Symantec™ Storage Foundation and High Availability Solutions 6.1 What's new in this release - AIX, Linux, Solaris

February 2014

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: 6.1

Document version: 6.1 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_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

What's new in this release

This document includes the following topics:

Introduction

This document covers the major new features, enhancements, and changes that are introduced in 6.1 for the Symantec Storage Foundation and High Availability

Solutions products. See the *Release Notes* for your product for a list of all changes in 6.1.

Note: The new features and enhancements listed in this document apply to AIX, Linux, and Solaris unless mentioned otherwise.

Featured product enhancements in 6.1

Symantec Storage Foundation and High Availability Solutions products 6.1 include the following major new features:

Caching on Solid-State Drives on Linux using:	■ Storage Foundation SmartIO See "SmartIO: Support for caching on Solid-State Drives on Linux" on page 15.
Flexible Storage Sharing on Linux using:	■ Cluster Volume Manager (CVM) in Storage Foundation Cluster File System High Availability (SFCFSHA) See "Support for Flexible Storage Sharing on Linux" on page 36.
Centralized installations using the Deployment Server	■ See "Support for centralized installations using the Deployment Server" on page 11.
AdaptiveHA using:	■ Symantec Cluster Server See "AdaptiveHA" on page 22.

Video presentations for these features are available on the Symantec Connect website at:

Changes related to product name branding

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

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

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

Old product name	New product names with Symantec branding
Veritas Storage Foundation	Symantec Storage Foundation (SF)

Table 1-1 Rebranded Storage Foundation and High Availability Solutions products *(continued)*

Old product name	New product names with Symantec branding
Veritas Dynamic Multi-Pathing	Symantec Dynamic Multi-Pathing (DMP)
Veritas Replicator Option	Symantec Replicator Option
Veritas File Replicator Option	Symantec File Replicator Option (VFR)
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 for Sybase ASE CE	Symantec Storage Foundation for Sybase ASE CE
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

Changes related to installation and upgrades

The product installer includes the following changes in 6.1.

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

The following applies to all products except Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE):

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

For SF Sybase CE:

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.

Support for Solaris 11 Live Upgrade

You can use Live Upgrade on Solaris 11 systems to perform an upgrade of the product and the Solaris operating system. For the Live Upgrade process, an alternate boot environment is created on the primary boot disk by ZFS storage application. All boot environments are saved in the current disk. Thus, an alternate boot disk is not needed anymore.

See the *Installation Guide* for more information.

Improved patching and updating process

You can now download product maintenance releases and public hot fix releases directly from the Symantec Operations Readiness Tools (SORT) website using the installer. When you use the `installer` command with the `-version` option, the installer now lists the available GA releases, maintenance releases, and hot fix

releases. If you have Internet access, you can follow the installer prompts to download available patches and hot fixes to your local system.

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

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

See the *Installation Guide* for more information.

Automatic download of installer hot fixes

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

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

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

See the *Installation Guide* for more information.

Support for centralized installations using the Deployment Server

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

The Deployment Server lets you do the following as described in Table 1-2.

Table 1-2 Deployment Server functionality

Feature	Description
Manage release images	■ 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.
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.

Web installation program supports phased upgrade

You can now perform a phased upgrade of your product with the web-based installer. The installer detects and upgrades the product that is currently installed on the specified system or systems.

See the *Installation Guide* for more information.

Changes related to Symantec Dynamic Multi-Pathing (DMP)

The following sections describe changes in this release related to Symantec Dynamic Multi-Pathing (DMP).

DMP support for ZFS root on Solaris

Starting with this release, Dynamic Multi-Pathing (DMP) supports the ZFS root file system. When you install DMP with native support enabled, or enable native support with the tunable `dmp_native_support`, DMP also migrates the ZFS root pool to DMP. Reboot the system for the change to take effect.

DMP support for ZFS root requires Solaris 11 update 1 or later.

For more information about configuring ZFS root, see the *Symantec Dynamic Multi-Pathing Administrator's Guide - Solaris*.

Enhancements to DMP support for rootvg on AIX

The root volume group (rootvg) is supported on DMP devices. This release includes the following enhancements:

- The operating system commands `bosboot`, `ADI`, `mksysb restore`, and related operations no longer require an additional DMP step. In previous releases, these operations required some steps to run the `vxdmpadm native release` command and the `vxdmpadm native acquire` command. These steps are no longer required. The commands `extendvg` and `reducevg`, which are less frequently used than other boot management commands, still require steps to release and acquire the device paths. See the administrator's guide for detailed steps.
- The outputs for the `lspv` command and the `lsvg` command are changed for the rootvg devices that DMP controls. In previous releases, the output showed the DMP device name. In this release, the output shows the device path names.
- Certain upgrade paths require that you uninstall the `VRTSvxvm` fileset. In previous releases, uninstalling the `VRTSvxvm` fileset failed if the DMP root support was enabled. The upgrade required that you disable DMP root support first, which required an additional reboot of the system. In this release, uninstalling the `VRTSvxvm` fileset automatically disables DMP root support and the uninstallation succeeds. Removing a `VRTSvxvm` patch also automatically disables DMP root support, even if the `vxconfigd` daemon is not running. The new behavior reduces the number of reboots that are required to uninstall or upgrade.

