Veritas Storage Foundation™ and High Availability Solutions 6.0.3 Release Notes - Solaris

6.0.3 Maintenance Release

May 2013

Veritas Storage Foundation and High Availability Solutions Release Notes 6.0.3

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

Product version: 6.0.3

Document version: 6.0.3 Rev 4

Legal Notice

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

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

Contents

Chapter 1

About Veritas Storage Foundation and High Availability Solutions

This chapter includes the following topics:

Introduction

This document provides information about the Veritas Storage Foundation and High Availability Solutions 6.0.3 release.

For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:

http://www.symantec.com/docs/TECH164885

The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware visit:

http://www.symantec.com/docs/TECH170013

Before installing or upgrading Veritas Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

This Maintenance Release applies to the following releases of Storage Foundation and High Availability products:

- Storage Foundation and High Availability Solutions 6.0.1

This Maintenance Release is available as 6.0.3.

About the installmr and the uninstallmr scripts

Veritas Storage Foundation and High Availability Solutions 6.0.3 provides an upgrade script.

See "Supported upgrade paths" on page 164.

Symantec recommends that you use the upgrade script. The `installmr` script allows you to upgrade all the patches associated with the packages installed, after which you can reboot to start all of the processes.

The installmr script options

Table 1-1 The command line options for the product upgrade script

Command Line Option	Function
`[ system1 system2... ]`	Specifies the systems on which to run the upgrade options. If not specified, the command prompts for a system name.

Table 1-1 The command line options for the product upgrade script *(continued)*

Command Line Option	Function
`[ -precheck ]`	Use the `-precheck` option to confirm that systems meet the products' installation requirements before the installation.
`[ -postcheck ]`	Use the `-postcheck` option after an installation or upgrade to help you determine installation-related problems and provide troubleshooting information.
`[ -responsefile` *`response_file`* `]`	Use the `-responsefile` option to perform automated installations or uninstallations using information stored in a file rather than prompting for information. *`response_file`* is the full path of the file that contains configuration definitions.
`[ -logpath` *`log_path`* `]`	Use the `-logpath` option to select a directory other than `/opt/VRTS/install/logs` as the location where the installmr log files, summary file, and response file are saved.
`[ -tmppath` *`tmp_path`* `]`	Use the `-tmppath` option to select a directory other than `/var/tmp` as the working directory for `installmr`. This destination is where initial logging is performed and where filesets are copied on remote systems before installation.
`[ -timeout` *`timeout_value`* `]`	Use the `-timeout` option to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the `-timeout` option overrides the default value of 1200 seconds. Setting the `-timeout` option to 0 will prevent the script from timing out. The `-timeout` option does not work with the `-serial` option.
`[ -rootpath` *`root_path`* `]`	Use the `-rootpath` option to re-root the installation of all packages to the given path. On Solaris, -rootpath passes -R *root_path* to pkgadd.

Table 1-1 The command line options for the product upgrade script *(continued)*

Command Line Option	Function
`[ -jumpstart jumpstart_path]`	Use the `-jumpstart` option to generate finish scripts. You can use the finish scripts with the Solaris JumpStart Server to automate installation of all packages and patches for every product. You need to specify an available location to store the finish scripts as a complete path. The `-jumpstart` option is supported on Solaris only.
`[ -keyfile ssh_key_file ]`	Use the `-keyfile` option to specify a key file for SSH. When you use this option the `-i ssh_key_file` is passed to every SSH invocation.
`[ -hostfile hostfile_path ]`	Use the `-hostfile` option to specify the location of a file containing the system names for installer.
`[ -patchpath patch_path ]`	Use the `-patchpath` option to define the complete path of a directory that is available to all install systems (usually NFS mounted) that contains all patches to be installed by `installmr`.
`[ -flash_archive flash_archive_path]`	Use the `-flash_archive` option to generate Flash archive scripts which can be used by Solaris Jumpstart Server for automated Flash archive installation of all packages and patches for every product, an available location to store the post deployment scripts should be specified as a complete path. The `-flash_archive` option is supported on Solaris only.

Table 1-1 The command line options for the product upgrade script *(continued)*

Command Line Option	Function
`[ -serial | -rsh | -redirect | -pkgset | -pkgtable | -pkginfo | -listpatches ]`	Use the `-serial` option to perform installation, uninstallation, start and stop operations, typically performed simultaneously on all systems, in a serial fashion. Use the `-rsh` option when rsh and rcp are to be forced for communication though ssh and scp is also setup between the systems. Use the `-redirect` option to display progress details without showing the progress bar. Use the `-pkgset` option to discover the package set installed on the systems specified. Use the `-pkgtable` option to display product rpms in correct installation order. Use the `-pkginfo` option is used to display the correct installation order of packages and patches. This option is available with or without one of following options: `-allpkgs`, `-minpkgs`, and `-recpkgs`. Use the `-listpatches` option to display product patches in the correct installation order.

Table 1-1 The command line options for the product upgrade script *(continued)*

Command Line Option	Function
[-makeresponsefile | -comcleanup | -version | -nolic]	Use the `-makeresponsefile` option to generate a response file without doing an actual installation. Text displaying install, uninstall, start, and stop actions are simulations. These actions are not being performed on the system. Use the `-comcleanup` option to remove the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated. Use the `-version` option to check the status of installed products on the system. Use the `-nolic` option to install product packages on systems without entering product licenses. Configuration, startup, or installation of license based features are not performed when using this option.
`[-ignorepatchreqs]`	Use the `-ignorepatchreqs` option to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.

Table 1-1 The command line options for the product upgrade script *(continued)*

Command Line Option	Function
`[ -upgrade_kernelpkgs | -upgrade_nonkernelpkgs | -rolling_upgrade | -rollingupgrade_phase1 | -rollingupgrade_phase2]`	The `-upgrade_kernelpkgs` option has been renamed to `-rollingupgrade_phase1`. The `-upgrade_nonkernelpkgs` option has been renamed to `-rollingupgrade_phase2`. Use the `-rolling_upgrade` option to perform rolling upgrade. Using this option, installer will detect the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly. Use the `-rollingupgrade_phase1` option to to perform rolling upgrade phase 1. During this phase, the product kernel packages will be upgraded to the latest version. Use the `-rollingupgrade_phase2` option perform rolling upgrade phase 2. During this phase, VCS and other agent packages will be upgraded to the latest version. During this phase, product kernel drivers will be rolling-upgraded to the latest protocol version.

The uninstallmr script options

Veritas Storage Foundation and High Availability Solutions 6.0.3 provides an uninstallation script.

Note: On Solaris 11, rolling back is not supported.

Symantec recommends that you use the uninstallation script. The `uninstallmr` script uninstalls all the patches associated with packages installed, and starts the processes. Do not use the `uninstall`*`prodvers`* script for rolling back, because it removes the entire stack.

Note: On Solaris 11, the `uninstallmr` script is not supported.

Table 1-2 The command line options for the `uninstallmr` script

Command Line Option	Function
`[ system1 system2... ]`	Specifies the systems on which to run the upgrade options. If not specified, the command prompts for a system name.
`[ -responsefile response_file ]`	Use the `-responsefile`to perform automated installations or uninstallations using information stored in a file rather than prompting for information. *response_file* is the full path of the file that contains configuration definitions.
`[ -logpath log_path ]`	Use the `-logpath` option to select a directory other than `/opt/VRTS/install/logs` as the location where uninstallmr log files, summary file, and response file are saved.
`[ -tmppath tmp_path ]`	Use the `-tmppath` option to select a directory other than `/var/tmp` as the working directory for uninstallmr. This destination is where initial logging is performed and where packages are copied on remote systems before installation.
`[ -timeout <timeout_value> ]`	Use the `-timeout`to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the `-timeout` option overrides the default value of 1200 seconds. Setting the `-timeout` option to 0 will prevent the script from timing out. The `-timeout` option does not work with the `-serial` option.
`[ -keyfile ssh_key_file ]`	Use the `-keyfile` option to specify a key file for SSH. When you use this option the `-i ssh_key_file` is passed to every SSH invocation.
`[ -hostfile hostfile_path ]`	Use the `-hostfile` option to specify the location of a file containing the system names for installer.

Table 1-2 The command line options for the `uninstallmr` script *(continued)*

Command Line Option	Function
`[ -rootpath` *`root_path`* `]`	Use the `-rootpath` option to re-root the installation of all packages to the given path. On Solaris, -rootpath passes -R *root_path* to pkgadd or pkgrm.

Table 1-2 The command line options for the `uninstallmr` script *(continued)*

Command Line Option	Function
`[ -serial | -rsh | -redirect | -listpatches | -makeresponsefile | -comcleanup | -version ]`	Use the `-serial` option to perform install, uninstall, start, and stop operations, typically performed simultaneously on all systems, in serial fashion. Use the `-rsh` option to have the script use rsh and rcp for communication between the systems. System communication using rsh and rcp is auto-detected by the script, so the `-rsh` option is only required when ssh and scp (default communication method) is also configured between the systems. Use the `-redirect` option to have the script display progress details without the use of advanced display functionality so that the output can be redirected to a file. Use the `-listpatches` option to display product patches in correct installation order. Use the `-makeresponsefile` option to generate a response file without doing an actual installation. Text displaying install, uninstall, start, and stop actions are simulations. These actions are not being performed on the system. Use the `-comcleanup` option to remove the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated. Use the `-version` option to have the installer check and report the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable.

Table 1-2 The command line options for the `uninstallmr` script *(continued)*

Command Line Option	Function
`[-ignorepatchreqs]`	Use the `-ignorepatchreqs` option to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.

Overview of the installation and upgrade process

Follow these instructions to make sure that you have the latest patches for the installer before you install or upgrade the product.

To install or upgrade

1. If you are upgrading to 6.0.3, skip to step 2.

   If you are installing 6.0.3 for the first time:

   - Download Storage Foundation and High Availability Solutions 6.0.1 from http://fileConnect.symantec.com.
   - Extract the tar ball into a directory called `/tmp/sfha601`.
   - Check http://sort.symantec.com/patches to see if there are any patches available for the 6.0.1 Installer. Download applicable P-patches and extract them to the `/tmp` directory.
   - Change the directory to `/tmp/sfha601`:

     ```
     # cd /tmp/sfha601
     ```

   - Install the 6.0.1 software. Follow the instructions in the Installation Guide.

     ```
     # ./installer -require complete_path_to_601_installer_patch
     ```

2. Download SFHA 6.0.3 from http://sort.symantec.com/patches and extract it to a directory called `/tmp/sfha603`.

3. Check http://sort.symantec.com/patches to see if there are patches available for the 6.0.3 installer. Download applicable P-patches and extract them to the `/tmp` directory.

4. Change the directory to `/tmp/sfha603`:

   ```
   # cd /tmp/sfha603
   ```

5. Install 6.0.3:

   ```
   # ./installmr -require complete_path_to_603_installer_patch
   ```

Changes introduced in 6.0.3

This section lists the changes in 6.0.3.

Changes introduced in Veritas Cluster Server 6.0.3

This section lists the Veritas Cluster Server changes in 6.0.3.

Db2udb Agent support extended to DB2 10.1

The DB2udb Agent for VCS 6.0.3 now supports DB2 10.1.

VCS support for logical domains with control domain reboot in multiple I/O domain environment

When an OVM 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), guest domain continues to function even if the control domain is shutdown or rebooted, as long as the I/O services from other I/O domain are available.

To use this feature

1. Set the LDom resource attribute DomainFailurePolicy with master domain and it's failure policy to ignore (primary domain will be set with 'stop' failure policy by default).
2. Set the LDom service group attribute `SysDownPolicy` to `AutoDisableNoOffline`.

See "Configuring VCS to manage a Logical Domain using services from multiple I/O domains" on page 221.

The LDom agent has added the following new attribute to support this feature.

DomainFailurePolicy

This attribute specifies the list of master domains and the failure policy of master domains for a guest domain. The key of the attribute is the name of the master domain and the value for the key of the attribute is the failure policy enacted by the master domain on the guest domain. The failure policy will be enacted by the master domain in the event of loss of the master domain. The possible values for the failure policy are ignore, stop, reset, and panic. For more information on the failure policies of the master domain, refer to the *ldm(1M) man page*.

By default, the DomainFailurePolicy attribute is set with master domain as 'primary' and failure policy as 'stop'.

The DomainFailurePolicy attribute need to be set to a non-default value only when the guest domain is provided with storage and network services from more than one I/O domain and the guest domain need to be made available even when the primary domain is rebooted or shut down for maintenance.

It is highly recommended to set the same failure policy for a master domain for all the LDom resources (guest domains) configured on a physical system. If the attribute is set to different failure policies for the same master domain for different LDom resources, then the agent ensures that the failure policy with the highest priority is set on the master domain. For more information on failure policy priority, see Notes for the DomainFailurePolicy attribute.

You can change the attribute value dynamically when the LDom resource is online. The LDom agent ensures the changed failure policy is set on the master domain in the order of priority dynamically, without the need to bring down the LDom resource. For more information on the behavior of this attribute, see the Notes for the DomainFailurePolicy attribute section.

Type-dimension: string-association

Default: {primary = "stop"}

Example: {primary= ignore, secondary = "stop"}. In this example, primary and secondary are the master domains from where storage and network services are exported to the guest domain.

Notes for the DomainFailurePolicy attribute

When the DomainFailurePolicy attribute is set, the LDom agent sets the master domain of the guest domain with the key of the attribute and the value of the key as the failure policy of the guest domain.

The LDom agent uses the following command to set the master for the guest domain:

```
# ldm set-domain master=master-domain guestldom
```

The LDom agent uses the following command to set the failure policy for the master domain:

```
# ldm set-domain failure-policy=failure-policy master-domain
```

As the DomainFailurePolicy attribute is available at the resource level, it is possible to set the failure policy of the master domain to different values for different LDom resources either knowingly or unknowingly. When multiple LDom resources define the failure policy of the same master domain differently, the LDom agent uses internal priority when setting the failure policy of the master domain.

The internal priority is as follows:

- panic: highest
- reset: high
- stop: low
- ignore: lowest

If the failure policy of the master domain is set to a lower priority on the system than the one set in the LDom resource for the DomainFailurePolicy attribute, then the failure policy of the master domain will be changed to the value in the attribute.

If the failure policy of the master domain is set to a higher priority on the system than the one set in the LDom resource for the DomainFailurePolicy attribute, then the failure policy of the master domain will not be changed to the value in the attribute. The LDom agent logs a message to indicate the conflict for the first time.

If the failure policy of the master domain is set to ignore, then the LDom agent does not add the master domain to the master list of the guest domain. If the master domain is part of the masters list of the guest domain, the LDom agent removes the master domain from the masters list.

Note: Symantec does not recommend to set the failure policy of any of the master domains to panic.

Example 1

Failure policy of the master domain (primary) is set to ignore on the system and the DomainFailurePolicy attribute for the LDom resource is changed to { primary = “stop” }. To check whether the failure policy of the master domain (primary) is set to ignore on the system, enter the following command:

```
# ldm list-bindings primary | grep failure-policy
```

In this example, as the internal priority of the LDom agent is assigned to stop and as it is higher than ignore, the failure policy of the primary domain will be changed to stop. The LDom agent uses the following command to change the failure policy of the primary domain to stop:

```
# ldm set-domain failure-policy=stop primary
```

Example 2

Failure policy of the master domain (primary) is set to panic on the system and the DomainFailurePolicy attribute for the LDom resource is changed to { primary = "stop" }. To check whether the failure policy of the master domain (primary) is set to panic on the system, enter the following command:

```
# ldm list-bindings primary | grep failure-policy
```

In this example, as the internal priority of the LDom agent is assigned to stop and as it is lower than panic, the failure policy of the primary domain will be retained as panic.

If the failure policy of a master domain need to be set to a value of lower priority than the value currently set on the system, you must manually execute the `ldm` command. The LDom agent uses the following command to change the failure policy of the primary domain to stop from reset or panic:

```
# ldm set-domain failure-policy=stop primary
```

Example 3

If the value of the failure policy of the master domain is specified as ignore in the DomainFailurePolicy attribute, then the master domain is excluded from the masters list of the guest domain by the LDom agent.

If the masters list of a guest domain contains primary and secondary and if the DomainFailurePolicy attribute of the LDom resource for the guest domain is changed to {primary = ignore, secondary = "stop" }, then the primary domain is removed from the masters list of the guest domain.

Before you change the DomainFailurePolicy attribute, you can enter the following command to check whether the masters list of a guest domain contains primary and secondary:

```
# ldm list-bindings guestldom | grep master
```

The following output shows that the guest domain contains both primary and secondary:

```
master=primary, secondary
```

After you change the DomainFailurePolicy attribute, you can enter the following command to check whether the primary domain is removed from the masters list of the guest domain.

```
# ldm list-bindings guestldom | grep master
```

The following output shows that the primary domain is removed from the masters list:

```
master= secondary
```

For use case scenarios and for VCS configuration where the DomainFailurePolicy attribute must be set, refer to the *Veritas Storage Foundation and High Availability Solutions Virtualization Guide*.

