = "$SH"
   RestartLimit = 3
   )
```

Upgrade Symantec Cluster Server online, while keeping your applications online

You can perform an online upgrade of Symantec Cluster Server using the installer, while keeping your applications online. Your applications can run seamlessly when the upgrade is in progress. The upgrade behavior otherwise remains same as the one in the previous release. Note that the application monitoring does not happen as long as the upgrade is in progress.

Release level terminology changes

With the 6.2 release, terms that are used to describe patch-based releases have changed as follows:

Table 1-2 Release level terminology changes

Pre 6.0.1	6.0.x, 6.1, 6.1.x	6.2 and forward	Status	Available from
P-Patch	Public hot fix	Patch	Official	SORT
Hot fix	Private hot fix	Hot fix	Unofficial	Customer support

Official patch releases are available from SORT. This release was previously referred to as a P-Patch or a Public hot fix and is now referred to as a Patch. Unofficial patch releases are available from customer support. Hot fix is the only unofficial patch release.

Changes related to Symantec Dynamic Multi-Pathing (DMP)

This section describes changes in this release related to Symantec DMP.

DMP includes the new features and changes introduced in 6.2 of the underlying products:

See "Changes related to installation and upgrades" on page 9.

See the *Symantec Dynamic Multi-Pathing Release Notes* for more details.

Changes related to Symantec Storage Foundation (SF)

Symantec Storage Foundation includes the following changes in 6.2:

SmartIO: Support for caching on Solid-State Drives

This topic applies to AIX and Solaris.

The SmartIO feature of Storage Foundation and High Availability Solutions (SFHA Solutions) enables data efficiency on your solid-state devices through I/O caching. Using SmartIO to improve efficiency, you can optimize the cost per I/O per second (IOPS). SmartIO does not require in-depth knowledge of the hardware technologies

underneath. SmartIO uses advanced, customizable heuristics to determine what data to cache and how that data gets removed from the cache. The heuristics take advantage of SFHA Solutions' knowledge of the characteristics of the workload.

SmartIO supports read and write-back caching for Veritas File System (VxFS) mounted on Veritas Volume Manager (VxVM) volumes, in several caching modes and configurations.

- Read caching for applications running on VxVM volumes
- Read caching for applications running on VxFS file systems
- Write-back caching on applications running on VxFS file systems
- Database caching on VxFS file systems
- Database caching on VxVM volumes

To use SmartIO, you set up a cache area on the target device. You can do this task simply with one command, while the application is online. When the application issues an I/O request, SmartIO checks to see if the I/O can be serviced from the cache. As applications access data from the underlying volumes or file systems, certain data is moved to the cache based on the internal heuristics. Subsequent I/Os are processed from the cache.

You can also customize which data is cached, by adding advisory information to assist the SmartIO feature in making those determinations.

See the *Symantec™ Storage Foundation and High Availability Solutions SmartIO for Solid State Drives Solutions Guide* for details.

Support for SmartIO caching and vMotion in the VMware guest

This topic applies to Linux.

Starting with release 6.1, Storage Foundation and High Availability (SFHA) Solutions supported SmartIO caching when the SFHA Solutions product was installed in the VMware guest. In this configuration, the Solid State Devices (SSD) were local to the host, so vMotion operations could not be supported.

Starting in release 6.2, SFHA Solutions supports the vMotion operations and SmartIO within the VMware guests. This functionality is enabled by a no-cost, no-license configuration of Dynamic Multi-Pathing (DMP) for VMware in ESXi hosts.

In this configuration, DMP for VMware enables the pooling of locally attached devices such as SSDs at the ESXi host layer. The aggregation of the local devices is called SmartPool. From the SmartPool, you can provision SmartDisks to be used as caching areas by SmartIO in the ESXi guests running SFHA. By dividing the SmartPool into several SmartDisks, you can share the caching storage across multiple virtual machines. Using SmartPools gives you the flexibility to move virtual

machines across ESXi hosts while SmartIO caching is in progress. Although each host has its own SSD, you can configure each host to have a comparable view of the SmartDisk. When you use vMotion to migrate the virtual machines that have Storage Foundation running, SmartIO shuts down the cache on the source node and restarts the cache on the target host. SmartIO caching stays online during the migration. You can dynamically resize the SmartPool by adding or removing storage devices to the SmartPool.