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 Symantec Storage Foundation (SF)

Symantec Storage Foundation includes the following changes in 6.1:

SmartIO: Support for caching on Solid-State Drives on Linux

Solid-State Drives (SSDs) are devices that do not have spinning disks. Today's solid-state technologies, such as DRAM and NAND flash, provide faster data access, are more efficient, and have a smaller footprint than traditional spinning disks. The data center uses solid-state technologies in many form factors: in-server, all flash arrays, all flash appliances, and mixed with traditional HDD arrays. Each form factor offers a different value proposition. SSDs also have many connectivity types: PCIe, FC, SATA, and SAS.

Due to the current cost per gigabyte of SSD devices, the best value of SSDs is not as high capacity storage devices. The benefit of adopting SSDs is to improve performance and reduce the cost per I/O per second (IOPS). Data efficiency and placement is critical to maximizing the returns on any data center's investment in solid state.

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
- Writeback 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.

Changes related to Veritas Volume Manager

Enhancements to the disk cloning operations

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

- When you import a disk group, the disks with the `udid_mismatch` flag display the `clone_disk` flag regardless of whether the system sees the original source disks. In previous releases, the `clone_disk` flag was hidden if the source disks were not visible to the system.
- By default, VxVM now prevents the import of a partial set of disks in a clone disk group when the `-o updateid` option is specified. This behavior prevents the missing disks from being permanently detached from the new disk group. You can specify the `-f` option to partially import the clone disk group with `-o updateid`.
- When you import a set of clone disks with the `-o updateid` option and specify a new disk group name, the disk group becomes a standard disk group with updated disk and disk group identifiers. This operation clears the `udid_mismatch` flag or the `clone_disk` flag from the disks.
- When you import a set of clone disks with the `-o updateid` option, you can use the `vxdg import` with the `-c` option to convert the existing disk group to a standard disk group with updated disk and disk group identifiers. This operation clears the `udid_mismatch` flag or the `clone_disk` flag from the disks. You cannot perform this operation if the source disk group is already imported on the same host.
- You can now update the UDID for a disk and remove the `udid_mismatch` flag and the `clone_disk` flag with a single operation. Updating the UDID aligns it with the UDID detected by the DDL.

  `vxdisk -c updateudid` *`diskname`*
- You cannot create disk groups on `udid_mismatch` or `clone_disk` disks.
- If disks are falsely marked as `udid_mismatch`, you can use `vxdg -c init` option to create disk groups on them.
- If the disk group has multiple clone copies, and you import the disk group with a tagname, the disks that have tags set will be selected. The tag-based import operation gives higher priority to disks with the tags set rather than the set of disks that were last imported. In previous releases, if multiple clone copies had the same disk group id, the import operation gave preference to the last import time.

Enhancements to the Dynamic Reconfiguration tool

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

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

Changes related to Veritas File System

Support for 64-bit quotas

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

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

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

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

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

maxlink support

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

On AIX:

By default maxlink is disabled.

On Linux and Solaris:

By default maxlink is enabled.

See the *Administrator's Guide*.

Disk layout Version 10

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

On Linux:

Version 10 disk layout enables support for SmartIO and maxlink.

On AIX and Solaris:

Version 10 disk layout enables support for maxlink.

See the *Administrator's Guide*.

vxfsstat command can display per file system memory and VOP statistics

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

`-B` Displays per file system metadata buffer cache statistics.

`-I` Displays per file system inode cache and DNLC statistics.

`-x` An already existing option that displays per file system statistics, and now additionally displays the newly added memory and VOP counters. VOP counters include VOP time and VOP count.

Changes related to replication

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

New vfradmin job promote and vfradmin job recover commands simplify changing replication direction

The `vfradmin` command now has the `job promote` keyword and `job recover` keyword that enable you to change the replication direction with a single command instantiation. You use `job recover` after a disaster occurred, and `job promote` under normal circumstances.

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

VVR replication performance improvements using bulk transfer

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

VVR I/O throughput improvements using batched writes

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

Changes related to SFDB tools

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

Reverse Resync for Oracle database recovery

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

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

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

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

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

  `Reverse_Resync_Recovery`

  `Reverse_Resync_Archive_Log`

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

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

---

Note: Reverse resync is not supported for RAC databases.

Supported DB2 configurations

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

Supported Oracle configurations

In 6.1 release, SFDB tools support Oracle 12c release for Oracle databases.

Note: For Oracle 12c, the SFDB tools do not support the Multitenant database features, including the CDB and PDB databases.

Support for instant mode snapshots for Oracle RAC databases

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

Changes related to 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*.

Changes related to virtualization support in VCS

Disaster recovery support for RHEV-based virtual machines using VCS

You can now configure disaster recovery (DR) for virtual machines on Linux that are created using Redhat Enterprise Virtualization (RHEV). You can replicate the storage used for virtual machine boot disks 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 KVMGuest agent supports network reconfiguration when hypervisors are separated by geographical distances.