System requirements

This section describes the system requirements for this release

Supported Solaris operating systems

Table 1-3 shows the supported operating systems for this release.

Table 1-3 Supported operating systems

Operating systems	Levels	Chipsets
Solaris 10	Update 8, 9, 10 and 11	SPARC
Solaris 10	Update 8, 9, 10 and 11	x64
Solaris 11	Solaris 11 SRU1, Solaris 11.1	SPARC
Solaris 11	Solaris 11 SRU1, Solaris 11.1	x64

Supported Oracle VM for SPARC versions are 2.0, 2.1, 2.2 and 3.0.

If necessary, upgrade Solaris before you install the Veritas products.

See http://www.symantec.com/docs/TECH202397 before upgrading to Oracle Solaris 11.1.

Install all the latest required Solaris patches listed in this *Release Notes*.

See "Required Solaris patches" on page 27.

For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:

http://www.symantec.com/docs/TECH75362

Required Solaris patches

Before installing Veritas product, ensure that the correct Solaris patches are installed.

See http://support.oracle.com for the latest Solaris patch updates.

The following patches (or a later revision of those patches) are required for Solaris SPARC:

Table 1-4 Solaris SPARC patches

Operating system	Oracle patch number
Solaris 10	119254-06 119042-02 125731-02 128306-05 127111-01

The following patches (or a later revision of those patches) are required for Solaris x64:

Table 1-5 Solaris x64 patches

Operating system	Oracle patch number
Solaris 10	118344-14 118855-36 119043-11 119131-33 120012-14 125732-05 127128-11

VMware Environment

For information about the use of this product in a VMware Environment, refer to http://www.symantec.com/docs/TECH51941

Note: This TechNote includes information specific to all 5.1 releases. Please check this technote for the latest information.

Database requirements

The following TechNote identifies the most current information on supported databases (Oracle Single Instance, DB2, and Sybase) and operating system combinations:

http://www.symantec.com/docs/DOC4039

Note: Veritas Storage Foundation (SF) and Veritas Storage Foundation Cluster File System (SFCFS) do not support running SFDB tools with Sybase, but they support running Oracle and Sybase on VxFS and VxVM.

http://www.symantec.com/docs/TECH44807

Veritas Storage Foundation memory requirements

Symantec recommends 2 GB of memory over the minimum requirement for the operating system.

Disk space requirements

Before installing your products, confirm that your system has enough free disk space.

Use the **Perform a Pre-installation Check (P)** menu for the Web-based installer to determine whether there is sufficient space.

Or, go to the installation directory and run the installer with the `-precheck` option.

```
# ./installmr -precheck
```

See “About the installmr and the uninstallmr scripts” on page 12.

Number of nodes supported

SFHA supports cluster configurations with up to 64 nodes.

List of products

Apply these patches for the following Veritas Storage Foundation and High Availability products:

- Veritas Dynamic Multi-Pathing (DMP)
- Veritas Volume Manager (VM)

- Veritas File System (FS)
- Veritas Storage Foundation (SF)
- Veritas Cluster Server (VCS)
- Veritas Storage Foundation and High Availability (SFHA)
- Veritas Storage Foundation Cluster File System and High Availability (SFCFSHA)
- Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)
- Veritas Storage Foundation for Sybase ASE CE (SFSYBASECE)
- Symantec VirtualStore (SVS)

Fixed issues

This section describes the issues fixed in 6.0.3.

See the `README_SYMC.`*`xxxxx-xx`* files in the `/patches` directory on the installation media for the symptom, description, and resolution of the fixed issue.

- Installation and upgrades fixed issues
- Veritas Dynamic Multi-pathing fixed issues
- Veritas Storage Foundation fixed issues
- Veritas Cluster Server fixed issues
- Veritas Storage Foundation and High Availability fixed issues
- Veritas Storage Foundation for Oracle RAC 6.0.3 fixed issues
- Veritas Storage Foundation Cluster File System High Availability fixed issues

Installation and upgrades fixed issues

This section describes the installation and upgrade issues fixed in 6.0.3.

Installation and upgrades: issues fixed in 6.0.3

This section describes the installation and upgrade issues fixed in 6.0.3.

Table 1-6 Installation and upgrades 6.0.3 fixed issues

Fixed issues	Description
2967125	Eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to execute arbitrary commands via the new constructor.
2880917	Veritas product services do not get enabled after phased upgrade.

Veritas Dynamic Multi-pathing fixed issues

See Veritas Volume Manager fixed issues for the Veritas Dynamic Multi-pathing fixed issues in 6.0.3.Veritas Volume Manager fixed issues inlcudes both the VxVM fixed issues and DMP issues.

Veritas Storage Foundation fixed issues

This section describes the Veritas Storage Foundation fixed issues in 6.0.3.

- Veritas Volume Manager fixed issues
- Veritas File System fixed issues
- Veritas Storage Foundation for Databases (SFDB) tools fixed issues

Veritas Volume Manager fixed issues

This section describes Veritas Volume Manager fixed issues in 6.0.3.

Veritas Volume Manager: issues fixed in 6.0.3

Table 1-7 describes the incidents that are fixed in Veritas Volume Manager in 6.0.3.

Table 1-7 Veritas Volume Manager 6.0.3 fixed issues

Fixed issues	Description
3002770	Accessing NULL pointer in dmp_aa_recv_inquiry() caused system panic
2970368	Enhancing handling of SRDF-R2 WD devices in DMP.
2965910	vxassist dump core with the `-o ordered` option.
2964547	About DMP message - cannot load module 'misc/ted'.

Table 1-7 Veritas Volume Manager 6.0.3 fixed issues *(continued)*

Fixed issues	Description
2962262	Uninstallation of DMP fails in presence of other multi-pathing solutions.
2948172	Executing the `vxdisk -o thin,fssize list` command can result in panic.
2942609	Message displayed when user quits from Dynamic Reconfiguration Operations is shown as error message.
2940446	Full fsck hangs on I/O in VxVM when cache object size is very large
2935771	In the VVR environment, RLINK disconnects after master switch.
2933138	panic in voldco_update_itemq_chunk() due to accessing invalid buffer
2930569	The LUNs in 'error' state in output of 'vxdisk list' cannot be removed through DR (Dynamic Reconfiguration) Tool.
2930396	vxdmpasm command can not work on the solaris10_x64 platform
2919720	vxconfigd core in rec_lock1_5()
2919714	exit code from vxevac is zero when migrating on thin luns but FS is not mounted
2919627	Dynamic Reconfiguration tool should be enhanced to remove LUNs feasibly in bulk.
2919318	The I/O fencing key value of data disk are different and abnormal in a VCS cluster with I/O fencing.
2916094	Enhancements have been made to the Dynamic Reconfiguration Tool(DR Tool) to create a separate log file every time DR Tool is started, display a message if a command takes longer time, and not to list the devices controlled by TPD (Third Party Driver) in 'Remove Luns' option of DR Tool.
2915751	Solaris machine panics during dynamic lun expansion of a CDS disk.
2915063	Rebooting VIS array having mirror volumes, master node panicked and other nodes CVM FAULTED
2911040	Restore from a cascaded snapshot when its source is DETACHED leaves the volume in unusable state
2910043	Avoid order 8 allocation by vxconfigd in node reconfig.

Table 1-7 Veritas Volume Manager 6.0.3 fixed issues *(continued)*

Fixed issues	Description
2907823	If the user removes the lun at the storage layer and at VxVM layer beforehand, DMP DR tool is unable to clean-up cfgadm (leadville) stack.
2899173	vxconfigd hang after executing the `vradmin stoprep` comand.
2898547	vradmind on VVR Secondary Site dumps core, when Logowner Service Group on VVR (Veritas Volume Replicator) Primary Site is shuffled across its CVM (Clustered Volume Manager) nodes.
2892983	vxvol dumps core if new links are added while the operation is in progress.
2886402	vxconfigd hang while executing tc ./scripts/ddl/dmpapm.tc#11
2886333	The `vxdg(1M) join` command should not allow mixing clone and non-clone disks in a DiskGroup.
2878876	vxconfigd dumps core in vol_cbr_dolog() due to race between two threads processing requests from the same client.
2875962	During the upgrade of VRTSaslapm package, a conflict is encountered with VRTSvxvm package because an APM binary is included in VRTSvxvm package which is already installed
2869594	Master node panics due to corruption if space optimized snapshots are refreshed and 'vxclustadm setmaster' is used to select master.
2866997	Initializing using vxdisksetup -i and Solaris patch 147440-20 gives error VxVM vxdisksetup ERROR V-5-2-43 : Invalid disk device for vxdisksetup
2866059	Improving error messages hit during the `vxdisk resize` operation.
2859470	SRDF R2 with EFI label is not recognized by VxVM and showing in error state
2858853	vxconfigd coredumps in dbf_fmt_tbl on the slave node after a Master Switch if you try to remove a disk from the DG
2851403	The `vxportal` and `vxfs` processes are failed to stop during first phase of rolling upgrade.
2851085	DMP doesn't detect implicit LUN ownership changes for some of the dmpnodes
2837717	The `vxdisk(1M) resize` command fails if `da name` is specified.
2836798	Prevent DLE on simple/sliced disk with EFI label

Table 1-7 Veritas Volume Manager 6.0.3 fixed issues *(continued)*

Fixed issues	Description
2836528	vxdisk resize is failing with error: "resize failed: New geometry makes partition unaligned"
2834046	NFS migration failed due to device reminoring.
2833498	vxconfigd hangs while reclaim operation is in progress on volumes having instant snapshots
2826125	VxVM script daemon is terminated abnormally when it is invoking with exact the same process id of the last invocation.
2815517	vxdg adddisk should not allow mixing clone & non-clone disks in a DiskGroup
2807158	On Solaris platform, sometimes system can hang during VM upgrade or patch installation.
2801962	Grow of a volume takes significantly large time when the volume has version 20 DCO (Data Change Object) attached to it
2798673	System panics in voldco_alloc_layout() while creating volume with instant DCO
2779580	Secondary node gives configuration error (no Primary RVG) after reboot of master node on Primary site.
2753954	At cable disconnect on port1 of dual-port FC HBA, paths via port2 are also marked SUSPECT
2744004	vxconfigd is hung on the VVR secondary node during VVR configuration.
2742706	Panic due to mutex not being released in vxlo_open
2715129	vxconfigd hangs during Master takeover in a CVM (Clustered Volume Manager) environment.
2692012	The vxevac move error message needs to be enhanced to be less generic and give clear message for failure.
2619600	Live migration of virtual machine having SFHA/SFCFSHA stack with data disks fencing enabled, causes service groups configured on virtual machine to fault.
2567618	VRTSexplorer coredumps in vxcheckhbaapi/print_target_map_entry
2510928	Extended attributes for SRDF luns reported as Mirror with EMC (VMAX array)

Table 1-7 Veritas Volume Manager 6.0.3 fixed issues *(continued)*

Fixed issues	Description
2398416	vxassist dumps core while creating volume after adding attribute "wantmirror=ctlr" in default vxassist rulefile
2273190	Incorrect setting of UNDISCOVERED flag can lead to database inconsistency
2149922	Record the diskgroup import and deport events in syslog
2000585	The `vxrecover -s` command does not start any volumes if a volume is removed whilst it is running.
1982965	vxdg import fails if da-name is based on naming scheme which is different from the prevailing naming scheme on the host
1973983	vxunreloc fails when dco plex is in DISABLED state
1903700	vxassist remove mirror does not work if nmirror and alloc is specified on VxVM 3.5
1901838	Incorrect setting of Nolicense flag can lead to dmp database inconsistency.
1859018	The `link detached from volume` warnings are displayed when a linked-breakoff snapshot is created.
1856733	Support for FusionIO on Solaris x64
1725593	The `vxdmpadm listctlr` command has to be enhanced to print the count of device paths seen through the controller.
1289985	vxconfigd core dumps upon running the `vxdctl enable` command.

Veritas File System fixed issues

This section describes Veritas File System fixed issues in 6.0.3.

Veritas File System: issues fixed in 6.0.3

Table 1-8 describes the incidents that are fixed in Veritas File System in 6.0.3.

Table 1-8 Veritas File System 6.0.3 fixed issues

Fixed issues	Description
3018869	On Solaris 11 update 1, the fsadm command shows that the mountpoint is not a vxfs file system.

Table 1-8 Veritas File System 6.0.3 fixed issues *(continued)*

Fixed issues	Description
3013950	Internal assert "f:vx_info_init:2" is hit during Solaris 11 update 1 validation.
2905820	process hangs during file system access
2895743	Accessing named attributes for some files seems to be slow.
2885592	vxdump to the vxcompress file system is aborted.
2881211	File ACLs not preserved in checkpoints properly if file has hardlink.
2858683	Reserve extent attributes changed after vxrestore, only for files greater than 8192bytes.
2857751	The internal testing hits the assert "f:vx_cbdnlc_enter:1a".
2857629	File system corruption can occur requiring a full fsck of the system.
2827751	When ODM is used with non-VxVM devices high kernel memory allocation is seen.
2806466	fsadm -R resulting in panic at LVM layer due to vx_ts.ts_length set to 2GB.
2756779	Write and read performance concerns on CFS when running applications that rely on posix file-record locking (fcntl).
2624262	fsdedup.bin hit oops at vx_bc_do_brelse.

Veritas Storage Foundation for Databases (SFDB) tools fixed issues

This section describes Veritas Storage Foundation for Databases (SFDB) tools fixed issues in 6.0.3.

Veritas Storage Foundation for Databases (SFDB) tools: issues fixed in 6.0.3

Table 1-9describes the incidents that are fixed in Veritas Storage Foundation for Databases (SFDB) tools in 6.0.3.

Table 1-9 Veritas Storage Foundation for Databases (SFDB) tools 6.0.3 fixed issues

Fixed issues	Description
3030663	`dbed_vmclonedb` does not read pfile supplied by `-p 'pfile_modification_file'` option.

Veritas Cluster Server fixed issues

This section describes the Veritas Cluster Server software limitations in 6.0.3.

Veritas Cluster Server: issues fixed in 6.0.3

Table 1-10describes the incidents that are fixed in Veritas Cluster Server in 6.0.3.

Table 1-10 Veritas Cluster Server 6.0.3 fixed issues

Fixed issues	Description
3025931	Sometimes gab module does not get loaded after system reboot automatically. We have to remove the driver manually and add it back to make it work.
3013962	Monitor fails to detect DB2 resource online for DB2 version 10.1.
3013940	If DB2 is installed in NON-MPP mode and UseDB2Start attribute is set to 0, we still use db2start command to start the DB2 process instead of using db2gcf command.
2980002	High availability support for logical domain when control domain is down with multiple I/O domains in Oracle VM (OVM) for SPARC environment.
2979745	`MultiNICA` is unable to detect Network connectivity lost.
2967536	MonitorProgram of Application does not work correctly with C shell of User environment.
2964772	If you take an NFSRestart resource offline, the NFSRestart agent may unexpectedly stop NFS processes in a local container Zones.
2941155	Group is not marked offline on faulted cluster in a GCO environment after a cluster failure is declared.
2937673	AMF driver panics the machine when amfstat is executed.
2861253	In vxfen driver log statement, jeopardy membership is printed as garbage.

Table 1-10 Veritas Cluster Server 6.0.3 fixed issues *(continued)*

Fixed issues	Description
2848009	AMF panicks the machine when an Agent is exiting.
2848005	VCS SMF service goes into maintenance state on a two-node cluster.
2737653	Incorrect descriptions about the RVGPrimary online script .
2736627	REMOTE CLUSTER STATE remains in INIT state and Icmp heartbeat status is UNKNOWN.

Veritas Storage Foundation and High Availability fixed issues

For fixed issues of Veritas Storage Foundation and High Availability in this release, see Veritas Storage Foundation fixed issues and Veritas Cluster Server fixed issues.

Veritas Storage Foundation for Oracle RAC 6.0.3 fixed issues

There are no issues fixed in SF Oracle RAC 6.0.3.

Veritas Storage Foundation Cluster File System High Availability fixed issues

This section describes the Veritas Storage Foundation Cluster File System High Availability fixed issues in 6.0.3.

Veritas Storage Foundation Cluster File System High Availability: issues fixed in 6.0.3

Table 1-11 describes the Veritas Storage Foundation Cluster File System fixed issues in 6.0.3.

Table 1-11 Veritas Storage Foundation Cluster File System High Availability 6.0.3 fixed issues

Fixed issues	Description
2977697	vx_idetach generated kernel core dump while filestore replication is running.
2942776	Mount fails when volumes in vset is not ready.
2923867	Internal test hits an assert "f:xted_set_msg_pri1:1".