You can install and use the no-license mode regardless of whether you are using DMP for VMware to manage storage multi-pathing in the host. If you plan to use DMP for VMware for multi-pathing in the host, you must have the appropriate license.

For more information, see the *Storage Foundation and High Availability Solutions Virtualization Guide for VMware ESXi*.

Support for atomic writes

This topic applies to Linux.

The Storage Foundation 6.2 release supports atomic write operations on RHEL6 on Fusion-io devices. Atomic write capable devices ensure that all blocks in write I/O operation (which may span multiple sectors) either pass or fail. If a write fails in-between, the storage reverts back to old data.

Atomic write resolves a problem of indeterminate status of failed writes that often requires two-part write – one write to an update log buffer and the other write on actual data volumes. Enabling atomic write eliminates the writes on the log buffer, which in turn results in a better performance.

Storage Foundation lets you configure the atomic write support when you create a Veritas Volume Manager (VxVM) volume on a device that has atomic write capability. The atomic write I/O size of an atomic write capable volume is 16 KB.

While creating an atomic write capable volume, VxVM ensures that all underlying subdisks are aligned to the 16 KB boundary. Atomic write capable volumes can span multiple atomic write enabled devices, but I/O crossing atomic write boundary is not supported.

Atomic write is supported on raw VxVM volumes as well as on VxFS configured on VxVM volumes.

For information about using the Storage Foundation atomic write I/O feature with MySQL, see the *Symantec Storage Foundation and High Availability Solutions Solutions Guide*.

Support for Red Hat Enterprise Virtualization Environment (RHEV)

This topic applies to Linux.

In RHEV environments, Symantec Storage Foundation can be configured as the backend storage for guest virtual machines. Symantec provides the `rhevadm` utility on RHEV Manager to configure storage for virtual machines. With SF as backend storage, you can leverage Flexible Shared Storage (FSS) feature to commission commodity hardware in place of costlier storage arrays. Veritas Volume Replicator (VVR) and Veritas File Replicator (VFR) provide volume and file level replication which enables you to perform disaster recovery of virtual machines.

Support for Red Hat Enterprise Linux (RHEL) 7 platform

This topic applies to Linux.

Support for RHEL 7 is added in this release. As part of this support, there is also an addition of new package VRTSveki. This package will be responsible for inter module communication across all kernel modules in the SFHA Solutions stack.

Note: SmartIO with Oracle on RHEL 7 (and the Oracle plugin for SmartIO) is not supported.

Changes related to Veritas Volume Manager

Layered volume enhancements for recovery and snapshots

In this release, a new enhancement is done for layered volumes so that when storage disconnection and subsequent reconnection happen, only inconsistent regions in the affected sub-volume are synchronized using the FastResync feature. In case of a storage failure, the mirror of the sub-volume on that storage will be detached and the future IOs on the sub-volume will be tracked by the DCO associated with the parent volume. When such a detached mirror is reattached after restoring storage connectivity, only regions that are inconsistent in the mirror would be synchronized using the FastResync feature.

Prior to this release, for a layered volume, if the storage within a mirror of a sub-volume became inaccessible, it led to full synchronization of that mirror when the storage was reconnected.

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

Read policy enhancement

In this release, to optimize the read performance, changes have been made in the plex read policies on VxVM volumes. When there are more than one mirror available to serve the read IO, VxVM will select the set of mirrors that will provide the optimal performance and round robin between those. In selecting the set of mirrors, the

internal logic will take into account various factors such as site locality, disk connectivity, media type, layout(striping), etc. You can override the logic and set any plex as the preferred mirror or set a round-robin read policy to round robin between all the mirrors of a volume.

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

Changes in default layout of cachearea volume used by SmartIO

This topic applies to Linux.