Live migration of service groups

VCS now supports live migration capabilities for service groups that have resources to monitor virtual machines. The process of migrating a service group involves concurrently moving the service group from the source system to the target system with minimum downtime. A new entry point titled “migrate” is introduced for agent developer for this process. This entry point is available with the Script60Agent. The behavior of migrate entry point can be controlled using new attributes - MigrateTimeout, MigrateWaitLimit and SupportedOperations.

This feature is supported in the following virtualization environments:

- LPAR on AIX
- LDoms on Solaris
- KVM and RHEV on Linux

For more information, see the *Symantec Cluster Server Administrator's Guide* and *Symantec Storage Foundation and High Availability Solutions Virtualization Guide*.

VCS-initiated live migration support in virtual environments

VCS supports the live migration initiation of virtual machine resources - LPAR, KVMGuest and LDOM on AIX, Linux and Solaris platforms respectively using VCS commands. This feature enables native live migration functionality as it is performed

through the architecture and VCS only includes the ability to pass commands to the architecture as a part of the cluster framework.

This feature is supported in the following virtualization environments:

- LPAR on AIX
- LDoms on Solaris
- KVM and RHEV on Linux

Refer to the following links for more information.

See "LPAR agent enhancements" on page 24.

See "VCS can initiate virtual machine migration" on page 25.

See "LDom agent enhancements" on page 25.

Changes to the VCS engine

OpenVCSCommunicationPort attribute to determine whether to allow external communication port

The OpenVCSCommunicationPort attribute determines whether or not the external communication port for VCS is open for communication.

If the external communication port for VCS is not open, the following restrictions apply:

- You cannot use Java Console to administer VCS.
- On AIX:
  RemoteGroup resources and users set up with the `hawparsetup` command cannot access VCS.
- On Linux:
  RemoteGroup resources cannot access VCS.
- On Solaris:
  RemoteGroup resources and users set up with the `hazonesetup` command cannot access VCS.

AdaptiveHA

AdaptiveHA enables VCS to make dynamic decisions about selecting the cluster node with maximum available resources to fail over an application. VCS dynamically monitors the available unused capacity of systems in terms of CPU, Memory, and Swap to select the most resourceful system. For more information on AdaptiveHA, refer to the *Symantec Cluster Server Administrator's Guide*.

Attributes modified to implement AdaptiveHA

To implement AdaptiveHA in VCS, the following attributes have been modified:

- HostUtilization: Indicates the percentage usage of the resources on the host as computed by the HostMonitor agent.
- FailOverPolicy: Governs how VCS calculates the target system for failover. Added a new policy value BiggestAvailable to this service group attribute.
  BiggestAvailable: VCS selects a system based on the forecasted available capacity for all the systems in the SystemList. The system with the highest forecasted available capacity is selected. This policy can be set only if the cluster attribute Statistics is enabled and the service group attribute Load is defined. Load must be defined in terms of CPU, Memory, or Swap in absolute units as specified in MeterUnit attribute.
- Load: Indicates the multidimensional value expressing load exerted by a service group of the system.
- HostMonitor: Contains list of host resources that the HostMonitor agent monitors.
- AvailableCapacity: Indicates the system's available capacity.
- Capacity: Represents total capacity of a system.

Note: AvailableCapacity, Capacity, Load, and DynamicLoad attributes have multi-dimensional values

Changes to VCS bundled agents

This section describes changes to the bundled agents for VCS.

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

IMF support for Apache HTTP server agent

The Apache HTTP server agent is IMF-aware and uses the AMF kernel driver for IMF notification. The agent also performs detailed monitoring on the Apache resource. You can tune the frequency of detailed monitoring with the LevelTwoMonitorFreq attribute. The SecondLevelMonitor attribute is deprecated.

Support for direct mount inside non-global zones using Mount agent

You can mount VxFS directly inside a non-global zone. To mount VxFS inside a non-global zone, override the ContainerOpts attribute at the resource level and set the value of the RunInContainer attribute to 1.

Support for level two monitoring in Application agent when MonitorProgram attribute is configured

If the Application resource is configured with MonitorProcesses, PidFiles or both along with MonitorProgram, you can configure the Application resource to run MonitorProgram as a level two monitor. To enable level two monitoring, set the LevelTwoMonitorFreq attribute to a value greater than zero. The default value of LevelTwoMonitorFreq attribute for Application resource is 1 (one).

With this change, the Application agent can leverage AMF for instant notification even when MonitorProgram is configured along with MonitorProcess or PidFiles or both.

Proxy agent logs improved to provide more detail

The Proxy agent log messages now provide more detail such as the reason for the agent going to unknown or faulted state. Debug messages are also logged when the Proxy resource goes online or offline.

Apache agent takes a resource offline when process stops [2978005]

Apache agent is now modified to take the resource offline immediately when the Apache processes stop as part of offline entry point.

LPAR agent enhancements

LPAR agent for AIX has been enhanced to include the following capabilities:

Support for migration of LPAR resource through VCS

A new migrate entry point is added to the LPAR agent to initiate live migration of LPAR through VCS.