Table 1-11 Veritas Storage Foundation Cluster File System High Availability 6.0.3 fixed issues *(continued)*

Fixed issues	Description
2923105	The upgrade VRTSvxfs5.0MP4HFaf hang at vxfs preinstall scripts.
2916691	Customer experiencing hangs when doing dedups.
2906018	The vx_iread errors are displayed after successful log replay and mount of the file system.
2843635	Internal testing is having some failures.
2841059	full fsck fails to clear the corruption in attribute in ode 15.
2750860	Performance issue due to CFS fragmentation in CFS cluster.
2715175	It takes 30 minutes to shut down a 4-node cluster.

Known issues

This section covers the known issues in 6.0.3 and 6.0.1.

- Issues related to installation and upgrade
- Veritas Dynamic Multi-pathing known issues
- Veritas Storage Foundation known issues
- Veritas Cluster Server known issues
- Veritas Storage Foundation and High Availability known issues
- Veritas Storage Foundation Cluster File System High Availability known issues
- Veritas Storage Foundation for Oracle RAC known issues
- Veritas Storage Foundation for Sybase ASE CE known issues
- Symantec VirtualStore known issues

Issues related to installation and upgrade

This section describes the known issues during installation and upgrade in 6.0.3 and 6.0.1.

During Live Upgrade, installer displays incorrect message about VRTSaa package removal (1710504)

If you use Live Upgrade to upgrade SF 5.0MP1 to SF 6.0.1, the installer may display a message that the VRTSaa package failed to uninstall.

Workaround: Verify whether the `VRTSaa` package was removed correctly from the alternate boot disk.

```
# pkginfo -R alternate_root_path -l VRTSaa
```

For example, run the following command

```
# pkginfo -R /altroot.5.10 -l VRTSaa
```

If the VRTSaa package was removed, you can ignore this error.

If the VRTSaa package was not removed, remove the package manually:

```
# pkgrm -R alternate_root_path -l VRTSaa
```

For example, run the following command

```
# pkgrm -R /altroot.5.10 -l VRTSaa
```

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

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

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

Live Upgrade to Solaris 10 Update 10 fails in the presence of zones (2521348)

SFCFSHA Live Upgrade from Solaris 10 Update 7 5.1SP1 to Solaris 10 Update 10 using the `vxlustart` commands fails in the presence of zones with the following error message:

```
ERROR: Installation of the packages from this media of the media failed;
pfinstall returned these diagnostics:
Processing default locales
        - Specifying default locale (en_US.ISO8859-1)
```

```
Processing profile
ERROR: This slice can't be upgraded because of missing usr packages for
the following zones:
ERROR:    zone1
ERROR:    zone1
ERROR: This slice cannot be upgraded because of missing usr packages for
one or more zones.
The Solaris upgrade of the boot environment <dest.27152> failed.
```

This is a known issue with the Solaris `luupgrade` command.

Workaround: Check with Oracle for possible workarounds for this issue.

Live Upgrade to 6.0.1 on Solaris 10 with dmp_native_support enabled fails (2632422)

During Live Upgrade to 6.0.1 on Solaris 10, the `vxlustart` command fails if `dmp_native_support` is enabled. Veritas Dynamic Multi-Pathing (DMP) support for native devices requires that the naming scheme be set to enclosure-based naming (EBN). DMP 6.0.1 does not allow changing the naming scheme from EBN when support for native devices is enabled.

Due to a bug in DMP 5.1 Service Pack 1 (5.1SP1), the naming scheme could be set to operating-system based naming (OSN). However, this is not a supported configuration. With the naming scheme set to OSN, the `vxlustart` command fails.

Workaround: Disable `dmp_native_support` on all nodes.

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

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

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

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

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

If you install or configure SF and then close the Web installer, if you have other browser windows open, the Web installer does not ask for authentication in the subsequent sessions. Since there is no option to log out of the Web installer, the session remains open as long as the browser is open on the system.

Workaround: Make sure that all browser windows are closed to end the browser session and subsequently log in again.

Stopping the Web installer causes Device Busy error messages (2633924)

If you start the Web installer, and then perform an operation (such as prechecking, configuring, or uninstalling), you may get an error message saying the device is busy.

Workaround: Do one of the following:

- Kill the start.pl process.
- Start the webinstaller again. On the first Web page you see that the session is still active. Either take over this session and finish it or terminate it directly.

Perl module error on completion of SF installation (2873102)

When you install, configure, or uninstall SF, the installer prompts you to optionally upload installation logs to the Symantec Web site. If the installer encounters connectivity problems, you may see an error similar to the following:

```
Status read failed: Connection reset by peer at
<midia_path>/../perl/lib/5.14.2/Net/HTTP/Methods.pm line 269.
```

Workaround:

Ignore this error. It is harmless.

Installed 5.0 MP3 without configuration, then upgrade to 6.0.1, installer cannot continue (2016346)

If you install the 5.0 MP3 release without configuring the product, then you cannot upgrade to the 6.0.1 release. This upgrade path is not supported.

Workaround: Uninstall 5.0 MP3, and then install 6.0.1.

On Sparc, Live Upgrade from Solaris 9 to Solaris 10 Update 10 may fail (2424410)

On Sparc, Live Upgrade from Solaris 9 to Solaris 10 Update 10 may fail with the following error:

```
Generating file list.
Copying data from PBE <source.24429> to ABE <dest.24429>.
99% of filenames transferredERROR: Data duplication process terminated
unexpectedly.
ERROR: The output is </tmp/lucreate.13165.29314/lucopy.errors.29314>.

29794 Killed
Fixing zonepaths in ABE.
Unmounting ABE <dest.24429>.
100% of filenames transferredReverting state of zones in PBE
<source.24429>.
ERROR: Unable to copy file systems from boot environment <source.24429>
to BE <dest.24429>.
ERROR: Unable to populate file systems on boot environment <dest.24429>.
Removing incomplete BE <dest.24429>.
ERROR: Cannot make file systems for boot environment <dest.24429>.
```

This is a known issue with the Solaris `lucreate` command.

Workaround: Install Oracle patch 113280-10,121430-72 or higher before running `vxlustart`.

During upgrade from 5.1SP1 to 6.0.1 with an encapsulated root disk, splitting the root mirror fails if the target disk group name is used by a deported disk group (2280560)

During an upgrade from SF 5.1 SP1 to SF 6.0.1 with an encapsulated root disk, splitting the root mirror fails if the target disk group name for the split operation is used by an existing deported disk group.

Workaround:

Specify a different disk group name as a target for the split operation.

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

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

Workaround:

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

To unfreeze the service groups manually

1. List all the frozen service groups

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

2. Unfreeze all the frozen service groups:

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

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

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

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

After a locale change restart the vxconfig daemon (2417547)

You need to restart the vxconfig daemon you change the locale of nodes that use it. The vxconfig daemon starts at boot. If you have changed locale, you need to restart the daemon.

Workaround: Refer to the *Veritas Storage Foundation Cluster File System High Availability Administrator's Guide* for the section, "vxconfigd daemon recovery."

After performing a manual rolling upgrade, make sure the CVM is online on all nodes without errors (2595441)

Make sure that the CVM is online on all nodes without errors after you perform the first phase of a manual rolling upgrade. The CVM protocol version will not upgrade successfully on the nodes where CVM is offline or has errors.

If the CVM protocol version does note upgrade successfully, upgrade the CVM protocol on the CVM master node.

To upgrade the CVM protocol on the CVM master node

1 Find out which node is the CVM master:

```
# vxdctl -c mode
```

2 On the CVM master node, upgrade the CVM protocol:

```
# vxdctl upgrade
```

Unable to stop some SF processes (2329580)

If you install and start SF, but later configure SF using `installvcs601`, some drivers may not stop successfully when the installer attempts to stop and restart the SF drivers and processes. The reason the drivers do not stop is because some dependent SF processes may be in the running state.

Workaround: To re-configure the product, use the corresponding `install`*`productversion`* command to re-configure the product. Otherwise some processes may fail to stop or start.

For example, use `installsfrac601` to re-configure SF rather than using `installvcs601`.

The vxdisksetup command fails to initialize disks in cdsdisk format for LDOM disks greater than 1 TB (2557072)

The `vxdisksetup` command fails to initialize disks in `cdsdisk` format for LDOM disks greater than 1 TB. This issue is due to an LDOM operating system command which fails when the number of partitions in the GUID partition table (GPT) label is greater than 9. The `cdsdisk` format requires at least 128 partitions to be compatible with Linux systems.

Workaround: There is no workaround for this issue.

Verification of Oracle binaries incorrectly reports as failed during Oracle Grid Infrastructure installation

The verification of Oracle binaries may incorrectly report as failed during the Oracle Grid Infrastructure installation using the SF installer. The message is erroneously reported due to a break in passwordless SSH communication. The SSH communication fails because execution of the `root.sh` script changes the owner of the operating system root directory to the grid user directory.

Issues with keyless licensing reminders after upgrading VRTSvlic [2141446]

After upgrading from 5.1 to higher versions of VCS, some keyless licenses may be left in the system. As a result, you may see periodic reminders being logged if the VOM server is not configured.

This happens if you are using keyless licenses before upgrading to 5.1SP1 or higher versions of VCS. After the upgrade, you install real keys and run `vxkeyless set NONE`. In this case, the keyless licenses may not be completely removed and you see warning messages being logged after two months (if VOM server is not configured). This does not result in any functionality impact.

To resolve this issue, perform the following steps:

1. Note down the list of products configured on the node for keyless licensing. Run `vxkeyless display` to display the list.
2. Set the product level to *NONE* with the command:

   ```
   # vxkeyless set NONE
   ```

3. Find and delete the keyless licenses left over in the system. To do this, perform the following steps for every key stored in `/etc/vx/licenses/lic`:
   - Verify if the key has `VXKEYLESS` feature Enabled using the following command:

     ```
     # vxlicrep -k <license_key> | grep VXKEYLESS
     ```

   - Delete the key if and only if `VXKEYLESS` feature is Enabled.

   Note: When performing the search, do not include the .vxlic extension as part of the search string.

4. Restore the previous list of products with the command:

   ```
   # vxkeyless set product1[|,product]
   ```

Instaling VRTSvlic package on Solaris system with local zones displays error messages [2555312]

If you try to install VRTSvlic package on a Solaris system with local zones in installed state, the system displays the following error messages:

```
cp: cannot create /a/sbin/vxlicinst: Read-only file system
cp: cannot create /a/sbin/vxlicrep: Read-only file system
cp: cannot create /a/sbin/vxlictest: Read-only file system
```

Workaround: On the Solaris system, make sure that all non-global zones are started and in the running state before you install the VRTSvlic package.

VRTSvcsea package cannot be uninstalled from alternate disk in manual live upgrade

Description: In manual live upgrade procedure from 5.1x to 5.1SP1 , all packages are copied to an alternate root disk. However, VRTSvcsea package cannot be uninstalled from alternate disk to upgrade it to 5.1SP1.

Workaround : Instead of removing the VRTSvcsea package, you must apply a patch to upgrade this package to 5.1SP1 version.

VCS Zone users must be added after upgrade to VCS 6.0

If you upgrade your configuration containing Zone resources to VCS 6.0 from:

- VCS 5.1SP1RP1 or later VCS releases with DeleteVCSZoneUser attribute of Zone agent set to 1
- VCS 5.1SP1 or ealier VCS releases

You may see the following issue.

Zone agent offline/clean entry points delete VCS Zone users from configuration. After upgrade to VCS 6.0, VCS Zone users need to be added to the configuration. VCS Zone users can be added by running `hazonesetup` utility with new syntax after upgrade. See the *Veritas Storage Foundation and High Availability Solutions Virtualization Guide* for Solaris for more information on `hazonesetup` utility and see the *Veritas Storage Foundation and High Availability Solutions Virtualization Guide* for Solaris.

VCS installation with CPI fails when a non-global zone is in installed state and zone root is not mounted on the node (2731178)

On Solaris 10, CPI tries to boot a zone in installed state during installation/ or uninstallation. The boot fails if the underlying storage for zone root is not imported and mounted onto the node, causing the installation or uninstallation to fail.

Workaround: Make sure that the non-global zones are in running or configured state when CPI is invoked for installation or uninstallation.

Lack of install script to configure product after installing sfcfsha6.0.1 (2978290)

For Solaris11 U1, there are no install scripts in the `/opt/VRTS/install` directory to configure the SF product.

Workaround:

On Solaris 11 U1, install 6.0.1, upgrade to 6.0.3 and then configure the product using the newly generated `install` scripts under `/opt/VRTS/install`.

The svc:/system/VRTSperl-runonce:default SMF service in the maintenance state (3089938)

After upgrade from 6.0.1 to 6.0.3 on Solaris 11 SPARC, the svc:/system/VRTSperl-runonce:default SMF service may be in the maintenance state.

Workaround:

If you find the svc:/system/VRTSperl-runonce:default SMF service in the maintenance state, perform the following steps:

1. `# svcadm disable svc:/system/VRTSperl-runonce:default`

2. `# svccfg delete -f svc:/system/VRTSperl-runonce:default`

Also you can ignore the following message from the console:

```
svc.startd[11]: svc:/system/VRTSperl-runonce:default: Method
"/opt/VRTSperl/bin/runonce" failed with exit status 127
```

SF failed to upgrade when Application HA is installed (3088810)

If you have installed both ApplicationHA 6.0 and SF 6.0.1, the installer can’t upgrade SF 6.0.1 to 6.0.3. The following error message is displayed:

```
CPI ERROR V-9-30-1303 SFHA 6.0.100 does not appear to be installed
on <your system>
```

Workaround:

Use the following command to specify the exact product for the upgrade:

```
# ./installmr -prod SF60
```

Ignore the warning message that SFHA is already installed after the pre-check and continue the upgrade.

Enabling or installing DMP for native support might not migrate LVM volumes to DMP (2737452)

The `lvm.conf` file has the `obtain_device_list_from_udev` variable. If `obtain_device_list_from_udev` is set to 1, then LVM uses devices and symlinks specified by udev database, only.

Workaround:

In the `lvm.conf` file, set the `obtain_device_list_from_udev` variable to `0`. This enables LVM to recognize `/dev/vx/dmp/` devices when performing a `vgscan`, which enables volume group migration to succeed.

Veritas Dynamic Multi-pathing known issues

This section describes the Veritas Dynamic Multi-pathing known issues in 6.0.3 and 6.0.1.

Creating a zpool fails with a incorrect disk size error (2277875)

When the tunable parameter dmp_native_support is turned on, creating a zpool on DMP devices may fail with the following error:

```
one or more devices is less than the minimum size (64 M)
```

This error may occur even if the device size is greater than the required minimum size.

Workaround:

To resolve this issue, use one of the following commands:

- `# vxdisk scandisks`
- `# format -e dmp_device`

DMP aggregates EFI labelled LUNS to a 0_0 disk (2558408)

While performing `vxdiskunsetup` of some luns, if you format and label the disks as EFI, all the EFI labelled luns are aggregated to a 0_0 disk.

Workaround:

When changing the label of a disk from SMI to EFI, or vice-versa, Symantec recommends that the label be changed on all accessible paths to a disk. That is, use the `format -e` command to stamp the new label on all accessible paths. For Active/Passive (A/P) class of arrays, this should be done only on the active paths. For other arrays, all paths should be labeled.

Symantec also recommends the installation of the patch provided by Oracle for EFI label issues (IDR144101-01 or IDR144249-01 or release kernel patch 142909-17). If this patch is installed, you can run the `format -e` command only on one path. After that, perform a read operation (such as `dd if=/dev/rdsk/<path> of=/dev/null count=1`) on the other accessible paths to propagate the label.

Splitting a mirror from a zpool causes a core dump (2273367)

The following operation to split a mirror from a zpool fails:

```
# zpool split my_pool new_pool mirror
```

This issue is an Oracle issue with zpool. This issue occurs whether DMP is controlling the devices or not. That is, whether the dmp_native_support tunable is on or off.

Suppressing the primary path of an encapsulated SAN boot disk from Veritas Volume Manager causes the system reboot to fail (1933631)

If you suppress the primary path of an array from VxVM control and then reboot the system, the system boot fails.

If you have an encapsulated SAN boot device with multiple primary paths, the issue occurs when you suppress the first primary path. When you configure a SAN boot device, the primary path is set as a boot device. In general, the first path of the SAN boot device corresponds to the first configured path during SAN boot. Even if another primary path is configured as a boot device, suppressing the first device from VxVM causes the boot to fail.

Workaround:

When the boot device is suppressed from VxVM, change the OS boot device sequencing accordingly.

For Solaris SPARC system, use the `eeprom` *`boot-device`* command to set the boot device sequencing.