When cachearea is created on multiple devices, stripe layout is used by default instead of concat for creating the cachearea volume. A new option is added to sfcache CLI to override this behavior.

Changes in array names for Fusion-io devices

Prior to this release, the generic array name, fusionio, was used for all Fusion-io devices. Starting in this release, the array name indicates the type of Fusion-io card. For example, the ioDrive cards display names such as fiodrive0_0.

Use the `vxdisk list` command to display the array name.

For example:

```
# vxdisk list

fiodrive0_0  auto:cdsdisk    -            -            online ssdtrim
fiodrive0_1  auto:cdsdisk    -            -            online ssdtrim
```

Changes related to Veritas File System

There are no changes related to VxFS in this release.

Changes related to SFDB tools

The following sections describe the changes related to Storage Foundation for Databases (SFDB) tools in 6.2.

Support for multitenant databases

This topic applies to AIX, Linux, and Solaris.

SFDB tools support operations on Oracle 12c multitenant databases. The SFDB tools do not support operations on individual Pluggable Databases (PDB).

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

Support for DB2 configurations

This topic applies to AIX and Linux.

In this release, SFDB tools support DB2 10.5 release.

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

Device name format changes in RHEL 7 environments after encapsulation

This topic applies to Linux.

With RHEL 7, the format of volumes in the `/etc/fstab` file after root disk encapsulation has changed.

Table 1-3 lists the changes in RHEL 7 environments.

Table 1-3 Volume formats changes in RHEL 7 environments

Before RHEL 7	With RHEL 7
Volume format: `/dev/vx/dsk/bootdg/<volume>`	Volume format: `/dev/vx_dsk_bootdg_<volume>`

Contents of `/etc/fstab` file where the rootdisk has two partitions, namely, `/` and `swap`:
 	
`# cat /etc/fstab`
 	
`/dev/vx/dsk/bootdg/rootvol \`
`/ ext4 defaults 1 1`
`/dev/vx/dsk/bootdg/swapvol \`
`swap swap defaults 0 0`
 	
`#NOTE: volume rootvol (/) \`
`encapsulated partition sda1`
`#NOTE: volume swapvol (swap) \`
`encapsulated partition sda2`
	Contents of `/etc/fstab` file where the rootdisk has two partitions, namely, `/` and `swap`:
	
	`# cat /etc/fstab`
	
	`/dev/vx_dsk_bootdg_rootvol \`
	`/ ext4 defaults 1 1`
	`/dev/vx_dsk_bootdg_swapvol \`
	`swap swap defaults 0 0`
	
	`#NOTE: volume rootvol (/) \`
	`encapsulated partition sda1`
	`#NOTE: volume swapvol (swap) \`
	`encapsulated partition sda2`

Note: Though the format of the device names in the `/etc/fstab` has changed, there is no change in the output of the `mount` utility. The `mount` utility still displays the mounted volumes in the old format.

Changes related to Symantec Cluster Server (VCS)

The following sections contain changes related to VCS kernel components such as LLT, GAB, and I/O fencing, and clusters in secure mode.

For more information on changes related to VCS, see the *Symantec Cluster Server Release Notes*.

Attributes introduced in VCS 6.2

The following section describes the attributes introduced in VCS 6.2.

Cluster level attributes

DefaultGuestAccess	Enables guest access for any authenticated user to the secure cluster.
GuestGroups	Contains a list of user groups that have guest access.

LDom agent attributes

These attributes are applicable on Solaris

Meter	Defines the meters based on which the failover decision is taken for the service group containing the LDom resource.
MeterControl	Defines the interval after which meter entry point should get called.
MeterTimeout	The maximum time for the meter entry point to complete.
AvailableMeters	Defines the meters that the agent supports.
MeterRetryLimit	Defines the number of times the meter operation can be retried before it succeeds.
MeterRegList	It is an ordered list of attributes. If MeterRegList attribute or any attribute that are defined in MeterRegList is changed then the meter entry point is called immediately.

LPAR agent attributes

These attributes are applicable on AIX.