Added support for LPAR profile management with LPAR live migration

LPAR agent is enhanced to support LPAR failover along with live migration of LPAR. When an LPAR resource is live migrated from a physical source server to a physical target server, the migration process deletes the LPAR profile on the physical source

server. If the migrated LPAR on target physical server faults or if the LPAR service group is required to switch back from the target server, the LPAR cannot be brought online on the physical source server due to unavailability of the LPAR profile configuration. In order to facilitate the failover of the LPAR back to the physical source server, you must first create the LPAR profile configuration. The LPAR agent is enhanced to read LPAR configuration file as configured in ProfileFile attribute and create the LPAR on failover physical server while bringing the LPAR resource online. Similarly, the LPAR agent is enhanced to delete the LPAR configuration while bringing LPAR offline depending on RemoveProfileOnOffline attribute value.

VCS can initiate virtual machine migration

KVMGuest agent is enhanced to implement newly introduced migrate entry point for initiating a virtual machine migration in KVM and RHEV environments.

New agent function for the Mount agent

The Mount agent supports the attr_changed function. This function unlocks the mount when you change the value of the VxFSMountLock attribute from either 1 or 2 to 0.

LDom agent enhancements

LDom agent for Solaris has been enhanced to include the following capabilities:

- Support for migration of LDom resource through VCS:
  A new migrate entry point is added to the LDom agent to initiate migration of guest domains through VCS. Two new attributes UserName and Password are introduced to support the migration of guest domain.
- VCS supports logical domains with control domain restart in multiple I/O domain environments
  Guest domain continues to function even if control domain is restarted or shut down, provided I/O services from the primary or alternate I/O domain are available. In this case, the Oracle VM for SPARC guest domain (LDom) is provided with I/O services from more than one I/O domains (typically the primary domain and the alternate I/O domain).
- New command to configure Oracle VM server for SPARC
  A new command `haldomsetup` is introduced to help you configure Oracle VM server for SPARC guest domain under VCS management. Refer to the *Symantec Cluster Server manual pages* for more information.

See “Attributes introduced in VCS 6.1” on page 31.

Default value of MonitorCPU attribute for LDom agent on Solaris changed to 0 (zero)

A resource was declared as faulted when the MonitorCPU attribute was enabled and if CPU usage of all the virtual CPUs attached to the LDom was equal to either 0% or 100%.

Setting the default value of the MonitorCPU attribute to 0 prevents the resource from faulting.

Changes to LLT, GAB, and I/O fencing

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

Disable LLT, GAB, and I/O fencing on a single node cluster

Disable LLT, GAB, and I/O fencing kernel modules on a single node Symantec Cluster Server (VCS) cluster if you only want to manage applications and use the application restart capabilities of VCS for the node.

Note that disabling the kernel modules means that you cannot provide high availability to applications across multiple nodes. However, in future, if you decide to extend the cluster to multiple nodes, you can enable the modules and make the applications highly available.

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

Kernel components will no longer install package metadata inside non-global zones on Solaris 10

VCS kernel components VRTSllt, VRTSgab, VRTSvxfen, and VRTSamf packages will no longer install package meta data inside non-global zones on Solaris 10 operating system.

Changes to LLT

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

LLT and GAB support RDMA technology on Linux for faster interconnect between nodes

Remote direct memory access (RDMA) is a direct memory access capability that allows server to server data movement directly between application memories with minimal CPU involvement. LLT and GAB support RDMA for faster interconnect between nodes. RDMA is supported on InfiniBand and RDMA over Converged Ethernet (RoCE) networks. RDMA provides high throughput, low latency, and

minimized host CPU usage thereby improving application performance. RDMA provides performance boost for the use cases of the Flexible Storag Sharing with Cluster Volume Manager (CVM) and Cluster File System (CFS), and IO Shipping with CVM in clustered environments.

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

LLT command changes

The following command changes are introduced in this release.

Updates in `lltconfig`:

- On Linux, LLT supports a new link type called "rdma". You can use this link type to dynamically add an RDMA link under LLT at run time.
- A new option `lltconfig -l` is introduced. When you add a new link, you can use the `-l` option to specify that the link is a low priority link.

Updates in `lltstat` on Linux:

- A new option `lltstat -r` is introduced. Use the `-r` option in conjunction with the `-nvv` option. The `-r` option additionally displays the status of the RDMA channel connectivity.
- The output of `lltstat -lv` option has changed. The verbose information is displayed in a different format. For ether and udp links, this option does not display the verbose information. For the rdma links, this option displays information about the packets that are sent or received over the rdma and udp channels.

Updates in `lltping`:

- A new option `lltping -F` is introduced. Use this option to check the LLT connectivity over RDMA channel.

Updates in `lltest`:

- A new option `lltest -F` is introduced. Use this option to the test the LLT protocol over RDMA channel.

Changes to GAB

Symantec Cluster Server (VCS) includes the following changes to GAB in 6.1:

Adaptive GAB tunables to prevent false failover

You can configure the VCS environment variables, `VCS_GAB_TIMEOUT_SECS` and `VCS_GAB_PEAKLOAD_TIMEOUT_SECS`, to make GAB adaptive to different load conditions on a node (per CPU load). GAB calculates the timeout range for the load

period based on the load average number provided by the operating system and the variable values that are set for HAD. GAB kills HAD after the timeout period.