For Solaris x86-64 systems, use the `eeprom` *`bootpath`* command to set the boot device sequencing.

Adding a DMP device or its OS device path as a foreign disk is not supported (2062230)

When DMP native support is enable, adding a DMP device or its OS device path as a foreign disk using the `vxddladm addforeign` command is not supported. Using this command can lead to unexplained behavior.

ZFS pool creation on a DMP device fails when the LUN size is between 1 TB and 2TB (2010919)

Creating a ZFS pool on a DMP device using the whole disk of size > 1TB and < 2TB that contains a SMI SUN label fails. The issue is that zpool create on a whole disk changes the device label from SMI to EFI. This causes confusion between the OS device paths of the same DMP device due to a bug in the Sun SCSI layer. This is due to SUN BugID: 6912703.

After changing the preferred path from the array side, the secondary path becomes active (2490012)

For EVA arrays, DMP requires that the prefer bit is static. If the prefer bit is not static, issues like the following may occur. After changing the prefer path of LUN from the array side, and performing a disk discovery (`vxdisk scandisks`) from the host, the secondary path becomes active for the LUN.

Workaround:

To work around this issue

1. Set the pref bit for the LUN.
2. Perform disk discovery again:

```
# vxdisk scandisks
```

Continuous trespass loop when a CLARiiON LUN is mapped to a different host than its snapshot (2761567)

If a CLARiiON LUN is mapped to a different host than its snapshot, a trespass on one of them could cause a trespass on the other. This behavior could result in a loop for these LUNs, as DMP tries to fail back the LUNs if the primary paths are available.

Workaround:

To avoid this issue, turn off the `dmp_monitor_ownership` tunable:

```
# vxdmpadm settune dmp_monitor_ownership=off
```

After excluding devices managed by PowerPath from VxVM, the devices still show as DMP devices (2494632)

The issue happens after EMC PowerPath is installed and all devices are under PowerPath control. If you want to maintain the devices under PowerPath control, you use the following command to exclude the device that is managed by PowerPath from VxVM:

```
# vxdmpadm exclude dmpnodename=PowerPath_device _name
```

After system reboot, the PowerPath device still shows as a DMP device, although the device is managed by EMC PowerPath.

Workaround:

This issue is seen only during the first bootup discovery after reboot. To resolve the issue, manually trigger DMP device discovery:

```
 # vxdisk scandisks
```

The system may hang with Solaris 11 SRU1 (2876211)

When running Solaris 11 SRU1, the system may hang due to an Oracle bug. The Oracle Bug ID is 7105131 deadman panic.

Workaround: SRU1 for Solaris 11 should be updated to SRU2a. The bug is fixed in SRU2a: Oracle Solaris 11 Support Repository Updates (SRU) Index (Doc ID 1372094.1)

System panics because dmp_signal_event() called psignal() with incorrect vxesd proc pointer (3041167)

On Solaris 11 SPARC SRU1, system panics after executing the `vxrecover` operation on the master node.

Workaround:

There is no workaround for this issue in 6.0.3.

Veritas Storage Foundation known issues

This section describes the Veritas Storage Foundation known issues in 6.0.3 and 6.0.1.

- Veritas Storage Foundation known issues
- Veritas Volume Manager known issues
- Veritas File System known issues

- Replication known issues
- Veritas Storage Foundation for Databases (SFDB) tools known issues

Veritas Storage Foundation known issues

This section describes the known issues in this release of Veritas Storage Foundation (SF).

Some dbed DST commands do not work correctly in non-POSIX locales (2138030)

Some dbed DST commands do not work correctly in non-POSIX locale settings.

Workaround:

Set the environment variable `LANG=C` systemwide in the `/etc/profile` file.

In an IPv6 environment, db2icrt and db2idrop commands return a segmentation fault error during instance creation and instance removal (1602444)

When using IBM DB2 `db2icrt` command to create a DB2 database instance on a pure IPv6 environment, the `db2icrt` command returns segmentation fault error message. For example:

```
$ /opt/ibm/db2/V9.5/instance/db2icrt -a server -u db2fen1 db2inst1
/opt/ibm/db2/V9.5/instance/db2iutil: line 4700: 26182 Segmentation fault
$ {DB2DIR?}/instance/db2isrv -addfcm -i ${INSTNAME?}
```

The `db2idrop` command also returns segmentation fault, but the instance is removed successfully after the `db2idrop` command is issued. For example:

```
$ /opt/ibm/db2/V9.5/instance/db2idrop db2inst1
/opt/ibm/db2/V9.5/instance/db2iutil: line 3599:  7350 Segmentation fault
$ {DB2DIR?}/instance/db2isrv -remove -s DB2_${INSTNAME?} 2> /dev/null

DBI1070I  Program db2idrop completed successfully.
```

This happens on DB2 9.1, 9.5, and 9.7.

This issue has been identified as an IBM issue. Once IBM has fixed this issue, then IBM will provide a hotfix for this segmentation problem.

At this time, you can communicate in a dual-stack to avoid the segmentation fault error message until IBM provides a hotfix.

To communicate in a dual-stack environment

- Add an IPv6 hostname as an IPv4 loopback address to the `/etc/hosts` file. For example:

  ```
  127.0.0.1 swlx20-v6
  ```

  Or

  ```
  127.0.0.1 swlx20-v6.punipv6.com
  ```

  `127.0.0.1` is the IPv4 loopback address.

  `swlx20-v6` and `swlx20-v6.punipv6.com` are the IPv6 hostnames.

Boot fails after installing or removing SF packages from a Solaris 9 system to a remote Solaris 10 system (1747640)

The following issue occurs if you install or remove a Storage Foundation package or patch from a Sparc Solaris 9 system to a remote Solaris 10 system, using the `-R` *`rootpath`* option of the `pkgadd`, `patchadd`, `pkgrm` or `patchrm` commands.

Generally, when you install or remove a SF package on a Solaris 10 system, the package scripts update the boot archive. However if the local system is Solaris 9 and the remote system is Solaris 10, the scripts fail to update the boot archive on the Solaris 10 system.

Note: The boot archive is synchronized correctly when you upgrade SF using Solaris Live Upgrade.

Workaround:

The workaround is to manually clear the boot archive when you boot the alternate. The SUN boot process detects that the boot archive is out sync and displays instructions for how to correct the situation.

For example:

```
WARNING: The following files in / differ from the boot archive:

     stale //kernel/drv/sparcv9/vxportal
     stale //kernel/drv/vxportal.conf
     stale //kernel/fs/sparcv9/vxfs
     ...
     new     /kernel/drv/vxlo.SunOS_5.10
     new     /kernel/drv/vxlo.conf
     changed /kernel/drv/vxspec.SunOS_5.9
     changed /kernel/drv/vxspec.conf
```

```
The recommended action is to reboot to the failsafe archive to correct
the above inconsistency. To accomplish this, on a GRUB-based platform,
reboot and select the "Solaris failsafe" option from the boot menu.
On an OBP-based platform, reboot then type "boot -F failsafe". Then
follow the prompts to update the boot archive. Alternately, to continue
booting at your own risk, you may clear the service by running:
"svcadm clear system/boot-archive"
```

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

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

Tools like `dbca` may hang during database creation.

Workaround: There is no workaround for this, as Oracle 11gR1 does not fully support pure IPv6 environment. Oracle 11gR2 release may work on a pure IPv6 environment, but it has not been tested or released yet.

Sybase ASE version 15.0.3 causes segmentation fault on some Solaris version (1819595)

Sybase ASE 15.0.3 produces segmentation fault on Solaris SPARC 10 Update 6 in a pure IPv6 environment. However, Sybase ASE 15.0.3 works on Solaris SPARC 10 Update 5.

When running Sybase ASE 15.0.3 GA on a pure IPv6 environment on Solaris SPARC 10 Update 6, you may receive a segmentation fault message. For example:

```
Building Adaptive Server 'CDGV240AIPV6':
Writing entry into directory services...
Directory services entry complete.
Building master device...
Segmentation Fault - core dumped
Task failed
Server 'CDGV240AIPV6' was not created.
```

This is a Sybase known issue. You should use Sybase Adaptive Server Enterprise Suite version 15.0.3 ESD 1 that supports Solaris 10 Update 6 or later. For details, refer to the Sybase Product Download Center regarding ESD 1.

Not all the objects are visible in the VOM GUI (1821803)

After upgrading SF stack from 5.0MP3RP2 to 5.1, the volumes are not visible under the Volumes tab and the shared diskgroup is discovered as Private and Deported under the Disgroup tab in the SFM GUI.

Workaround:

To resolve this known issue

- On each manage host where `VRTSsfmh` 2.1 is installed, run:

  ```
  # /opt/VRTSsfmh/adm/dclisetup.sh -U
  ```

An error message is received when you perform off-host clone for RAC and the off-host node is not part of the CVM cluster (1834860)

There is a known issue when you try to perform an off-host clone for RAC and the off-host node is not part of the CVM cluster. You may receive a similar error message:

```
Cannot open file /etc/vx/vxdba/rac11g1/.DB_NAME
(No such file or directory).
SFORA vxreptadm ERROR V-81-8847 Cannot get filename from sid
for 'rac11g1', rc=-1.
SFORA vxreptadm ERROR V-81-6550 Could not connect to repository
database.
VxVM vxdg ERROR V-5-1-582 Disk group SNAP_rac11dg1: No such disk
group SFORA
vxsnapadm ERROR V-81-5623 Could not get CVM information for
SNAP_rac11dg1.
SFORA dbed_vmclonedb ERROR V-81-5578 Import SNAP_rac11dg1 failed.
```

Workaround:

Currently there is no workaound for this known issue. However, if the off-host node is part of the CVM cluster, then off-host clone for RAC works fine.

Also the `dbed_vmclonedb` command does not support LOCAL_LISTENER and REMOTE_LISTENER in the `init.ora` parameter file of the primary database.

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

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

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

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

To resolve this issue

1 In the Web GUI, go to **Settings** > **Deployment**.

2 Select **HF020008500-06 hotfix**.

3 Click **Install**.

4 Check the **force** option while reinstalling the hotfix.

A volume's placement class tags are not visible in the Veritas Enterprise Administrator GUI when creating a dynamic storage tiering placement policy (1880081)

A volume's placement class tags are not visible in the Veritas Enterprise Administrator (VEA) GUI when you are creating a SmartTier placement policy if you do not tag the volume with the placement classes prior to constructing a volume set for the volume.

Workaround:

To see the placement class tags in the VEA GUI, you must tag the volumes prior to constructing the volume set. If you already constructed the volume set before tagging the volumes, restart `vxsvc` to make the tags visible in the GUI.

NULL pointer dereference panic with Solaris 10 Update 10 on x86 and Hitachi Data Systems storage (2616044)

Due to a limitation with Solaris 10 Update 10 on x86, when the server is connected to Hitachi Data storage, the system panics due to a NULL pointer deference during the boot cycle with the following stack trace:

```
fffffe8000988570 unix:die+da ()
fffffe8000988650 unix:trap+5e6 ()
fffffe8000988660 unix:cmntrap+140 ()
fffffe8000988870 scsi_vhci:hds_sym_path_get_opinfo+62 ()
fffffe8000988920 scsi_vhci:vhci_update_pathinfo+5b ()
fffffe80009889a0 scsi_vhci:vhci_pathinfo_online+2df ()
fffffe8000988a10 scsi_vhci:vhci_pathinfo_state_change+202 ()
fffffe8000988a70 genunix:i_mdi_pi_state_change+148 ()
fffffe8000988ab0 genunix:mdi_pi_online+32 ()
fffffe8000988b20 fcp:ssfcp_online_child+ff ()
fffffe8000988b90 fcp:ssfcp_trigger_lun+2b0 ()
fffffe8000988bc0 fcp:ssfcp_hp_task+88 ()
fffffe8000988c40 genunix:taskq_thread+295 ()
fffffe8000988c50 unix:thread_start+8 ()
```

For more information, see Oracle bug ID 7079724.

Workaround:

Disable Solaris I/O multi-pathing on the server to avoid the system panic.

To disable Solaris I/O multi-pathing on the server

1. Disable Solaris I/O multi-pathing:

   ```
   # stmsboot -d
   ```

2. Reboot the server:

   ```
   # reboot
   ```

Veritas Volume Manager known issues

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

Dynamic LUN expansion is not supported for EFI disks in simple or sliced formats (2836798)

Dynamic LUN expansion is not supported for EFI (Extensible Firmware Interface) disks in simple or sliced formats. It may lead to corruption. The recommended format is the Cross-platform Data Sharing (CDS) disk format.

Workaround:

Convert the disk format to CDS using the `vxcdsconvert` utility.

The vxrecover command does not handle RAID5 volumes correctly (2715124)

The `vxrecover` command calls the recovery process for the top-level volume, which internally takes care of recovering its subvolumes. The `vxrecover` command does not handle RAID5 volumes correctly. The recovery process fails to recover the subvolumes, which remain in the NEEDSYNC state.

Workaround:

Manually recover the RAID5 volumes using the `vxvol` utility, as follows:

```
# vxvol -g diskgroup resync volume
```

The vxcdsconvert utility is supported only on the master node (2616422)

The `vxcdsconvert` utility should be run only from the master node, not from the slave nodes of the cluster.

Veritas Volume Manager (VxVM) might report false serial split brain under certain scenarios (1834513)

VxVM might detect and report a false serial split brain when all of the following conditions are met:

- One or more arrays that provide the shared storage for the cluster are being powered off
- At the same time when the arrays are being powered off, an operation that requires an internal transaction is initiated (such as VxVM configuration commands)

In such a scenario, disk group import will fail with a split brain error and the vxsplitlines output will show 0 or 1 pools.

Workaround:

To recover from this situation

1. Retrieve the disk media identifier (dm_id) from the configuration copy:

   ```
   # /etc/vx/diag.d/vxprivutil dumpconfig device-path
   ```

   The dm_id is also the serial split brain id (ssbid)

2. Use the dm_id in the following command to recover from the situation:

   ```
   # /etc/vx/diag.d/vxprivutil set device-path ssbid=dm_id
   ```

The relayout operation fails when there are too many disks in the disk group. (2015135)

The attempted relayout operation on a disk group containing approximately more than 300 LUNs or disks may fail with the following error:

```
Cannot setup space
```

Expanding a LUN to a size greater than 1 TB fails to show correct expanded size (2123677)

This issue occurs when you perform a Dynamic LUN Expansion for a LUN that is smaller than 1 TB and increase the size to greater than 1 Tb. After the expansion, Veritas Volume Manager (VxVM) fails ongoing I/O, and the public region size is reset to original size. After you run the `vxdisk scandisks` command, VxVM does not show the correct expanded size of the LUN. The issue is due to underlying Solaris issues. Refer to Sun Bug Id 6929449 and Sun Bug Id 6912703.

Workaround:

There is no workaround for this issue.

Co-existence check might fail for CDS disks (2214952)

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

GUID Partition Table (GPT) to initialize the cdsdisk layout on devices larger than 1 TB.

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

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

Workaround:

There is no workaround for this issue.

Probing vxio with DTrace fails on SPARC machines. (2180635)

This issue exists because of inability of DTrace to load a module whose text size is greater than 2MB on SPARC machines. While trying to load `vxio` with DTrace you may see following warning messages on console:

```
dtrace: WARNING: couldn't allocate SDT table for module vxio
fbt: WARNING: couldn't allocate FBT table for module vxio
```

Workaround:

There is no workaround for this issue.

The "vxdg listclone" command output may not list all the disks with "clone_disk" or "udid_mismatch" flag set (2354560)

In Cluster Volume Manager environment, "vxdg listclone" command output may not list all the disks with "clone_disk" or "udid_mismatch" flag set. This can happen on master/slave nodes.

Workaround:

Administrator has to run "vxdisk scandisks" or "vxdisk -o alldgs list" followed by "vxdg listclone" to get all the disks containing "clone_disk" or "udid_mismatch" flag on respective host.

The vxsnap print command shows incorrect value for percentage dirty (2360780)

The `vxsnap print` command can display the percentage of regions that differ between snapshots, shown as the %dirty. In SF 6.0, if this command is run while the volumes are online and being actively used, the shown %dirty may lag from actual percentage dirty for instant snap data cache object (DCO) volumes. That is, the command output may show less %dirty than actual.

Issues with the disk state on the CVM slave node when vxconfigd is restarted on all nodes (2615680)

When a CVM master node and a slave node have lost storage access, and `vxconfigd` is restarted on all nodes, the disk state on the CVM slave node shows as invalid.

Workaround:

To work around this issue

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

Removing an array node from an IBM Storwize V7000 storage system also removes the controller (2816589)

When using an IBM Storwize V7000 storage system, after removing one array node, the corresponding controller is also removed.

Workaround: The following procedure resolves this issue.