DROpts	Stores the primary and disaster recovery network configuration for the LPAR.

SFCache agent attributes

CacheArea	Specifies the name of the cache area.
CacheMode	Specifies the caching mode.
CacheFaultPolicy	Specifies the action to be performed in case of a cache fault.
CacheObjectName	Specifies the cache object name; it can be a mount point or disk group/volume.
FaultOnMonitorTimeouts	Defines whether VCS interprets the Monitor timeout as a resource fault. By default, the FaultOnMonitorTimeouts attribute is set to 4, but the SFCache agent overrides this value and sets it to 0.
NumThreads	Number of threads that are used within the agent process for managing resources. This number does not include the number of threads that are used for other internal purposes.

IP agent attributes

These attributes are applicable on Solaris.

IpadmIfProperties	Interface properties for the `ipadm set-ifprop` command. IpadmIfProperties attribute is applicable for Solaris 11 only. On Solaris 10, this attribute value is ignored.
IpadmAddrProperties	Address properties for the `ipadm set-addrprop` command. IpadmAddrProperties attribute is applicable for Solaris 11 only. On Solaris 10, this attribute value is ignored.

Resource level attributes

This attribute is appliable on Solaris.

Utilization	The virtual machine agent meters the CPU and memory requirement of the virtual machine and populates this attribute value for the virtual machine resource.

System attributes

These attributes are applicable on Solaris.

ServerAvailableCapacity	The HostMonitor agent meters the free CPU and memory on the physical server which are available to other virtual machines and populates this attribute.
ServerAvailableForecast	The HostMonitor agent forecasts the free CPU and memory of the physical server and populates this attribute value.
ServerCapacity	The HostMonitor agent meters the total CPU and memory of the physical server and populates this attribute value.
ServerReservedCapacity	This is an internal attribute populated by the VCS engine.

NFS agent attributes:

This attribute is applicable on Linux.

Port	Specifies the list of ports for NFS daemons. The NFS and NFSRestart agents use this attribute to ensure that the NFS daemons are running using the specified port.

Oracle agent attributes:

PDBName	This attribute must be configured for pluggable database (PDB) and the value should be set for a PDB database name. Do not set this attribute for traditional and container (CDB) database.

Mount agent attributes:

CacheRestoreAccess	Determines whether to perform restore access operation or not. This attribute is applicable only if: ■ File system type is VxFS. ■ Writeback caching is enabled for the SmartIO feature.

Cluster Manager Java GUI support consideration

The Cluster Manager Java GUI is End of Life but continues to be supported by Symantec to ensure that it works with the core clustering solutions of VCS and ApplicationHA in Linux and Windows environments. The Java GUI remains available for download with support for all VCS features available in pre-6.0 releases. Customers can manage service groups, generate new configurations, and perform other traditional cluster management operations. The Java GUI will be supported only on the Linux and Windows platforms.

Additional feature capabilities and platform support added in VCS 6.0 and later releases are available exclusively through Veritas Operations Manager (VOM). Symantec recommends the use of VOM to manage clusters and for all advanced capabilities.

Platform support introduced in this release

The following platform support is introduced in this release.

Support for Oracle Linux Unbreakable Enterprise Kernel

This topic applies to Linux.

VCS is enhanced to support Oracle Linux 6 Update 4 and 5 on Unbreakable Enterprise Kernel Release 2. Earlier, VCS supported Oracle Linux with RHEL compatible kernel only.

VCS 6.2 supports RHEL7

This topic applies to Linux.

RHEL7 platform support is introduced in this release. VRTSveki package will be shipped on RHEL 7 from VCS 6.2.

Note: DiskReservation agent will not be supported on RHEL7

Changes related to virtualization support in VCS

Symantec Cluster Server supports RHEV 3.4

This topic applies to Linux.

Symantec Cluster Server 6.2 support RHEV version 3.4.

VCS 6.2 will no longer support RHEV version 3.1/3.2.

Disaster recovery support for LPARs using VCS

This topic applies to AIX.