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

Changes to I/O fencing

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

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

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

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

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

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

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

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

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

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

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

Preferred fencing with Group policy resets the node weight if the VCS engine instance on that node is killed

Preferred fencing with Group policy resets the node weight to zero if the VCS engine instance on that node is killed. During a network partition, the node with the VCS engine instance running on it is given preference over a node that does not have

the VCS engine instance running even though the node with the VCS engine has lower priority applications. The surviving sub-cluster wins the race for coordination points. As the surviving sub-cluster has VCS engine running it has the ability to make the applications on the lost sub-cluster highly available.

For more information refer to the *Symantec Cluster Server Administrator's Guide*.

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

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

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

Site-based preferred fencing policy

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

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

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

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

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

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

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

Changes to the Oracle agent

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

VCS agent for Oracle uses the Oracle health check APIs to determine intentional offline of an Oracle instance

The Symantec Cluster Server agent for Oracle uses the Oracle health check APIs to determine whether the Oracle instance on a node was shut down gracefully or aborted. When an oracle instance is shut down gracefully outside of VCS control the agent acknowledges the operation as intentional offline.

From the VCS 6.1 release onwards, the pre-built health check binaries will not be shipped. You need to run the `build_oraapi.sh` script to build the oracle health check binaries based on the Oracle Version.

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

VCS will no longer ship Oracle health check binaries

From the VCS 6.1 release, the pre-built health check binaries will not be shipped. You need to run the `build_oraapi.sh` script to build the oracle health check binaries based on the Oracle Version.

Changes to campus clusters

Multi-site management

You can create sites to use in an initial failover decision in campus clusters by configuring the SiteAware cluster level attribute. You can define sites and add systems to the sites that you have defined. A system can belong to only one site. Site definitions are uniform across VCS, Veritas Operations Manager, and VxVM. You can define site dependencies to restrict connected applications to fail over within the same site.

If sites are configured for a cluster, a service group tries to stay within its site before choosing a host in another site. For example, in a campus cluster with two sites, site A and site B, you can define a site dependency among service groups in a three-tier application infrastructure consisting of Web, application, and database to restrict the failover within the same site.

You must have the Veritas Operations Manager 6.0 to define sites and dependencies and configure site for a cluster.

Refer to the *Administrator's Guide* for more information.

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.

Configuring applications through a wizard is supported in VCS on Linux

You can configure applications in VCS using the Symantec High Availability Configuration wizard. You can launch this wizard through Veritas Operations Manager (VOM), from a browser window, or by using the haappwizard utility. In case of VMware-based Linux virtual machines, the wizard can also be launched through a vSphere client. In this release, the following applications can be configured through the wizard:

Table 1-3 Environment-based supported application configuration

Environment	Configuration supported
Linux on VMware guests	Generic application Oracle WebSphere MQ SAP
Linux on physical hosts	Generic application

For more details on configuration, refer to the respective application guides. In future releases, configuration of more applications may happen through the wizard.

Attributes introduced in VCS 6.1

The following section describes the attributes introduced in VCS 6.1.

LDom agent attributes on Solaris

DomainFailurePolicy:	Specifies the list of master domains and the failure policies of master domains for a guest domain. Attribute key: Name of the master domain. Key value: Failure policy enacted by the master domain on the guest domain. To use this feature: ■ Set the LDom resource attribute DomainFailurePolicy to the master domain and its failure policy. ■ Set the LDom service group attribute SysDownPolicy to AutoDisableNoOffline.
UserName:	Specifies the user name authorized to migrate the logical domain on the host from another host.
Password:	Specifies the encrypted password for the user specified in the UserName attribute.
RegregPGR (Solaris)	If this attribute is set to 1, then after the live migration of a logical domain using the `hagrp -migrate` command, the LDom agent runs the `vxdmpadm pgrrereg` command inside the logical domain.

NFS agent attributes

Protocol	Specifies the protocol to run the nfsd daemon. The agent uses this attribute to ensure that the NFS daemon is running using the specified protocol.
MountdOptions (Linux and Solaris)	Specifies options for the mountd daemon.

LPAR agent attributes on AIX

ProfileFile	Specifies the path to the LPAR profile configuration file.

RemoveProfileOnOffline	Enables deleting the LPAR profile from the physical source server while bringing the LPAR resource offline or when the LPAR resource faults to facilitate the LPAR migration in future.

NotifierMngr agent attribute

MessageExpiryInterval	Specifies time in seconds after which the messages expire. If the engine does not send a message to the notifier within MessageExpiryInterval, it deletes the message from the message queue of the engine.

DiskGroup agent attribute

ClearClone	Clears the "clone" and "udid_mismatch" flags form the disks of the disk group while importing it and laso updates the UDID if required.

KVMGuest agent attributes on Linux

RHEVInfo	Specifies information about the RHEV environment. ■ Enabled: Specifies virtualization environment (0 for KVM and 1 for RHEV). ■ URL: Specifies RHEV-M URL that can be used for REST API communication. ■ User: Specifies RHEV-M user that can be used for REST API communication. ■ Password: Specifies the encrypted password of RHEV-M user. ■ Cluster: Specifies the cluster name in RHEV-M to which the VCS host belongs. ■ UseManualRHEVMFencing : Enables or disables the use of manual RHEV-M fencing in case the physical host on which the virtual machine is running crashes.
DROpts	Defines DR options. Consists of various keys.