To resolve this issue

1. Set the `iotimeout` tunable to 600:

   ```
   # vxdmpadm setattr enclosure encl1 recoveryoption=throttle \
    iotimeout=600
   ```

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

   ```
   # vxdctl enable
   ```

vxmirror to SAN destination failing when 5 partition layout is present: for example, root, swap, home, var, usr (2815311)

The `vxmirror` command may fail with following error on a Solaris 10 host, for a thin LUN, if more than one partition excluding root and swap is present.

```
VxVM vxbootsetup WARNING V-5-2-5667 Max volume count 5 exceeded.
```

Example:

```
# /etc/vx/bin/vxmirror" -f -g rootdg_17_23_49 rootdisk01 \
rootdisk02
! vxassist -g rootdg_17_23_49 mirror swapvol rootdisk02
! vxassist -g rootdg_17_23_49 mirror rootvol rootdisk02
! vxassist -g rootdg_17_23_49 mirror usr rootdisk02
! vxassist -g rootdg_17_23_49 mirror var rootdisk02
! vxassist -g rootdg_17_23_49 mirror home rootdisk02
! vxbootsetup -g rootdg_17_23_49
VxVM vxbootsetup WARNING V-5-2-5667 Max volume count 5 exceeded.
VxVM vxbootsetup ERROR V-5-2-5678 Skipping volume 'home_dcl'
because no free partitions are available on disk 'disk_0'.
Either remove the volume or make a partition available
VxVM vxbootsetup WARNING V-5-2-5667 Max volume count 5 exceeded.
VxVM vxbootsetup ERROR V-5-2-5678 Skipping volume 'usr_dcl'
because no free partitions are available on disk 'disk_0'.
Either remove the volume or make a partition available
VxVM vxbootsetup WARNING V-5-2-5667 Max volume count 5 exceeded.
VxVM vxbootsetup ERROR V-5-2-5678 Skipping volume 'var_dcl' because
no free partitions are available on disk 'disk_0'.
Either remove the volume or make a partition available
/usr/lib/vxvm/bin/vxmksdpart: 3pardata0_2492: is not an identifier
```

Diskgroup import of BCV luns using -o updateid and -o useclonedev options is not supported if the diskgroup has mirrored volumes with DCO or has snapshots. (2831658)

VxVM uses guid stored in configuration to uniquely identify all objects. The DCO volume stores the guid of mirrors and snapshots. If the diskgroup is imported with -o updateid and -o useclonedev, it changes the guid of objects in VxVM configuration database and the guids stored in DCO volume are not updated. So the operations involving DCO will not be able to find objects with the stored guid and this could lead to failure of certain operations involving DCO or could lead to unexpected behaviour.

Workaround:

No workaround available.

Disks on the LDOM guest are claimed under other_disks category (2354005)

The disks on the LDOM guest are claimed under "other_disks" enclosure, because these disks are not capable of being multi-pathed by DMP. This is expected because these devices represent VxVM volumes in the host. By design, devices under other_disks enclosure have their name based on underlying OS path regardless of the DDL naming scheme.

Hardware paths for operating system paths have changed in DMP 6.0 (2410716)

In DMP 6.0, the hardware paths for operating system paths have changed. After upgrading to DMP 6.0, path attributes are reset to the default values. You must reconfigure any path-level attributes that were defined in the /etc/vx/dmppolicy.info file.

Workaround:

To configure path-level attributes

1. Remove the path entries from the `/etc/vx/dmppolicy.info` file.
2. Reset the path attributes.

Upgrading from Veritas Storage Foundation 5.x to 6.0.1 may fail for IBM XIV Series arrays (2715119)

Starting in the Veritas Storage Foundation 5.1 SP1 release, the Array Support Library (ASL) for the IBM XIV enclosures converts the LUN Serial Number from Hexadecimal to Decimal. Because of this change, the enclosure names differ from releases prior to the 5.1 SP1 releases. When you upgrade Veritas Storage Foundation from a release prior to that release to the current 6.0.1 release, XIV LUNs may go into an error state. Note that the latest RPs on 5.1/5.1SP1 are already modified to use the same logic for enclosure naming.

Workaround:

After the upgrade, run `vxddladm assign names`.

Cannot grow Veritas Volume Manager (VxVM) disk using the vxdisk resize command during Dynamic LUN Expansion operation (2064510)

The following error message is displayed during the Dynamic LUN Expansion operation of a LUN with the SIMPLE format:

```
VxVM vxdisk ERROR V-5-1-8643 Device <device name>: resize failed:
Invalid data in request
```

The `vxdisk resize` command keeps the cylinder size (number of the heads * total number of the sectors per track) constant before and after the resize operation, unless the number of cylinders go beyond 2^16-1 (65535) . Because of the VTOC limitation of storing geometry values only till 2^16 -1, if the number of cylinders increases beyond the limit, `vxdisk resize` increases the cylinder size. If this happens, the private region will overlap with the public region data and corrupt the user data.

As a result of this LUN geometry change, VxVM is unable to complete `vxdisk resize` on simple format disks. VxVM was not designed to handle such geometry changes during Dynamic LUN Expansion operations on simple disks.

Workaround:

The VxVM `vxdisk resize` command behaves differently depending on whether the disk is simple, sliced, or CDS format.

The problem shown above only occurs on simple disk configurations. As a result of this difference in behavior, if the geometry changes during a Dynamic LUN Expansion operation at the LUN level, you can convert the disk to a CDS format disk. Use the `vxcdsconvert` command on the disk. Then you can issue the `vxdisk resize` command.

See http://www.symantec.com/docs/TECH136240 for more information.

Expanding a LUN to a size greater than 1 TB fails to show correct expanded size (2123677)

This issue occurs when you perform a Dynamic LUN Expansion for a LUN that is smaller than 1 TB and increase the size to greater than 1 Tb. After the expansion, Veritas Volume Manager (VxVM) fails ongoing I/O, and the public region size is reset to original size. After you run the `vxdisk scandisks` command, VxVM does not show the correct expanded size of the LUN. The issue is due to underlying Solaris issues. Refer to Sun Bug Id 6929449 and Sun Bug Id 6912703.

Workaround:

There is no workaround.

1 TB luns goes in error state with Solaris x86 (2706776)

If you label a disk device as EFI using format on a subset of the paths or on the DMP device, Solaris will not be able to propagate the label to all the other paths of the LUN. This will lead the device to appear in the error state under 'vxdisk list'.

Workaround:

There is no workaround for this issue.

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

In an enviroment which includes devices that are managed by EMC PowerPath, a storage loss causes Veritas Volume Manager commands to be delayed. In the event of storage loss, VxVM sends SCSI inquiry from each LUN path to check the health of path, which are delayed by the presence of EMC PowerPath.

Complete site is detached, if plex detach operation is performed even after site consistency off (2845383)

By design, you cannot detach the last plex of a site on a site consistent volume without detaching the complete site. By default, attempting to detach the last plex causes an error. If you use the force detach option, then the complete site is detached to ensure site consistency. This behavior is seen even if you turn off the site consistent flag if the allsites flag is on.

Performance impact when a large number of disks are reconnected (2802698)

If the storage connectivity is lost to part of the storage, the disk group configuration copy is rebalanced to the disks that have connectivity. For example, if the storage for an entire enclosure is removed from a disk group with muliple enclosures. The rebalancing process takes time, during which time the `vxconfigd` daemon is busy and does not respond to commands.

Plex synchronization is not completed after resuming synchronization on a new master when the original master lost connectivity (2788077)

When you run `vxrecover -o force`, it recovers only one subvolume and it cannot detect that the rest of the volume needs recovery.

When you run the `vxassist mirror` command, you run the `vxplex att`command serially on each subvolume. If the failure happens before you start the `attach`operation (need to mark the concerned plex as the attach operation is in progress), `vxrecover` will not redo the attach operation because it cannot find any record of the attach operation in progress.

Workaround:

Run the following command on each subvolume to manually recover the complete volume:

```
# /usr/lib/vxvm/type/fsgen/vxplex -U fsgen -g diskgroup \
 -o force useopt att volume plex
```

CVMVolDg agent may fail to deport CVM disk group

The CVM disk group is deported based on the order in which the CVMVolDg resources are taken offline. If the CVMVolDg resources in the disk group contain a mixed setting of 1 and 0 for the `CVMDeportOnOffline` attribute, the disk group is deported only if the attribute value is 1 for the last CVMVolDg resource taken offline. If the attribute value is 0 for the last CVMVolDg resource taken offline, the disk group is not deported.

Workaround: If multiple CVMVolDg resources are configured for a shared disk group, set the value of the `CVMDeportOnOffline` attribute to 1 for all of the resources.

vxlustart failed due to lumount error when liveupgrade to Solaris 10 U11 (3035982)

Live Upgrade (LU) to Solaris 10 U11 using `vxlustart` fails with following error:

```
# lumount -n dest.7667 /altroot.5.10
ERROR: mount point directory </altroot.5.10> is not empty
ERROR: failed to create mount point </altroot.5.10> for file system
</dev/dsk/c1t1d0s0>
ERROR: cannot mount boot environment by name <dest.7667>
ERROR: vxlustart: Failed: lumount -n dest.7667 /altroot.5.10
```

Workaround:

Use the Solaris 10 U10 LU packages (SUNWlucfg, SUNWlur, SUNWluu) instead of the Solaris 10 U11 LU packages. Then use `vxlustart` to upgrade to Solaris 10 U11.

The `vradmin repstatus` shows incorrect status of DCM during the initial synchronization of setting up replication (3060327)

During the initial synchronization of setting up replication, the `vradmin repstatus` shows incorrect status of DCM. The output looks like:

```
root@hostname#vradmin -g dg1 repstatus rvg
Replicated Data Set: rvg
Primary:
  Host name:                  <primary ip>
  RVG name:                   rvg
  DG name:                    dg1
  RVG state:                  enabled for I/O
  Data volumes:               1
  VSets:                      0
  SRL name:                   srl
  SRL size:                   1.00 G
  Total secondaries:          1
Secondary:
  Host name:                  <primary ip>
  RVG name:                   rvg
  DG name:                    dg1
  Data status:                inconsistent
  Replication status:         resync in progress (smartsync autosync)
  Current mode:               asynchronous
  Logging to:                 DCM (contains  0  Kbytes) (autosync)
  Timestamp Information:      N/A
```

The issue is specific to configurations in which primary data volumes have VxFS mounted.

Workaround:

Use the `vxrlink status` command to view the number of remaining bytes.

Veritas File System known issues

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

Taking a FileSnap over NFS multiple times with the same target name can result in the 'File exists' error (2353352)

The "File exists" error occurs as a result of the caching behavior of the NFS client. Because the link operation is successful, the NFS client assumes that a file with the specified target name, such as `file2::snap:vxfs:`, was created.. As a result, the NFS client caches a file with this name.

Workaround: Remove the target file after a snapshot is created. This forces the NFS client to remove the name from the cache. For example:

```
# ln file1 file2::snap:vxfs:
# rm file2::snap:vxfs:
```

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

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

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

Workaround:

Use the `vxtunefs` command to turn off delayed allocation for the file system.

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

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

Workaround:

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

Deduplication can fail with error 110 (2591473)

In some cases, data deduplication fails with a message similar to the following example:

```
Saving    Status    Node            Type        Filesystem
---------------------------------------------------------------------
00%       FAILED    node01          MANUAL      /data/fs1
        2011/10/26 01:38:58 End full scan with error
```

In addition, the deduplication log contains an error similar to the following example:

```
2011/10/26 01:35:09 DEDUP_ERROR AddBlock failed. Error = 110
```

These errors indicate that the deduplication process is running low on space and needs more free space to complete.

Workaround:

Make more space available on the file system.

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

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

```
UX:vxfs fsadm: ERROR: V-3-20343: cannot shrink /dev/vx/rdsk/dg1/vol1 -
blocks are currently in use.
VxVM vxresize ERROR V-5-1-7514 Problem running fsadm command for volume
vol1, in diskgroup dg1
```

Workaround:

Rerun the shrink operation after stopping the I/Os.

System hang when using ls, du and find (2584531)

The system sometimes hangs when using the `ls`, `du`, or `find` commands. The hang occurs in the following stack:

```
schedule_timeout
vx_iget
vx_dirlook
vx_lookup
do_lookup
do_path_lookup
```

Workaround:

There is no workaround for this issue.

Warning message sometimes appear in the console during system startup (2354829)

During system startup, following messages sometimes appear in system console:

```
WARNING: couldn't allocate SDT table for module vxfs
WARNING: couldn't allocate FBT table for module vxfs
Loading smf(5) service descriptions: 2/2
```

These warnings indicate that the SDT and FBT DTrace probes might not be available for the VxFS module. The VxFS module still loads and works correctly. Dtrace SDT/FBT has limits on the size of module that it can support. Since the VxFS module exceeds the size that Dtrace can support, SDT and FBT Dtrace probes might not work for VxFS.

Workaround:

There is no workaround for this issue.

Possible assertion failure in vx_freeze_block_threads_all() (2244932)

There is a possible assertion failure in the `vx_freeze_block_threads_all`() call when the `pdir_threshold` tunable is set to 1.

Workaround:

There is no workaround for this issue.

Severe impact in read performance (sequential and random) on compressed files compared to uncompressed files (2609152)

The read throughput is highly degraded for compressed files. The difference is seen for sequential I/O and random I/O. For sequential reads, the degrdataion is visbile even when the amount of data read compressed files is one-third of the uncompressed files (compression ratio).

Workaround:

There is no workaround for this issue.

fsppadm operations issued on multi-volume file system fail if there are other mounted file systems with a disk layout Version less than 6 (2909206)

The `fsppadm` command checks all mounted file systems, and if it finds any file systems with a disk layout Version that is less than 6, then it exits with the following error message:

```
# fsppadm assign /dst_vset /tmp/pol_test.xml
```

```
UX:vxfs fsppadm: ERROR: V-3-26510: Low level Volume enumeration failure
on / with message  Function not implemented
```

This error occurs because the `fsppadm` command functionality is not supported on a disk layout Version that is less than 6.

Workaround:

There is no workaround for this issue.

Internal tests hit assert "f:vx_putpage1:1a" on Solaris11 U1 SRU2.5 (3060829)

The assert failure will not cause any outage but may lead to performance issues on systems with large memory and swap file configurations. This is due to a known defect on Solaris 11 update 1, refer to the Bug ID below for more details on the Oracle support site:

Bug ID: 15813035

SUNBT7194962 pageout no longer pushes pages asynchronously.

Workaround:

There is no workaround for this issue.

Replication known issues

This section describes the replication known issues in this release of Veritas Storage Foundation.

vradmin syncvol command compatibility with IPv6 addresses (2075307)

The `vradmin syncvol` command does not work with the compressed form of IPv6 addresses if the target disk group and volume names are not specified.

Workaround:

In IPv6 environments, if you run the `vradmin syncvol` command and identify the target host using the compressed form of the IPv6 address, then you also need to specify the target disk group and volume names.

RVGPrimary agent operation to start replication between the original Primary and the bunker fails during failback (2054804)

The RVGPrimary agent initiated operation to start replication between the original Primary and the bunker fails during failback – when migrating back to the original Primary after disaster recovery – with the error message:

```
VxVM VVR vxrlink ERROR V-5-1-5282 Error getting information from
remote host. Internal Error.
```

The issue applies to global clustering with a bunker configuration, where the bunker replication is configured using storage protocol. It occurs when the Primary comes back even before the bunker disk group is imported on the bunker host to initialize the bunker replay by the RVGPrimary agent in the Secondary cluster.

Workaround:

To resolve this issue

1. Before failback, make sure that bunker replay is either completed or aborted.
2. After failback, deport and import the bunker disk group on the original Primary.
3. Try the start replication operation from outside of VCS control.

Bunker replay did not occur when the Application Service Group was configured on some of the systems in the Primary cluster, and ClusterFailoverPolicy is set to "AUTO" (2047724)

The time that it takes for a global cluster to fail over an application service group can sometimes be smaller than the time that it takes for VVR to detect the configuration change associated with the primary fault. This can occur in a bunkered, globally clustered configuration when the value of the `ClusterFailoverPolicy` attribute is `Auto` and the `AppGroup` is configured on a subset of nodes of the primary cluster.

This causes the RVGPrimary online at the failover site to fail. The following messages appear in the VCS engine log:

```
RVGPrimary:RVGPrimary:online:Diskgroup bunkerdgname could not be
imported on bunker host hostname. Operation failed with error 256
and message VxVM VVR vradmin ERROR V-5-52-901 NETWORK ERROR: Remote
server unreachable... Timestamp VCS ERROR V-16-2-13066 (hostname)
```

```
Agent is calling clean for resource(RVGPrimary) because the resource
is not up even after online completed.
```

Workaround:

To resolve this issue

- ◆ When the configuration includes a bunker node, set the value of the `OnlineRetryLimit` attribute of the RVGPrimary resource to a non-zero value.