You can now configure disaster recovery (DR) for LPARs. You can replicate the `rootvg` of the LPAR to a DR site using a replication technology, such as Hitachi TrueCopy, EMC SRDF, and so on. VCS replication agents manage the replication configuration and the VCS LPAR agent supports network reconfiguration when hypervisors are separated by geographical distances.

Changes to the VCS engine

AdaptiveHA enhancement (virtual machine service group)

This topic is applicable to Solaris.

In a virtualized environment, VCS monitors and forecasts the available capacity of the physical server in terms of SCPU and SMem. For a virtual machine service group (VMSG) if you set FailOverPolicy (service group attribute) to BiggestAvailable, AdaptiveHA enables VCS to dynamically select the biggest available target physical server to online, switch, and failover the VMSG.

The following new attributes have been introduced:

- ServerAvailableCapacity
- ServerAvailableForecast
- ServerCapacity
- ServerReservedCapacity
- Utilization

For more information, refer to the *Administrator's Guide*.

New environment variables

In this release, the following VCS environment variables have been introduced:

- VCS_CONN_INIT_QUOTA
- VCS_CONN_HANDSHAKE_TIMEOUT

For more information, refer to the *Administrator's Guide*.

Atleast resource dependency

A new type of resource dependency has been introduced in this release wherein a parent resource can depend on a set of child resources. The parent resource is brought online or remains online only if a minimum number of child resources in this resource set are online. The system creates a set of child IP resources and the application resource depends on this set.

For example, if an application depends on five IPs and if this application has to be brought online or has to remain online, at least two IPs must be online. If two or more IP resources come online, the application attempts to come online. If the number of online resources falls below the minimum requirement, resource fault is propagated up the resource dependency tree.

For more information, refer to the *Administrator's Guide*.

Changes to VCS bundled agents

This section describes changes to the bundled agents for VCS.

See the *Administrator's Guide* and *Bundled Agents Reference Guide* for more information.

SFCache agent

SFCache agent is a new agent introduced in this release. The SFCache agent enables, disables, and monitors cache. In case of a cache fault, the application still runs without any issues on the very same system, but with degraded I/O performance. Considering this, the SFCache agent provides an attribute to control the agent behavior. You can either choose to receive “IGNORE” or initiate “FAILOVER” in case of cache fault.

For more information, see *Bundled Agents Reference Guide*.

New agent function for the LDom agent

This topic applies to Solaris.

In this release, the meter entry point has been introduced. This entry point measures the VCPU and Memory requirement of the LDom based on the keys in the Meters attribute.

Changes in Zpool agent

This topic applies to Solaris.

Zpool agent does not monitor the ZFS (Zettabyte File Systems) which have mount point property set to none or canmount property set to off. The agent does not monitor the file systems even when ChkZFSMounts attribute is set to 1. The agent considers these values as intentionally set and does not display a warning in such scenarios.

Solaris 11: `ipadm` command support for IP and NIC agents

This topic applies to Solaris.

On Solaris 11, IP and NIC agents now support the `ipadm` command. IP and NIC agents have been enhanced for performing online, offline, and monitor operations using the `ipadm` command.

For more information, refer to the *Bundled Agents Reference Guide*.

Coordpoint agent

The Coordpoint agent is always in the online state when the I/O fencing is configured in the majority or the disabled mode. For both these modes the I/O fencing does not have any coordination points to monitor. Thereby, the Coordpoint agent is always in the online state.

NFS and NFSRestart agent enhancement

This topic applies to Linux.

NFS and NFSRestart agents support running NFS daemons with the specified ports.

Changes to LLT, GAB, and I/O fencing

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

Changes to LLT

There are no changes to LLT in 6.2 release.

Changes to GAB

There are no changes to GAB in 6.2 release.