MigrateWaitLimit	Specifies the migrate wait limit. The monitor entry point runs for the number of times specified in the attribute value to determine whether or not the attempted resource migration failed.
MigrateTimeout	Specifies the timeout value for migrating virtual machines.

New attributes to enable AdaptiveHA

Statistics	Indicates if statistics gathering is enabled and whether the FaultOverPolicy can be set to BiggestAvailable. Statistics are gathered for system resources like CPU, Memory, Swap, and so on.
MeterWeight	Represents the weight given for the cluster attribute's HostMeters key to determine a target system for a service group when more than one system meets the group attribute's Load requirements.
HostAvailableMeters	Lists the meters that are available for measuring system resources. You cannot configure this attribute in main.cf.
HostMeters	Indicates the parameters (CPU, Mem, or Swap) that are currently metered in the cluster.
MeterControl	Indicates the intervals at which metering and forecasting for the system attribute AvailableCapacity are done for the keys specified in HostMeters.
HostAvailableForecast	Indicates the forecasted available capacities of the systems in a cluster based on the past metered AvailableCapacity.
MeterRecord	Acts as an internal system attribute with predefined keys. This attribute is updated only when the Cluster attribute Statistics is set to Enabled.

ReservedCapacity	Indicates the reserved capacity on the systems for service groups which are coming online and with FailOverPolicy is set to BiggestAvailable. It has all of the keys specified in HostMeters, such as CPU, Mem, and Swap. The values for keys are set in corresponding units as specified in the Cluster attribute MeterUnit.
CapacityReserved	Indicates whether capacity is reserved to bring service groups online or to fail them over. Capacity is reserved only when the service group attribute FailOverPolicy is set to BiggestAvailable.
UnSteadyCount	Represents the total number of resources with pending online or offline operations. This is a localized attribute.
MemThresholdLevel	Determines the threshold values for memory utilization based on which various levels of logs are generated.

Refer to *Administrator's Guide* for more information.

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

Storage Foundation and High Availability (SFHA) includes the new features and changes introduced in 6.1 of the underlying products.

See "Changes related to Symantec Storage Foundation (SF)" on page 14.

See "Changes related to Symantec Cluster Server (VCS)" on page 21.

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 6.1 of the underlying products.

See "Changes related to Symantec Storage Foundation (SF)" on page 14.

See "Changes related to Symantec Cluster Server (VCS)" on page 21.

The SVS functionality has moved to SFCFSHA

Symantec VirtualStore (SVS) functionality moved to the Storage Foundation Cluster File System High Availability (SFCFSHA) product except for the SVS VMware vCenter and View plug-in. The SVS VMware vCenter and View plug-in has been discontinued.

The following 3 SVS components are shipped with SFCFSHA:

- `svsdatastore`(1M)
- `svsiscsiadm`(1M)
- `svsdbsnap`(1M)
  The `svsdbsnap`(1M) manual page is located in the following tarball file:
  http://go.symantec.com/sfcfsutilitiesfororacle/

See the *Symantec Storage Foundation Cluster File System High Availability Administrator's Guide* for more information.

For more information on how to upgrade SVS to SFCFSHA 6.1, see the *Symantec Storage Foundation Cluster File System High Availability Installation Guide* for more information.

Support for Flexible Storage Sharing on Linux

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 product features, FSS with File System level caching, and campus cluster configuration.

Installing SFCFS automatically enables the FSS feature and no separate license is required.

SFRAC 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 6.1 of the underlying products.

CSSD agent enhancements

The CSSD agent is no longer a generic Application agent. It now has its own CSSD type definition that allows simpler configuration and flexible resource-handling.

The remaining changes are as follows:

- New attribute `RestartDaemons` introduced for Oracle RAC 11g Release 2 and later versions.
  The default value is set to 1 and indicates whether or not the Oracle Grid Infrastructure processes `ohasd`, `cssd`,`crsd`, and `evmd` are restarted if the status of these processes is unhealthy.
- Intelligent Monitoring Framework (IMF) is now supported for the `ohasd`, `cssd`,`crsd`, and `evmd` daemons.
  By default, IMF monitoring is enabled with a monitoring value of 3.
- The `Clean` function now uses the `force` option to forcibly stop Oracle Grid Infrastructure on nodes running Oracle RAC 11g Release 2.

As a result of these improvements, you will see the following changes during an upgrade:

- The agent type is set to `CSSD`.
- The installer prompts for the Oracle Clusterware home directory. This is optional. The agent uses this information to locate Oracle Clusterware process binaries. If the value is not provided, the agent reads the information from the Oracle configuration file.

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

SF Sybase CE includes the new features and changes introduced in 6.1 of the underlying products.

This release is supported only on Solaris SPARC.

See the *Release Notes* for details on supported opertaing system versions.