The RVGPrimary agent may fail to bring the application service group online on the new Primary site because of a previous primary-elect operation not being run or not completing successfully (2043831)

In a primary-elect configuration, the RVGPrimary agent may fail to bring the application service groups online on the new Primary site, due to the existence of previously-created instant snapshots. This may happen if you do not run the `ElectPrimary` command to elect the new Primary or if the previous `ElectPrimary` command did not complete successfully.

Workaround:

Destroy the instant snapshots manually using the `vxrvg -g` *`dg`* `-P` *`snap_prefix`* `snapdestroy` *`rvg`* command. Clear the application service group and bring it back online manually.

A snapshot volume created on the Secondary, containing a VxFS file system may not mount in read-write mode and performing a read-write mount of the VxFS file systems on the new Primary after a global clustering site failover may fail (1558257)

Issue 1:

When the `vradmin ibc` command is used to take a snapshot of a replicated data volume containing a VxFS file system on the Secondary, mounting the snapshot volume in read-write mode may fail with the following error:

```
UX:vxfs mount: ERROR: V-3-21268: /dev/vx/dsk/dg/snapshot_volume
is corrupted. needs checking
```

This happens because the file system may not be quiesced before running the `vradmin ibc` command and therefore, the snapshot volume containing the file system may not be fully consistent.

Issue 2:

After a global clustering site failover, mounting a replicated data volume containing a VxFS file system on the new Primary site in read-write mode may fail with the following error:

```
UX:vxfs mount: ERROR: V-3-21268: /dev/vx/dsk/dg/data_volume
is corrupted. needs checking
```

This usually happens because the file system was not quiesced on the original Primary site prior to the global clustering site failover and therefore, the file systems on the new Primary site may not be fully consistent.

Workaround:

The following workarounds resolve these issues.

For issue 1, run the `fsck` command on the snapshot volume on the Secondary, to restore the consistency of the file system residing on the snapshot.

For example:

```
# fsck -F vxfs /dev/vx/dsk/dg/snapshot_volume
```

For issue 2, run the `fsck` command on the replicated data volumes on the new Primary site, to restore the consistency of the file system residing on the data volume.

For example:

```
# fsck -F vxfs /dev/vx/dsk/dg/data_volume
```

In an IPv6-only environment RVG, data volumes or SRL names cannot contain a colon (1672410, 1672417, 1825031)

Issue: After upgrading VVR to an IPv6-only environment in 6.0 release, vradmin commands may not work when a colon is specified in the RVG, data volume(s) and/or SRL name. It is also possible that after upgrading VVR to an IPv6-only environment, vradmin createpri may dump core when provided with RVG, volume and/or SRL names containing a colon in it.

Workaround:

Make sure that colons are not specified in the volume, SRL and RVG names in the VVR configuration

vradmin commands might fail on non-logowner node after logowner change (1810827)

When VVR is used for replicating shared disk groups in a Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) or Veritas Storage Foundation for Oracle RAC (SFRAC) environment consisting of three or more nodes, a logowner change event might, in rare instances, render `vradmin` commands unusable on some or all of the cluster nodes. In such instances, the following message appears in the "Config Errors:" section of the output of the `vradmin repstatus` and `vradmin printrvg` commands:

```
vradmind not reachable on cluster peer
```

In addition, all other `vradmin` commands (except `vradmin printvol`) fail with the error:

```
"VxVM VVR vradmin ERROR V-5-52-488 RDS has configuration error related
to the master and logowner."
```

This is due to a defect in the internal communication sub-system, which will be resolved in a later release.

Workaround:

Restart `vradmind` on all the cluster nodes using the following commands:

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

While vradmin commands are running, vradmind may temporarily lose heart beats (2071568, 2275444)

This issue may occasionally occur when you use `vradmin` commands to administer VVR. While the `vradmin` commands run, `vradmind` may temporarily lose heartbeats, and the commands terminate with the following error message:

```
VxVM VVR vradmin ERROR V-5-52-803 Lost connection to host host;
terminating command execution.
```

Workaround:

To resolve this issue

1. Depending on the application I/O workload and network environment, uncomment and increase the value of the `IPM_HEARTBEAT_TIMEOUT` variable in the `/etc/vx/vras/vras_env` on all the hosts of the RDS to a higher value. The following example increases the timeout value to 120 seconds.

   ```
   export IPM_HEARTBEAT_TIMEOUT
   IPM_HEARTBEAT_TIMEOUT=120
   ```

2. Restart `vradmind` on all the hosts of the RDS to put the new `IPM_HEARTBEAT_TIMEOUT` value into affect. Enter the following on all the hosts of the RDS:

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

vxassist relayout removes the DCM (145413)

If you perform a relayout that adds a column to a striped volume that has a DCM, the DCM is removed. There is no message indicating that this has happened. To replace the DCM, enter the following:

```
#vxassist -g diskgroup addlog vol logtype=dcm
```

Cannot relayout data volumes in an RVG from concat to striped-mirror (2129601)

This issue occurs when you try a relayout operation on a data volume which is associated to an RVG, and the target layout is a striped-mirror.

Workaround:

To relayout a data volume in an RVG from concat to striped-mirror

1. Pause or stop the applications.
2. Wait for the RLINKs to be up to date. Enter the following:

   ```
   # vxrlink -g diskgroup status rlink
   ```

3. Stop the affected RVG. Enter the following:

   ```
   # vxrvg -g diskgroup stop rvg
   ```

4. Disassociate the volumes from the RVG. Enter the following:

   ```
   # vxvol -g diskgroup dis vol
   ```

5. Relayout the volumes to striped-mirror. Enter the following:

   ```
   # vxassist -g diskgroup relayout vol layout=stripe-mirror
   ```

6. Associate the data volumes to the RVG. Enter the following:

   ```
   # vxvol -g diskgroup assoc rvg vol
   ```

7. Start the RVG. Enter the following:

   ```
   # vxrvg -g diskgroup start rvg
   ```

8. Resume or start the applications.

Creating a primary diskgroup fails if there is no extra LUN to mirror the data change map (2478684)

Creating a primary diskgroup fails if there is no extra LUN to mirror the data change map (DCM), even if you have enough disk space.

Workaround:

Add a LUN to the diskgroup before creating the primary diskgroup.

vradmin verifydata operation fails when replicating between versions 5.1 and 6.0 (2360713)

When replicating in a cross-version VVR environment consisting of hosts running Storage Foundation 5.1 and hosts running Storage Foundation 6.0, the `vradmin verifydata` command fails with the following error:

```
VxVM VVR vxrsync ERROR V-5-52-2222 [from host]: VxVM in.vxrsyncd
ERROR V-5-36-2125 Server volume access error during [assign volids]
volume path: [/dev/vx/dsk/dg/snapshot_volume] reason: [this could be
because a target volume is disabled or an rlink associated with a
target volume is not detached during sync operation].
```

Workaround:

There are two workarounds for this issue.

- Upgrade the hosts running Storage Foundation 5.1 to Storage Foundation 5.1SP1 or later and re-run the `vradmin verifydata` command.
- Follow the offline verification procedure in the "Verifying the data on the Secondary" section of the *Veritas Storage Foundation and High Availability Solutions Replication Administrator's Guide*. This process requires ensuring that the secondary is up-to-date, pausing replication, and running the `vradmin syncrvg` command with the `-verify` option.

Replication hang when VVR logowner is on CVM slave node (2405943)

When VVR is used for asynchronous replication in shared disk group environment, one of the nodes of the cluster at the primary site is chosen as the logowner. When the logowner node is on a node which is a slave node for the underlying CVM cluster, in the presence of heavy I/O from a node that is not the logowner, it is possible to get into a replication hang. This is due to an internal defect which will be fixed in later releases.

Workaround:

Enable the PreOnline trigger of the RVGLogOwner agent so that the VVR logowner will always reside on the CVM master node. For the detailed procedure, refer to the RVGLogowner agent notes section in the *Veritas Cluster Server Bundled Agents Reference Guide*.

vradmin verifydata may report differences in a cross-endian environment (2834424)

When replicating between two nodes in a cross-platform environment, and performing an autosync or replication, the vradmin verifydata command may report differences. This is due to different endianness between the platforms. However, the file system on the secondary node will be consistent and up to date.

vradmin verifydata operation fails if the RVG contains a volume set (2808902)

In a VVR environment, the `vradmin verifydata` command fails with the following error if the replicated volume group (RVG) contains any volume set:

```
Message from Primary:
VxVM VVR vxrsync ERROR V-5-52-2009 Could not open device
/dev/vx/dsk/vvrdg/<volname> due to: stat of raw character volume path
failed
```

vradmin repstatus operation may display configuration error after cluster reconfiguration in a CVR environment (2779580)

In a CVR environment, if there is a cluster reconfiguration, the `vradmin repstatus` command may display the following error message:

```
No Primary RVG
```

The `vradmin repstatus` command functions normally on the Primary site.

Workaround:

Restart the `vradmind` daemon on both the Primary and Secondary nodes.

I/O hangs on the primary node when running vxrvg snaprestore operation (2762147)

In a CVR environment, if a secondary node is set as the logowner for an RVG, issuing the `vxrvg snaprestore` command on the primary node may result in an I/O hang.

The vxrecover command does not automatically recover layered volumes in an RVG (2866299)

The `vxrecover` command calls the recovery process for the top-level volume, which internally takes care of recovering its subvolumes. The `vxrecover` command does not handle layered volumes correctly. The recovery process fails to recover the subvolumes, which remain in the NEEDSYNC state.

Workaround:

Manually recover the layered volumes using the `vxvol` utility, as follows:

```
# vxvol -g diskgroup resync volume
```

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

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

Workaround:

To resize layered volumes that are associated to an RVG

1. Pause or stop the applications.
2. Wait for the RLINKs to be up to date. Enter the following:

   ```
   # vxrlink -g diskgroup status rlink
   ```

3. Stop the affected RVG. Enter the following:

   ```
   # vxrvg -g diskgroup stop rvg
   ```

4. Disassociate the volumes from the RVG. Enter the following:

   ```
   # vxvol -g diskgroup dis vol
   ```

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

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

6. Associate the data volumes to the RVG. Enter the following:

   ```
   # vxvol -g diskgroup assoc rvg vol
   ```

7. Start the RVG. Enter the following:

   ```
   # vxrvg -g diskgroup start rvg
   ```

8. Resume or start the applications.

Veritas Storage Foundation for Databases (SFDB) tools known issues

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

SFDB commands do not work in IPV6 environment (2619958)

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

Database Storage Checkpoint unmount may fail with device busy (2591463)

In some cases, when a database that is cloned using a Database Storage Checkpoint is shut down, an error similar to the following may occur:

```
SFAE Error:0457: Failed to unmount device
/dev/vx/dsk/datadg/datavol:Ckpt_1317707593_rw_1317708154.
Reason: VxFS returned error : umount: /tmp/clonedb/data: device is
busy
```

Workaround:

As an Oracle user, force shut down the clone database if it is up and then retry the unmount operation.

Attempt to use SmartTier commands fails (2332973)

The attempts to run SmartTier commands such as `dbdst_preset_policy` or`dbdst_file_move` fail with the following error:

```
fsppadm: ERROR: V-3-26551: VxFS failure on low level mechanism
with message - Device or resource busy
```

This error occurs if a sub-file SmartTier command such as `dbdst_obj_move` has been previously run on the file system.

There is no workaround for this issue. You cannot use file-based SmartTier and sub-file SmartTier simultaneously.

Attempt to use certain names for tiers results in error (2581390)

If you attempt to use certain names for tiers, the following error message is displayed:

```
SFORA dbdst_classify ERROR V-81-6107 Invalid Classname BALANCE
```

This error occurs because the following names are reserved and are not permitted as tier names for SmartTier:

- BALANCE
- CHECKPOINT
- METADATA

Workaround:

Use a name for SmartTier classes that is not a reserved name.

Clone operation failure might leave clone database in unexpected state (2512664)

If the clone operation fails, it may leave the clone database in an unexpected state. Retrying the clone operation might not work.

Workaround:

If retrying does not work, perform one the following actions depending on the point-in-time copy method you are using:

- For FlashSnap, resync the snapshot and try the clone operation again.
- For FileSnap and Database Storage Checkpoints, destroy the clone and create the clone again.
- For space-optimized snapshots, destroy the snapshot and create a new snapshot.

Contact Symantec support if retrying using the workaround does not succeed.

FlashSnap resync fails if there is an existing space-optimized snapshot (2479901)

If you try a FlashSnap resync operation when there is an existing space-optimized snapshot, the resync operation fails with the following error:

```
Error: VxVM vxdg ERROR V-5-1-4597 vxdg join FS_oradg oradg failed
datavol_snp : Record already exists in disk group
archvol_snp : Record already exists in disk group
```

Workaround:

Destroy the space-optimized snapshot first and then perform the FlashSnap resync operation.

Clone command fails if PFILE entries have their values spread across multiple lines (2844247)

If you have a `log_archive_dest_1` in single line in the init.ora file, then `dbed_vmclonedb` will work but `dbed_vmcloneb` will fail if you put in multiple lines for `log_archive_dest_1`.

Workaround

There is no workaround for this issue.

SFDB commands do not work with the ZHS16GBK character set (2715323)

SFDB commands do not work if the character set of the Oracle database is set to ZHS16GBK. This occurs because SFDB commands are not supported with multi-byte character sets except AL32UTF8 and ZHS16GBK is a multi-byte character set.

There is no workaround for this issue.

Data population fails after datafile corruption, rollback, and restore of offline checkpoint (2869259)

Sometimes when a datafile gets corrupted below its reservation size, the rollback may not pass and the file may not be rolled back correctly.

There is no workround at this point of time.

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

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

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

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

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

Workaround:

For the 6.0.3 release, create distinct archive and datafile mounts for the checkpoint service.

FileSnap detail listing does not display the details of a particular snap (2846382)

FileSnap does not support displaying a detailed listing of a snapshot or clone. FileSnap only supports displaying a summary of all the snapshots or clones. For example, for the CLI `vxsfadm -s filesnap -a oracle --name=snap1 -o list`, a summary listing all the snapshots is displayed, instead of a detailed listing of a particular snapshot.

Workaround:

There is no workaround for this issue.

'vxdbd' process is online after Flash archive installation (2869269)

After a Flash archive installation of the SF stack, the `vxdbd` process is up, even if the stack is not configured.

Workaround: You can ignore, or stop the `vxdbd` process using the `/opt/VRTSdbed/common/bin/vxdbdctrl stop`command.

Checkpoint clone fails in CFS environment if cloned using same checkpoint and same clone name on both nodes (2869268)

The Checkpoint clone of an oracle database fails in a CFS environment, if you create a clone with a clone name and checkpoint name same as another clone up on a different CFS node.

Workaround:

There is no workaround. Create a clone with a different clone name.

Very long off-host cloning times for large number of datafiles (2849540)

When cloning off-host in certain Oracle database configurations, particularly with several hundred datafiles, the cloning can take a very long time, upto an hour or more. This problem does not cause the cloning to fail. The problem applies to all services such as FlashSnap, Space-optimized snapshots, FileSnap, and Checkpoint.

Workaround:

There is no workaround at this point of time.

`sfua_rept_migrate` fails after phased SFRAC upgrade from 5.0MP3RP5 to 6.0.1 (2874322)

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

```
# ./sfua_rept_migrate
Mounting SFUA Sybase ASA repository.
Unmounting SFUA Sybase ASA repository.
UX:vxfs umount: ERROR: V-3-26388: file system /rep has been mount
locked
```

```
SFORA sfua_rept_migrate ERROR V-81-5550 umount /dev/vx/dsk/repdg/repvol
failed.
SFORA sfua_rept_migrate ERROR V-81-9162 Failed to umount repository.
```

Workaround:

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

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

For more information, see TECH64812.

Veritas Cluster Server known issues

This section describes the Veritas Cluster Server known issues in 6.0.3 and 6.0.1.

- Operational issues for VCS
- Issues related to the VCS engine
- Issues related to the bundled agents
- Issues related to the VCS database agents
- Issues related to the agent framework
- Issues related to VCS in Japanese locales
- Issues related to global clusters
- LLT known issues
- I/O fencing known issues
- Issues related to Intelligent Monitoring Framework (IMF)
- Issues related to the Cluster Manager (Java Console)
- Issues related to virtualization

NFS cluster I/O fails when storage is disabled [2555662]

The I/O from the NFS clusters are saved on a shared disk or a shared storage. When the shared disks or shared storage connected to the NFS clusters are disabled, the I/O from the NFS Client fails and an I/O error occurs.

Workaround: If the application exits (fails/stops), restart the application.