Changes to I/O fencing

Symantec Cluster Server (VCS) includes the following changes to I/O fencing in 6.2:

I/O fencing supports majority-based fencing mechanism, a new fencing mechanism that does not need coordination points

I/O fencing supports a new fencing mode called majority-based I/O fencing. Majority-based I/O fencing mode does not need coordination points to provide protection against data corruption and data consistency in a clustered environment. Use majority-based I/O fencing when there are no additional servers and or shared SCSI-3 disks to be used as coordination points. It provides a reliable arbitration method and does not require any additional hardware setup, such as CP Servers or shared SCSI3 disks.

In the event of a network failure, the majority sub-cluster wins the fencing race and survives the race. Note that even if the majority sub-cluster is hung or unresponsive, the minority sub-cluster loses the fencing race and the cluster panics. The cluster remains unavailable till the issue is resolved.

For more information, refer to the *Installation Guide* and *Administrator's Guide*.

Clear coordination point server registrations using the vxfenclearpre utility

The vxfenclearpre utility is enhanced to clear registrations from coordination point servers for the current cluster in addition to the existing functionality to remove SCSI3 registrations and reservation keys from the set of coordinator disks and shared data disks. The local node from where you run the utility must have the UUID of the current cluster at `/etc/vx/.uuids` directory in the `clusuuid` file.

Note that you may experience delays while clearing registrations on the coordination point servers because the utility tries to establish a network connection with IP addresses used by the coordination point servers. The delay may occur because of a network issue or if the IP address is not reachable or is incorrect.

For more information, refer to the *Administrator's Guide*.

Raw disk I/O fencing policy is not supported

Symantec does not support raw disk policy for I/O fencing. Use DMP as the I/O fencing policy for coordinator disks that have either a single hardware path or multiple hardware paths to nodes.

For more information, refer to the *Installation Guide* and *Administrator's Guide*.

SCSI3 fencing support inside Virtual Machines

SCSI3 fencing is now supported inside KVM and VMware Virtual Machines.

For more information, refer to *Virtualization Guide*.

Changes to the Oracle agent

This section mentions the changes made to the Symantec Cluster Server agent for Oracle.

VCS agent for Oracle supports management of container and pluggable databases

VCS supports the multitenant architecture introduced in Oracle 12c Release 1 (12.1). The multitenant architecture enables Oracle database to function as a multitenant container database (CDB) and one or many customized pluggabble databases (PDBs).

Note: IMF monitoring is not supported in a PDB resource.

For more information, refer to the *Agent for Oracle Installation and Configuration Guide*.

Changes to campus clusters

There are no changes to campus clusters in 6.2 release.

Changes to wizard support

You can use the Symantec High Availability Configuration wizard to configure application monitoring for generic applications running on Linux on a physical host.

New VCS configuration wizards introduced on Linux and UNIX

VCS Cluster Configuration Wizard and Symantec High Availability Configuration Wizard are introduced on all supported Linux and UNIX distributions in this release.

The two new wizards replace the Symantec High Availability Configuration Wizard that earlier provided a combined workflow for cluster configuration and application (high availability) configuration, and was supported only on Linux.

You can launch the wizards from the Symantec High Availability view. You can continue to access the view as required from Veritas Operations Manager, VMware vSphere Client, or a browser.

For more information, see the *Symantec Cluster Server Installation Guide* and *Symantec Cluster Server Administrator's Guide.* For steps to use the Symantec High Availability wizard, see the application-specific VCS agent installation and

configuration guides. For VMware specific information on this feature, see the *Symantec High Availability Solutions Guide for VMware*.

Symantec High Availability Configuration Wizard has provision to edit service group names before they are implemented

This topic is applies to Linux.

The Symantec High Availability Configuration Wizard allows you to rename the service groups before they are actually created. The wizard assigns a default name when you configure a service group for high availability. You can use this provision to assign more relevant or easy-to-remember names to the service group before the service groups are actually created.

Wizard detects existing main.cf file before configuring a service group

This topic applies to Linux.

The cluster configuration wizard detects an already existing main.cf file before configuring a service group on the cluster. It displays a message on the health view to indicate the presence of the main.cf file.

Changes to VCS agent framework

The following changes are introduced to the VCS agent framework.