Changes related to Symantec ApplicationHA

Symantec ApplicationHA includes the following changes in 6.1:

Change of packaging in the ApplicationHA 6.1 installation media

With this release, Symantec ApplicationHA is packaged along with the Storage Foundation and High Availability (SFHA) 6.1 installation media. This change eliminates the need to download and manage separate installation media for ApplicationHA.

Keyless licensing

Keyless licensing is a user-friendly licensing option for deploying and managing Storage Foundation and High Availability (SFHA) product installations.

Keyless licensing uses a management server model (via Veritas Operations Manager) to ensure fair and authorized installation and upgrades of all SFHA component products, including Symantec ApplicationHA. This method eliminates the need to maintain a large inventory of license keys for various instances and releases of SFHA stack products installed in your data center.

Support for centralized installations using the Deployment Server

The Deployment Server lets you store multiple release images in one central location and deploy them to systems of any supported platform.

You can load and store product binaries for Symantec products dating back to version 5.1 in a central repository. You can use the Deployment Server for performing the following tasks:

- Version checking
- Release image management
- Install or upgrade systems
- Update metadata and preferences

Added support for VMware versions

Symantec ApplicationHA provides an added support for the following VMware versions:

- vSphere Client 5.0 Update 1 a/b, 5.1, 5.5
- vCenter Server 5.0 Update 1 a/b, 5.1, and 5.5

- VMware ESXi Server 5.0 Patch 4, 5.1, and 5.5

Changes related to product documentation

The Symantec Storage Foundation and High Availability Solutions (SFHA Solutions) 6.1 release includes the following changes to the product documentation.

Table 1-4 lists the documents introduced in this release.

Table 1-4 New documents

New documents	Notes
Symantec™ Storage Foundation and High Availability Solutions SmartIO for Solid State Drives Solutions Guide - Linux	Provides information about the new SmartIO feature for Storage Foundation and High Availability Solutions.
Symantec™ Storage Foundation and High Availability Solutions Virtualization Guide - Linux on ESXi (This document is available online only.)	Provides information about using Storage Foundation and High Availability Solutions in the VMware ESXi virtualization environment.

The SFHA Solutions 6.1 release includes Symantec ApplicationHA. The ApplicationHA documentation set is included in this release.

Table 1-5 lists the documentation for Symantec ApplicationHA.

For Linux, SFHA Solutions 6.1 release also includes the Symantec High Availability Console and its documentation set.

Table 1-6 lists the documentation for the Symantec High Availability Console component.

Table 1-5 Symantec ApplicationHA documentation

Document title	File name	Description
Symantec ApplicationHA Release Notes	applicationha_notes_61_vmware_lin.pdf	Describes the new features and software and system requirements. This document also contains a list of limitations and issues known at the time of the release.
Symantec ApplicationHA Installation and Upgrade Guide	applicationha_install_61_vmware_lin.pdf	Describes the steps for installing and configuring and managing Symantec ApplicationHA. Some of the most common troubleshooting steps are also documented in this guide.

Table 1-5 Symantec ApplicationHA documentation *(continued)*

Document title	File name	Description
Symantec ApplicationHA User's Guide	applicationha_users_61_ vmware_lin.pdf	Provides information about configuring ApplicationHA in a local VMware cluster environment and the VMware site recovery environment. Some of the most common troubleshooting steps are also documented in the guide.
Symantec ApplicationHA Agent for Oracle Configuration Guide	applicationha_oracle_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for Oracle.
Symantec ApplicationHA Agent for SAP NetWeaver Configuration Guide	applicationha_sap_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for SAP NetWeaver.
Symantec ApplicationHA Agent for WebLogic Server Configuration Guide	applicationha_weblogicserver_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for WebLogic Server.
Symantec ApplicationHA Generic Agent Configuration Guide	applicationha_gen_agent_61_vmware_ lin.pdf	Describes how to configure application monitoring for a generic application.
Symantec ApplicationHA Agent for WebSphere MQ Configuration Guide	applicationha_webspheremq_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for WebSphere MQ.
Symantec ApplicationHA Agent for WebSphere Application Server Configuration Guide	applicationha_websphereas_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for WebSphere Application Server.
Symantec ApplicationHA Agent for DB2 Configuration Guide	applicationha_db2_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for DB2.
Symantec ApplicationHA Agent for Apache HTTP Server Configuration Guide	applicationha_apache_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for Apache HTTP Server.
Symantec™ ApplicationHA Agent for JBoss Application Server Configuration Guide	applicationha_jboss_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for JBoss Application Server.
Symantec™ ApplicationHA Agent for MySQL Configuration Guide	applicationha_mysql_agent_61_ vmware_lin.pdf	Describes how to configure application monitoring for MySQL.
Symantec ApplicationHA Release Notes	applicationha_notes_61_kvm_lin.pdf	Describes the new features and software and system requirements. This document also contains a list of limitations and issues known at the time of the release.