Operational issues for VCS

Some VCS components do not work on the systems where a firewall is configured to block TCP traffic

The following issues may occur if you install and configure VCS on systems where a firewall is installed:

- If you set up Disaster Recovery using the Global Cluster Option (GCO), the status of the remote cluster (cluster at the secondary site) shows as "initing".
- If you configure fencing to use CP server, fencing client fails to register with the CP server.
- Setting up trust relationships between servers fails.

Workaround:

- Ensure that the required ports and services are not blocked by the firewall. Refer to the *Veritas Cluster Server Installation Guide* for the list of ports and services used by VCS.
- Configure the firewall policy such that the TCP ports required by VCS are not blocked. Refer to your respective firewall or OS vendor documents for the required configuration.

Stale legacy_run services seen when VCS is upgraded to support SMF [2431741]

If you have VCS 5.0MPx installed on a Solaris 10 system, VCS uses RC scripts to manage starting services. If you upgrade VCS to any version that supports SMF for VCS, you see stale legacy_run services for these RC scripts in addition to the SMF services.

Workaround: There are two ways to remove these legacy services:

- Open svccfg console using `svccfg -s smf/legacy_run` and delete the legacy services.
  For example:

  ```
  svccfg -s smf/legacy_run
  svc:/smf/legacy_run> listpg *
  rc2_d_S70llt    framework     NONPERSISTENT
  rc2_d_S92gab    framework     NONPERSISTENT
  svc:/smf/legacy_run> delpg rc2_d_S70llt
  svc:/smf/legacy_run> delpg rc2_d_S92gab
  svc:/smf/legacy_run> exit
  ```

- Reboot the system.

The hastop -all command on VCS cluster node with AlternateIO resource and StorageSG having service groups may leave the node in LEAVING state

On a VCS cluster node with AlternateIO resource configured and StorageSG attribute contain service groups with Zpool, VxVM or CVMVolDG resources, `hastop -local` or `hastop -all` commands may leave the node in "LEAVING" state.

This issue is caused by lack of dependency between service group containing LDom resource and service groups containing storage resources exported to logical domain in alternate I/O domain scenarios. In this scenario VCS may attempt to stop the storage service groups before stopping logical domain which is using the resources.

Workaround: Stop the LDom service group before issuing `hastop -local` or `hastop -all` commands.

Missing characters in system messages [2334245]

You may see missing characters, especially in long system messages in response to certain commands.

Workaround: No workaround.

Issues related to the VCS engine

Character corruption observed when executing the uuidconfig.pl -clus -display -use_llthost command [2350517]

If password-less ssh/rsh is not set, the use of `uuidconfig.pl` command in non-English locale may print garbled characters instead of a non-English string representing the Password prompt.

Workaround: No workaround.

Trigger does not get executed when there is more than one leading or trailing slash in the triggerpath [2368061]

The path specified in TriggerPath attribute must not contain more than one leading or trailing '\' character.

Workaround: Remove the extra leading or trailing '\' characters from the path.

Service group is not auto started on the node having incorrect value of EngineRestarted [2653688]

When HAD is restarted by `hashadow` process, the value of EngineRestarted attribute is temporarily set to 1 till all service groups are probed. Once all service groups are probed, the value is reset. If HAD on another node is started at roughly the same time, then it is possible that it does not reset the value of EngineRestarted attribute. Therefore, service group is not auto started on the new node due to mismatch in the value of EngineRestarted attribute.

Workaround: Restart VCS on the node where EngineRestarted is set to 1.

Group is not brought online if top level resource is disabled [2486476]

If the top level resource which does not have any parent dependancy is disabled then the other resources do not come online and the following message is displayed:

```
VCS NOTICE V-16-1-50036 There are no enabled
 resources in the group cvm to online
```

Workaround: Online the child resources of the topmost resource which is disabled.

NFS resource goes offline unexpectedly and reports errors when restarted [2490331]

VCS does not perform resource operations, such that if an agent process is restarted multiple times by HAD, only one of the agent process is valid and the remaining processes get aborted, without exiting or being stopped externally. Even though the agent process is running, HAD does not recognize it and hence does not perform any resource operations.

Workaround: Terminate the agent process.

Parent group does not come online on a node where child group is online [2489053]

This happens if the AutostartList of parent group does not contain the node entry where the child group is online.

Workaround: Bring the parent group online by specifying the name of the system then use the `hargp -online [parent group] -any` command to bring the parent group online.

Cannot modify temp attribute when VCS is in LEAVING state [2407850]

An `ha` command to modify a temp attribute is rejected if the local node is in a LEAVING state.

Workaround: Execute the command from another node or make the configuration read-write enabled.

Oracle group fails to come online if Fire Drill group is online on secondary cluster [2653695]

If a parallel global service group faults on the local cluster and does not find a failover target in the local cluster, it tries to failover the service group to the remote cluster. However, if the firedrill for the service group is online on a remote cluster, offline local dependency is violated and the global service group is not able to failover to the remote cluster.

Workaround: Offline the Firedrill service group and online the service group on a remote cluster.

Oracle service group faults on secondary site during failover in a disaster recovery scenario [2653704]

Oracle service group fails to go online in the DR site when disaster strikes the primary site. This happens if the AutoFailover attribute on the Service Group is set to 1 and when the corresponding service group's FireDrill is online in the DR site. Firedrill Service group may remain ONLINE on the DR site.

Workaround: If the service group containing the Oracle (or any database) resource faults after attempting automatic DR failover while FireDrill is online in the DR site, manually offline the FireDrill Service Group. Subsequently, attempt the online of the Oracle Service Group in the DR site.

Service group may fail to come online after a flush and a force flush operation [2616779]

A service group may fail to come online after flush and force flush operations are executed on a service group where offline operation was not successful.

Workaround: If the offline operation is not successful then use the force flush commands instead of the normal flush operation. If a normal flush operation is already executed then to start the service group use `-any` option.

Startup trust failure messages in system logs [2721512]

If you configure a cluster with security enabled, there might be some messages logged in system message logs related to Symantec authentication. These messages can be ignored and have no effect on functionality.

Workaround: No workaround.

Elevated TargetCount prevents the online of a service group with `hagrp -online -sys` command [2871892]

When you initiate an offline of a service group and before the offline is complete, if you initiate a forced flush, the offline of the service group which was initiated earlier is treated as a fault. As start bits of the resources are already cleared, service group goes to OFFLINE|FAULTED state but TargetCount remains elevated.

Workaround: No workaround.

Auto failover does not happen in case of two successive primary and secondary cluster failures [2858187]

In case of three clusters (clus1, clus2, clus3) in a GCO with steward not configured, if clus1 loses connection with clus2, it sends the inquiry to clus3 to check the state of clus2 one of the following condition persists:

1. If it is able to confirm that clus2 is down, it will mark clus2 as FAULTED.
2. If it is not able to send the inquiry to clus3, it will assume that a network disconnect might have happened and mark clus2 as UNKNOWN

In second case, automatic failover does not take place even if the ClusterFailoverPolicy is set to Auto. You need to manually failover the global service groups.

Workaround: Configure steward at a geographically distinct location from the clusters to which the above stated condition is applicable.

The `ha` commands may fail for non-root user if cluster is secure [2847998]

The `ha` commands fail to work if you first use a non-root user without a home directory and then create a home directory for the same user.

Workaround

1. Delete `/var/VRTSat/profile/<user_name>`.
2. Delete `/home/user_name/.VRTSat`.
3. Delete `/var/VRTSat_lhc/`*`<cred_file>`* file which same non-root user owns.
4. Run `ha` command with same non-root user (this will pass).

Older ClusterAddress remains plumbed on the node while modifying ClusterAddress [2858188]

If you execute `gcoconfig` to modify ClusterAddress when ClusterService group is online, the older ClusterAddress remains plumbed on the node.

Workaround: Un-plumb the older ClusterAddress from the node manually or offline ClusterService group by executing the following command before running `gcoconfig`:

```
hagrp -offline -force ClusterService -any
```

or

```
hagrp -offline -force ClusterService -sys <sys_name>
```

VRTSvcs package may give error messages for package verification on Solaris 11 [2858192]

VRTSvcs package may give error messages for package verification on Solaris 11. This is because some of the VCS configuration files are modified as part of product configuration. This error can be ignored.

Workaround: No workaround.

GCO clusters remain in INIT state [2848006]

GCO clusters remain in INIT state after configuring GCO due to :

- Trust between two clusters is not properly set if clusters are secure.
- Firewall is not correctly configured to allow WAC port (14155).

Workaround: Make sure that above two conditions are rectified. Refer to *Veritas Cluster Server Administrator's Guide* for information on setting up Trust relationships between two clusters.

Older ClusterAddress remains plumbed on the node while modifying ClusterAddress [2847997]

If you execute `gcoconfig` to modify ClusterAddress when ClusterService group is online, the older ClusterAddress remains plumbed on the node.

Workaround: Un-plumb the older ClusterAddress from the node manually or offline ClusterService group by executing the following command before running `gcoconfig`:

```
hagrp -offline -force ClusterService
```

Verification with `ha -verify` shows no errors when ContainerInfo and ResContainerInfo are set with service groups having multiple zones [2859495]

When defining ResContainerInfo for any resource in group in main.cf, if you also define ContainerInfo the corresponding group in main.cf then ContainerInfo is used instead of ResContainerInfo when main.cf is loaded. Verification of the configuration file using `ha -verify` at this stage shows no errors.

Workaround: Make sure ContainerInfo is not defined while defining ResContainerInfo for corresponding group in main.cf .

NFS client reports error when server is brought down using `shutdown` command [2872741]

On Solaris 11, when the VCS cluster node having the NFS share service group is brought down using `shutdown` command, NFS clients may report "Stale NFS file handle" error. During shutdown, the SMF service svc:/network/shares un-shares all the shared paths before taking down the virtual IP. Thus, the NFS clients accessing this path get stale file handle error.

Workaround: Before you shutdown the VCS cluster node, disable the svc:/network/shares SMF service, so that only VCS controls the un-sharing of the shared paths during the shutdown operation.

Extremely high CPU utilization may cause HAD to fail to heartbeat to GAB [1744854]

When CPU utilization is very close to 100%, HAD may fail to heartbeat to GAB.

Missing host names in `engine_A.log` file (1919953)

The GUI does not read the `engine_A.log` file. It reads the `engine_A.ldf` file, gets the message id from it, and then queries for the message from the bmc file of the appropriate locale (Japanese or English). The bmc file does not have system names present and so they are read as missing.

The `hacf -cmdtocf` command generates a broken `main.cf` file [1919951]

The `hacf -cmdtocf` command used with the `-dest` option removes the include statements from the types files.

Workaround: Add include statements in the `main.cf` files that are generated using the `hacf -cmdtocf` command.

types.cf error after rollback 6.0.3 to 6.0.1(3067510)

On Solaris 10, if you rollback Storage Foundation and High Availability Solutions 6.0.3 to 6.0.1, the DomainFailurePolicy attribute, which is a new attribute in 6.0.3, cannot be automatically removed in the VCS configuration files `types.cf` and `main.cf`. This causes `types.cf` verification to fail and `had` not to start after the uninstallation because the DomainFailurePolicy attribute is not identified by SFHA 6.0.1.

Workaround:

1. Stop the cluster.
2. Remove all the occurrences of the DomainFailurePolicy attribute in the `types.cf` and `main.cf` files at `/etc/VRTSvcs/conf/config`.
3. Start the cluster from the node where the configuration files are modified.
4. Start VCS on all other nodes.

Issues related to the bundled agents

Solaris mount agent fails to mount Linux NFS exported directory

The Solaris mount agent mounts the mount directories. At this point, if it tries to mount a Linux NFS exported directory, the mount fails showing the following error:

```
nfs mount: mount: <MountPoint>: Not owner
```

This is due to system NFS default version mismatch between Solaris and Linux.

The workaround for this is to configure `MountOpt` attribute in mount resource and set `vers=3` for it.

Example

```
root@north $ mount -F nfs south:/test /logo/
nfs mount: mount: /logo: Not owner
root@north $
Mount nfsmount (
                MountPoint = "/logo"
                BlockDevice = "south:/test"
                FSType = nfs
                MountOpt = "vers=3"
               )
```

Process and ProcessOnOnly agent rejects attribute values with white spaces [2303513]

Process and ProcessOnOnly agent does not accept Arguments attribute values that are separated by multiple whitespaces. The Arguments attribute specifies the set of arguments for a process. If a script controls the process, the script is passed as an argument. You must separate multiple arguments by using a single whitespace. A string cannot accommodate more than one space between arguments, or allow leading or trailing whitespace characters. This attribute must not exceed 80 characters.

Workaround: You should use only single whitespace to separate the argument attribute values. Make sure you avoid multiple whitespaces between the argument attribute values or trailing whitespace characters.

The zpool commands hang and remain in memory till reboot if storage connectivity is lost [2368017]

If the FailMode attribute of `zpool` is set to continue or wait and the underlying storage is not available, the `zpool` commands hang and remain in memory until the next reboot.

This happens when storage connectivity to the disk is lost, the `zpool` commands hang and they cannot be stopped or killed. The zpool commands run by the monitor entry point remains in the memory.

Workaround: There is no recommended workaround for this issue.

Application agent cannot handle a case with user as root, envfile set and shell as csh [2490296]

Application agent does not handle a case when the user is root, envfile is set, and shell is csh. The application agent uses the `system` command to execute the `Start`/`Stop`/`Monitor`/`Clean` Programs for the root user. This executes `Start`/`Stop`/`Monitor`/`Clean` Programs in `sh` shell, due to which there is an error when root user has csh shell and EnvFile is written accordingly.

Workaround: Do not set `csh` as shell for root user. Use `sh` as shell for root instead.

IMF registration fails for Mount resource if the configured MountPoint path contains spaces [2442598]

If the configured MountPoint of a Mount resource contains spaces in its path, then the Mount agent can online the resource correctly, but the IMF registration for ONLINE monitoring fails. This is due to the fact that the AMF driver does not support spaces in the path. Leading and trailing spaces are handled by the Agent and IMF monitoring can be done for such resources.

Workaround: Symantec recommends to turn off the IMF monitoring for a resource having spaces in its path. For information on disabling the IMF monitoring for a resource, refer to Veritas Cluster Server Administrator's Guide.

Offline of zone resource may fail if `zoneadm` is invoked simultaneously [2353541]

Offline of zone EP uses `zoneadm` command to offline a zone. Therefore, if `zoneadm` is invoked simultaneously for multiple zones, the command may fail. This is due to Oracle bug 6757506 that causes a race condition between multiple instances of `zoneadm` command and displays the following message:

```
zoneadm: failed to get zone name: Invalid argument
```

Workaround: No workaround.

Password changed while using `hazonesetup` script does not apply to all zones [2332349]

If you use the same user name for multiple zones, updating password for one zone does not updated the password of other zones.

Workaround: While updating password for VCS user which is used for multiple zones, update password for all the zones.

RemoteGroup agent does not failover in case of network cable pull [2588807]

A RemoteGroup resource with ControlMode set to OnOff may not fail over to another node in the cluster in case of network cable pull. The state of the RemoteGroup resource becomes UNKNOWN if it is unable to connect to a remote cluster.

Workaround:

- Connect to the remote cluster and try taking offline the RemoteGroup resource.
- If connection to the remote cluster is not possible and you want to bring down the local service group, change the ControlMode option of the RemoteGroup resource to MonitorOnly. Then try taking offline the RemoteGroup resource. Once the resource is offline, change the ControlMode option of the resource to OnOff.

CoordPoint agent remains in faulted state [2852872]

The CoordPoint agent remains in faulted state because it detects `rfsm` to be in replaying state.

Workaround: After HAD has stopped, reconfigure fencing.

NIC resource may fault during group offline or failover on Solaris 11 [2754172]

When NIC resource is configured with exclusive IP zone, NIC resource may fault during group offline or failover. This issue is observed as zone takes long time in shutdown on Solaris 11. If NIC monitor is invoked during this window, NIC agent may treat this as fault.

Workaround: Increase ToleranceLimit for NIC resource when it is configured for exclusive IP zone.

Share resource goes offline unexpectedly causing service group failover [1939398]

Share resource goes offline unexpectedly and causes a failover when NFSRestart resource goes offline and UseSMF attribute is set to 1 (one).

When NFSRestart resource goes offline, NFS daemons are stopped. When UseSMF attribute is set to 1, the exported file systems become unavailable, hence Share resource unexpectedly goes offline.

Workaround: Set the value of ToleranceLimit of Share resource to a value more than 1.

Mount agent does not support all scenarios of loopback mounts

For a mount point under VCS control, you can create loop back mounts for the mount point. For example, mount point /mntpt is mounted on /a as loop back mount and /a is mounted on /b as loop back mount, then offline and online of the mount resource fails.

Workaround: Mount the mount point /mntpt on /b as loop back mount.