AdaptiveHA is extended for Solaris LDom

This topic is applicable to Solaris.

The CPU and Memory requirement of LDom is metered and used in the BiggestAvailable failover policy for service groups containing LDom resource.

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

Storage Foundation and High Availability (SFHA) includes the new features and changes introduced in 6.2 of the underlying products.

See “Changes related to Symantec Storage Foundation (SF)” on page 13.

See “Changes related to Symantec Cluster Server (VCS)” on page 19.

Changes related to Symantec Storage Foundation Cluster File System High Availability (SFCFSHA)

Symantec Storage Foundation Cluster File System High Availability (SFCFSHA) includes the new features and changes introduced in 6.2 of the underlying products.

See "Changes related to Symantec Storage Foundation (SF)" on page 13.

See "Changes related to Symantec Cluster Server (VCS)" on page 19.

Support for Flexible Storage Sharing

This topic applies to AIX and Solaris.

Cluster Volume Manager (CVM) introduced the Flexible Storage Sharing (FSS) feature, which enables network sharing of local storage, cluster wide. The local storage can be in the form of Direct Attached Storage (DAS) or internal disk drives. Network shared storage is enabled by using a network interconnect between the nodes of a cluster.

FSS allows network shared storage to co-exist with physically shared storage, and logical volumes can be created using both types of storage creating a common storage namespace. Logical volumes using network shared storage provide data redundancy, high availability, and disaster recovery capabilities, without requiring physically shared storage, transparently to file systems and applications.

FSS use cases include support for current SFCFSHA and SF Oracle RAC use cases, off-host processing, DAS SSD benefits leveraged with existing SFHA Solutions features, FSS with File System level caching, and campus cluster configuration.

SF Oracle RAC certification for the FSS feature is currently in progress.

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

Changes related to Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)

SF Oracle RAC includes the new features and changes introduced in 6.2 of the underlying products.

Support for container and pluggable databases in Oracle 12c

SF Oracle RAC now supports the creation and configuration of container databases and pluggable databases in Oracle 12c environments. You can add the container

and pluggable database resources to be managed by VCS. For steps on configuring these resources under VCS, see the *Symantec Storage Foundation for Oracle RAC Installation and Configuration Guide*.

Note: Oracle Dataguard is supported only with administrator-managed Oracle 12c databases.

SmartIO now supported in SF Oracle RAC environments

The SmartIO feature of Storage Foundation and High Availability Solutions (SFHA Solutions) enables data efficiency on your SSDs through I/O caching. Using SmartIO to improve efficiency, you can optimize the cost per IOPS. SmartIO does not require in-depth knowledge of the hardware technologies underneath. SmartIO uses advanced, customizable heuristics to determine what data to cache and how that data gets removed from the cache. The heuristics take advantage of SFHA Solutions' knowledge of the characteristics of the workload. SmartIO supports read and write caching for VxFS file systems mounted on VxVM volumes, in several caching modes and configurations.

- Read caching for applications running on VxVM volumes
- Read caching for applications running on VxFS file systems
- Database caching on VxFS file systems
- Database caching on VxVM volumes

Note: SmartIO writeback caching is not supported in SF Oracle RAC environments.

To use SmartIO, you set up a cache area on the target device. You can do this task simply with one command, while the application is online. When the application issues an I/O request, SmartIO checks to see if the I/O can be serviced from the cache. As applications access data from the underlying volumes or file systems, certain data is moved to the cache based on the internal heuristics. Subsequent I/Os are processed from the cache. You can also customize which data is cached, by adding advisory information to assist the SmartIO feature in making those determinations.

For more information, see the *Symantec. Storage Foundation and High Availability Solutions SmartIO for Solid State Drives Solutions Guide* for details.

Changes related to Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE)

SF Sybase CE includes the new features and changes introduced in 6.2 of the underlying products:

See "Changes related to installation and upgrades" on page 9.

See "Changes related to Symantec Cluster Server (VCS)" on page 19.

This release is supported only on Solaris SPARC.