Table 1-5 Symantec ApplicationHA documentation *(continued)*

Document title	File name	Description
Symantec ApplicationHA Installation Guide	applicationha_install_61_kvm_lin.pdf	Describes the steps for installing and configuring Symantec ApplicationHA. Some of the most common troubleshooting steps are also documented in this guide.
Symantec ApplicationHA User's Guide	applicationha_users_61_kvm_lin.pdf	Provides information about configuring and managing Symantec ApplicationHA in Kernel-based Virtual Machine (KVM) virtualization environments. Some of the most common troubleshooting steps are also documented in the guide.
Symantec ApplicationHA Agent for Oracle Configuration Guide	applicationha_oracle_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for Oracle.
Symantec ApplicationHA Generic Agent Configuration Guide	applicationha_gen_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for a generic application.
Symantec ApplicationHA Agent for WebSphere MQ Configuration Guide	applicationha_webspheremq_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for WebSphere MQ.
Symantec ApplicationHA Agent for WebSphere Application Server Configuration Guide	applicationha_websphereas_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for WebSphere Application Server.
Symantec ApplicationHA Agent for DB2 Configuration Guide	applicationha_db2_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for DB2.
Symantec ApplicationHA Agent for Apache HTTP Server Configuration Guide	applicationha_apache_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for Apache HTTP Server.
Symantec™ ApplicationHA Agent for MySQL Configuration Guide (This document is available online)	applicationha_mysql_agent_61_kvm_lin.pdf	Describes how to configure application monitoring for MySQL.
Symantec ApplicationHA Release Notes	applicationha_notes_61_ldom_sol.pdf	Describes the new features and software and system requirements. This document also contains a list of limitations and issues known at the time of the release.

Table 1-5 Symantec ApplicationHA documentation *(continued)*

Document title	File name	Description
Symantec ApplicationHA Installation Guide	applicationha_install_61_ldom_sol.pdf	Describes the steps for installing and configuring product. Some of the most common troubleshooting steps are also documented in this guide.
Symantec ApplicationHA User's Guide	applicationha_users_61_ldom_sol.pdf	Provides information about configuring and managing product in Oracle VM Server for SPARC (OVM) virtualization environments. Some of the most common troubleshooting steps are also documented in the guide.
Symantec ApplicationHA Agent for Oracle Configuration Guide	applicationha_oracle_agent_61_ ldom_sol.pdf	Describes how to configure application monitoring for Oracle.
Symantec ApplicationHA Generic Agent Configuration Guide	applicationha_gen_agent_61_ ldom_sol.pdf	Describes how to configure application monitoring for a generic application.
product Agent for Apache HTTP Server Configuration Guide	applicationha_apache_agent_61_ ldom_sol.pdf	Describes how to configure application monitoring for Apache HTTP Server.
Symantec ApplicationHA Release Notes	applicationha_notes_61_lpar_aix.pdf	Describes the new features and software and system requirements. This document also contains a list of limitations and issues known at the time of the release.
Symantec ApplicationHA Installation Guide	applicationha_install_61_lpar_aix.pdf	Describes the steps for installing and configuring Symantec ApplicationHA. Some of the most common troubleshooting steps are also documented in this guide.
Symantec ApplicationHA User's Guide	applicationha_users_61_lpar_aix. pdf	Provides information about configuring and managing Symantec ApplicationHA in Logical Partition (LPAR) virtualization environments. Some of the most common troubleshooting steps are also documented in the guide.
Symantec ApplicationHA Agent for Oracle Configuration Guide	applicationha_oracle_agent_ 61_lpar_aix.pdf	Describes how to configure application monitoring for Oracle.

Table 1-5 Symantec ApplicationHA documentation *(continued)*

Document title	File name	Description
Symantec ApplicationHA Generic Agent Configuration Guide	applicationha_gen_agent_61_lpar_aix.pdf	Describes how to configure application monitoring for a generic application.
Symantec ApplicationHA Agent for DB2 Configuration Guide	applicationha_db2_agent_61_lpar_aix.pdf	Describes how to configure application monitoring for DB2.
Symantec ApplicationHA Agent for Apache HTTP Server Configuration Guide	applicationha_apache_agent_61_lpar_aix.pdf	Describes how to configure application monitoring for Apache HTTP Server.

Table 1-6 Symantec High Availability Console documentation

Document title	File name	Description
Symantec High Availability Console Release Notes	sha_console_notes_61.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the Symantec High Availability Console. The component is essential to deploy Symantec Cluster Sever (VCS) or Symantec ApplicationHA in a VMware virtual environment by using the VMware vSphere Client GUI.
Symantec High Availability Console Installation and Upgrade Guide	sha_console_install_61.pdf	Provides information required to install or upgrade the Symantec High Availability Console.

Table 1-7 lists the documents that are deprecated in this release.

Table 1-7 Deprecated documents

Deprecated documents	Notes
Symantec VirtualStore Administrator's Guide	Symantec VirtualStore (SVS) functionality moved to the Storage Foundation Cluster File System High Availability (SFCFSHA) product except for the VirtualStore VMware vCenter and View plug-in. SVS VMware vCenter and View plug-in has been discontinued. See the *Symantec Storage Foundation Cluster File System High Availability Administrator's Guide* for more information
Symantec VirtualStore Installation Guide	You can upgrade SVS to SFCFSHA 6.1. See the *Symantec Storage Foundation Cluster File System High Availability Installation Guide* for more information
Symantec VirtualStore Release Notes	See the *Symantec Storage Foundation Cluster File System High Availability Release Notes* for more information