For details on the features and the supported operating system versions, see the *Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE) Release Notes*.

Changes related to Symantec ApplicationHA

Symantec ApplicationHA includes the following changes in 6.2:

vSphere Web Client integration

This change is only applicable to ApplicationHA users working in a VMware virtual environment.

Symantec has introduced the Symantec HA Plug-in for vSphere Web Client as part of Veritas Operations Manager 6.1 release. Installing and configuring VOM Management Server 6.1 in your virtualization environment, along with the plug-in, helps you perform ApplicationHA operations directly from the vSphere Web Client menu. This is in addition to the existing integration with the vSphere Client menu (desktop) via the Symantec High Availability Console. For detailed information on the vSphere Web Client integration see VOM 6.1 documentation.

For the latest information on ApplicationHA installation, configuration, and administration support via vSphere Web Client, see the following technical note:

http://www.symantec.com/docs/TECH222796

Change in packaging of certain ApplicationHA agents and VRTSacclib

Starting with this release, certain Symantec ApplicationHA agents and VRTSacclib will not be packaged as part of the ApplicationHA installation media. You must download the required application agents from the latest Agent Pack release on SORT.

Note: This packaging change has no impact on ApplicationHA installation in the Oracle VM Server for SPARC or IBM PowerVM virtual environments:

Also note that there is no change in the packaging of the ApplicationHA agents for the following applications; they continue to be packaged as part of the ApplicationHA installation media.

- Oracle Database
- Apache HTTP Server
- DB2 (not supported in Oracle VM Server for SPARC)
- Generic (custom) applications

For the VMware virtual environment, the following table lists each supported application and the related ApplicationHA agent RPMs that you must download from SORT:

Table 1-4

Application	ApplicationHA agent package
JBoss Application Server	VRTSjboss
MySQL Server	VRTSmysql
SAP Web Application Server SAP NetWeaver	VRTSsapcms VRTSsaplc VRTSsapnw04 VRTSsapwebas71
WebSphere Application Server	VRTSvcswas
WebSphere MQ	VRTSmq6
WebLogic Server	VRTSwls
Required for all the above applications	VRTSacclib

For the KVM (Linux) virtual environment, the following table lists each application and the related ApplicationHA agent RPMs that you must download from SORT:

Table 1-5

Application	ApplicationHA agent package
JBoss Application Server	VRTSjboss

Table 1-5 *(continued)*

Application	ApplicationHA agent package
MySQL Server	VRTSmysql
WebSphere Application Server	VRTSvcswas
WebSphere MQ	VRTSmq6
Required for both the above applications	VRTSacclib

Intelligent Monitoring Framework

VRTSamf is a new package introduced in this release. The package enables Symantec ApplicationHA agents to leverage the Intelligent Monitoring Framework (IMF) module.

In this release, the VRTSveki fileset is also introduced as part of the ApplicationHA filesets for IBM PowerVMs in an AIX environment. VRTSveki contains the kernel interface, which is a common set of modules that the IMF driver uses.

IMF offers a way for ApplicationHA agents to avoid polling for state changes among the monitored application components. IMF allows the agents to register which components to monitor. When the state of an applicationcomponent changes, IMF immediately notifies the agent. Corrective action can therefore be immediately taken once an event occurs. IMF enables the ApplicationHA agents to monitor a large number of components with a minimal effect on performance.

IMF support for the following ApplicationHA agents is introduced in this release:

- Apache HTTP Server
- DB2 Database (not applicable to Oracle VM Server for SPARC environment)
- Oracle Database
- Generic (custom) applications

Note: The Symantec High Availability Configuration wizard by default enables IMF support. To disable IMF support, you must use Symantec Cluster Server (VCS) commands.

Online upgrade for ApplicationHA

You can perform an online upgrade to ApplicationHA 6.2 by using the installer, while keeping your applications online. Ensure that you use one of the supported upgrade paths listed in the *Symantec ApplicationHA Installation Guide*.

During this upgrade process, ApplicationHA does not monitor the configured applications for high availability.