NFS client reports I/O error because of network split brain [2564517]

When network split brain occurs, the failing node may take some time to panic. Thus, the service group on the failover node may fail to come online, as some of the resources (like IP resource) are still online on the failing node or disk group on the failing node may get disabled but IP resource on the same node continues to be online.

Workaround: Configure the preonline trigger for the service group containing DiskGroup resouce on each system in the service group:

1. Copy the preonline_ipc trigger from `/opt/VRTSvcs/bin/sample_triggers/VRTSvcs` to `/opt/VRTSvcs/bin/triggers/preonline/` as T0preonline_ipc.

   ```
   # cp /opt/VRTSvcs/bin/sample_triggers/VRTSvcs/preonline_ipc
    /opt/VRTSvcs/bin/triggers/preonline/T0preonline_ipc
   ```

2. Enable PREONLINE trigger for the service group.

   ```
   # hagrp -modify <group_name> TriggersEnabled PREONLINE
    -sys <node_name>
   ```

Some agents may fail to come online after full upgrade to VCS 6.0 if they were online before the upgrade [2618482]

Resources of type NFSRestart, DNS and Project do not come online automatically after a full upgrade to VCS 6.0 if they were previously online.

Workaround:

Online the resources manually after the upgrade, if they were online previously.

Invalid Netmask value may display code errors [2583313]

If you specify invalid Netmask value for the IP resource attribute, you may see the code errors similar to the following when you try to online the resource.

```
==================================
Illegal hexadecimal digit 'x' ignored at
/opt/VRTSperl/lib/site_perl/5.12.2/Net/Netmask.pm line 78.
ifconfig: <Netmask_value>: bad address
==============================================
```

Workaround: Make sure you specify a valid Netmask value.

Zone root configured on ZFS with ForceAttach attribute enabled causes zone boot failure (2695415)

On Solaris 11 system, attaching zone with `-F` option may result in zone boot failure if zone root is configured on ZFS.

Workaround: Change the ForceAttach attribute of Zone resource from 1 to 0. With this configuration, you are recommended to keep the default value of DetachZonePath as 1.

Error message is seen for Apache resource when zone is in transient state [2703707]

If the Apache resource is probed when the zone is getting started, the following error message is logged:

```
Argument "VCS ERROR V-16-1-10600 Cannot connect to VCS engine\n"
isn't numeric in numeric ge (>=) at /opt/VRTSvcs/bin/Apache/Apache.pm
line 452.
VCS ERROR V-16-1-10600 Cannot connect to VCS engine
LogInt(halog call failed):TAG:E:20314 <Apache::ArgsValid> SecondLevel
MonitorTimeOut must be less than MonitorTimeOut.
```

Workaround: You can ignore this message. When the zone is started completely, the `halog` command does not fail and Apache agent monitor runs successfully.

Monitor falsely reports NIC resource as offline when zone is shutting down (2683680)

If a NIC resource is configured for an Exclusive IP zone, the NIC resource is monitored inside the zone when the zone is functional. If the NIC monitor program is invoked when the zone is shutting down, the monitor program may falsely report the NIC resource as offline. This may happen if some of the networking services are offline but the zone is not completely shut down. Such reports can be avoided if you override and set the ToleranceLimit value to a non-zero value.

Workaround: When a NIC resource is configured for an Exclusive IP zone, you are recommended to set the ToleranceLimit attribute to a non-zero value.

Calculate the ToleranceLimit value as follows:

Time taken by a zone to completely shut down must be less than or equal to NIC resource's MonitorInterval value + (MonitorInterval value x ToleranceLimit value).

For example, if a zone take 90 seconds to shut down and the MonitorInterval for NIC agent is set to 60 seconds (default value), set the ToleranceLimit value to 1.

Apache resource does not come online if the directory containing Apache pid file gests deleted when a node or zone restarts (2680661)

The directory in which Apache http server creates PidFile may get deleted when a node or zone restarts. Typically the PidFile is located at `/var/run/apache2/httpd.pid`. When the zone reboots, the `/var/run/apache2` directory may get removed and hence the http server startup may fail.

Workaround: Make sure that Apache http server writes the PidFile to an accessible location. You can update the PidFile location in the Apache http configuration file (For example: `/etc/apache2/httpd.conf`).

Online of LDom resource may fail due to incompatibility of LDom configuration file with host OVM version (2814991)

If you have a cluster running LDom with different OVM versions on the hosts, then the LDom configuration file generated on one host may display error messages when it is imported on the other host with a different OVM version. Thus, the online of LDom resource may also fail.

For example, if you have a cluster running LDom with OVM versions 2.2 on one and OVM 2.1 on the other node, the using XML configuration generated on the host with OVM 2.2 may display errors when the configuration is imported on the host with OVM 2.1. Thus, the online of LDom resource fails.

The following error message is displayed:

```
ldm add-domain failed with error Failed to add device
/ldom1/ldom1 as ld1_disk1@primary-vds0 because this device
is already  exported on LDom primary. Volume ld1_disk1
already exists in vds primary-vds0.
```

Workaround: If the CfgFile attribute is specified, ensure that the XML configuration generated is compatible with the OVM version installed on the nodes.

Online of IP or IPMultiNICB resource may fail if its IP address specified does not fit within the values specified in the allowed-address property (2729505)

While configuring an IP or IPMultiNICB resource to be run in a zone, if the IP address specified for the resource does not match the values specified in the

allowed-address property of the zone configuration, then the online of IP resource may fail. This behavior is seen only on Solaris 11 platform.

Workaround: Ensure that the IP address is added to **allowed-address** property of the zone configuration.

Application resource running in a container with PidFiles attribute reports offline on upgrade to VCS 6.0 or later [2850927]

Application resource configured to run in a container configured with PidFiles attribute reports state as offline after upgrade to SF 6.0 or later versions.

When you upgrade SF from lower versions to 6.0 or later, if application resources are configured to run in a container with monitoring method set to PidFiles, then upgrade may cause the state of the resources to be reported as offline. This is due to changes introduced in the Application agent where if the resource is configured to run in a container and has PidFiles configured for monitoring the resource then the value expected for this attribute is the pathname of the PID file relative to the zone root.

In releases prior to SF 6.0, the value expected for the attribute was the pathname of the PID file including the zone root.

For example, a configuration extract of an application resource configured in SF 5.0MP3 to run in a container would appear as follows:

```
Application apptest (
User = root
StartProgram = "/ApplicationTest/app_test_start"
StopProgram = "/ApplicationTest/app_test_stop"
PidFiles = {
      "/zones/testzone/root/var/tmp/apptest.pid" }
ContainerName = testzone
)
```

Whereas, the same resource if configured in SF 6.0 and later releases would be configured as follows:

```
Application apptest (
User = root
StartProgram = "/ApplicationTest/app_test_start"
StopProgram = "/ApplicationTest/app_test_stop"
PidFiles = {
      "/var/tmp/apptest.pid" }
)
```

Note: The container information is set at the service group level.

Workaround: Modify the PidFiles pathname to be relative to the zone root as shown in the latter part of the example.

```
# hares -modify apptest PidFiles /var/tmp/apptest.pid
```

Mounting a / file system of NFS server is not supported [2847999]

Mount agent do not support BlockDevice attribute with / file system of NFS server for NFS file system.

Workaround: No workaround.

SambaShare agent clean entry point fails when access to configuration file on shared storage is lost [2858183]

When the Samba server configuration file is on shared storage and access to the shared storage is lost, SambaShare agent clean entry point fails.

Workaround: No workaround.

SambaShare agent fails to offline resource in case of cable pull or on unplumbing of IP [2848020]

When IP is unplumbed or in case of cable pull scenario, agent fails to offline SambasShare resource.

Workaround: No workaround.

Entry points that run inside a zone are not cancelled cleanly [1179694]

Cancelling entry points results in the cancellation of only the `zlogin` process. The script entry points that run inside a zone are forked off using the `zlogin` command. However, the `zlogin` command forks off an `sh` command, which runs in the context of the Solaris zone. This shell process and its family do not inherit the group id of the `zlogin` process, and instead get a new group id. Thus, it is difficult for the agent framework to trace the children or grand-children of the shell process, which translates to the cancellation of only the `zlogin` process.

Workaround: Oracle must provide an API or a mechanism to kill all the children of the `zlogin` process that was started to run the entry point script in the local-zone.

The zpool command runs into a loop if all storage paths from a node are disabled

The Solaris Zpool agent runs `zpool` commands to import and export zpools. If all paths to the storage are disabled, the zpool command does not respond. Instead, the zpool export command goes into a loop and attempts to export the zpool. This continues till the storage paths are restored and zpool is cleared. As a result, the offline and clean procedures of Zpool Agent fail and the service group cannot fail over to the other node.

Workaround: You must restore the storage paths and run the zpool clear command for all the pending commands to succeed. This will cause the service group to fail over to another node.

Zone remains stuck in down state if tried to halt with file system mounted from global zone [2326105]

If zone halts without unmounting the file system, the zone goes to down state and does not halt with the `zoneadm` commands.

Workaround: Unmount the file system manually from global zone and then halt the zone. For VxFS, use following commands to unmount the file system from global zone.

To unmount when VxFSMountLock is 1

```
umount -o mntunlock=VCS <zone root path>/<Mount Point>
```

To forcefully unmount when VxFSMountLock is 1:

```
# umount -f -o mntunlock=VCS <zone root path>/<Mount Point>
```

To unmount when VxFSMountLock is 0:

```
# umount <zone root path>/<Mount Point>
```

To forcefully unmount when VxFSMountLock is 0:

```
# umount -f <zone root path>/<Mount Point>
```

To halt the zone, use following command:

```
# zoneadm -z <zone_name>  halt
```

Prevention of Concurrency Violation (PCV) is not supported for applications running in a container [2536037]

For an application running in a container, VCS uses a similar functionality as if that resource is not registered to IMF. Hence, there is no IMF control to take a resource offline. When the same resource goes online on multiple nodes, agent detects and reports to engine. Engine uses the offline monitor to take the resource offline. Hence, even though there is a time lag before the detection of the same resource coming online on multiple nodes at the same time, VCS takes the resource offline.

PCV does not function for an application running inside a local Zone on Solaris

Workaround: No workaround.

For IPv6 configuration, the MultiNICA Agent is unable to detect loss of network connectivity (2979745)

While monitoring the Network Interface Cards (NIC) configured with the MultiNICA Resource, if the NIC is not able to ping the Network Hosts, the Agent tries to ping the broadcast address to check whether the NIC is healthy. The agent uses the packet count of the NIC to check if the network is reachable. But the packet count may increase even due to the NIC replying to itself rather than the replies from the systems in the network. Thus, Veritas Cluster Server (VCS) may incorrectly report the NIC as healthy. This issue exists only for IPv6 addresses.

Workaround:

There is no workaround for this issue.

Issues related to the VCS database agents

Health check monitoring is not supported for Oracle database 11g R1 and 11g R2 [1985055]

Health check monitoring is not supported for Oracle database 11g R1 and 11g R2.

Workaround: Set MonitorOption attribute for Oracle resource to 0.

Health check monitoring does not work with VCS agent for Oracle [2101432]

The health check monitoring in Oracle agent for VCS does not work due to incompatibility of the health check APIs provided by Oracle.

Workaround: Disable health check monitoring by setting the MonitorOption attribute to 0 (zero).

Intentional Offline does not work for VCS agent for Oracle [1805719]

Due to issues with health check monitoring, Intentional Offline does not work for VCS agent for Oracle.

The ASMInstAgent does not support having pfile/spfile for the ASM Instance on the ASM diskgroups

The ASMInstAgent does not support having pfile/spfile for the ASM Instance on the ASM diskgroups.

Workaround:

Have a copy of the pfile/spfile in the default `$GRID_HOME/dbs` directory to make sure that this would be picked up during the ASM Instance startup.

VCS agent for ASM: Health check monitoring is not supported for ASMInst agent

The ASMInst agent does not support health check monitoring.

Workaround: Set the MonitorOption attribute to 0.

NOFAILOVER action specified for certain Oracle errors

The Veritas High Availability agent for Oracle provides enhanced handling of Oracle errors encountered during detailed monitoring. The agent uses the reference file `oraerror.dat`, which consists of a list of Oracle errors and the actions to be taken.

See the *Veritas Cluster Server Agent for Oracle Installation and Configuration Guide* for a description of the actions.

Currently, the reference file specifies the NOFAILOVER action when the following Oracle errors are encountered:

```
ORA-00061, ORA-02726, ORA-6108, ORA-06114
```

The NOFAILOVER action means that the agent sets the resource's state to OFFLINE and freezes the service group. You may stop the agent, edit the `oraerror.dat` file, and change the NOFAILOVER action to another action that is appropriate for your environment. The changes go into effect when you restart the agent.

ASMInstance resource monitoring offline resource configured with OHASD as application resource logs error messages in VCS logs [2846945]

When the Oracle High Availability Services Daemon (OHASD) is configured as an application resource to be monitored under VCS and if this resource is offline on the failover node then the ASMInstance resource in the offline monitor logs the following error messages in the VCS logs:

```
ASMInst:asminst:monitor:Cluster Synchronization Service
process is not running.
```

Workaround: Configure the application in a separate parallel service group and ensure that the resource is online.

Issues related to the agent framework

Issues with configuration of resource values (1718043)

If you configure a resource that has more than 425 values in its **ArgListValues**, the agent managing that resource logs a message such as:

```
VCS WARNING V-16-2-13806 Thread(1437547408) ArgListValues overflow;
```

```
Cannot append values more than upper limit of (425).
```

Normally, the number of values in **ArgListValues** for a resource must not exceed 425. However, in case of a keylist, association or vector type of attribute appears in the ArgList for a resource-type. Since these attributes can take multiple values, there is a chance for the resource values in **ArgListValues** to exceed 425.

Agent may fail to heartbeat under heavy load [2073018]

An agent may fail to heart beat with the VCS engine under heavy load.

This may happen when agent does not get enough CPU to perform its tasks and when the agent heartbeat exceeds the time set in the AgentReplyTimeout attribute. The VCS engine therefore stops the agent and restarts it. The VCS engine generates a log when it stops and restarts the agent.

Workaround: If you are aware that the system load is likely to be high, then:

- The value of AgentReplyTimeout attribute can be set to a high value
- The scheduling class and scheduling priority of agent can be increased to avoid CPU starvation for the agent, using the AgentClass and AgentPriority attributes.

Agent framework cannot handle leading and trailing spaces for the dependent attribute (2027896)

Agent framework does not allow spaces in the target resource attribute name of the dependent resource.

Workaround: Do not provide leading and trailing spaces in the target resource attribute name of the dependent resource.

The agent framework does not detect if service threads hang inside an entry point [1442255]

In rare cases, the agent framework does not detect if all service threads hang inside a C entry point. In this case it may not cancel them successfully.

Workaround: If the service threads of the agent are hung, send a kill signal to restart the agent. Use the following command: `kill -9` *`hung agent's pid`*. The `haagent -stop` command does not work in this situation.

IMF related error messages while bringing a resource online and offline [2553917]

For a resource registered with AMF, if you run `hagrp -offline` or `hagrp -online` explicitly or through a collective process to offline or online the resource respectively, the IMF displays error messages in either case.

The errors displayed is an expected behavior and it does not affect the IMF functionality in any manner.

Workaround: No workaround.

Issues related to VCS in Japanese locales

This section covers the issues that apply to SF in a Japanese locale.

The hares -action command displays output in English [1786742]

The `hares -action` command incorrectly displays output in English.

Character corruption issue

Character corruption occurs if installer is run with HIASCII option on French locale. [1539754, 1539747]

Workaround: No workaround.

Messages inside the zone are not localized

Locale is not set correctly for Solaris zone. Therefore, you may not see localized messages inside the zone.

Workaround: No workaround.

System messages having localized characters viewed using `hamsg` may not be displayed correctly

If you use `hamsg` to view system messages, the messages containing a mix of English and localized characters may not be displayed correctly. [2405416]

Workaround: No workaround. However, you can view English messages in the VCS log file.

Standalone utilities display output in English [2848012]

The following utilities display output in English:

- `-haping`
- `-hamultinicb`
- `-haipswitch`

Workaround: No workaround.

Issues related to global clusters

The engine log file receives too many log messages on the secure site in global cluster environments [1919933]

When the WAC process runs in secure mode on one site, and the other site does not use secure mode, the engine log file on the secure site gets logs every five seconds.

Workaround: The two WAC processes in global clusters must always be started in either secure or non-secure mode. The secure and non-secure WAC connections will flood the engine log file with the above messages.

Application group attempts to come online on primary site before fire drill service group goes offline on the secondary site (2107386)

The application service group comes online on the primary site while the fire drill service group attempts to go offline at the same time, causing the application group to fault.

Workaround: Ensure that the fire drill service group is completely offline on the secondary site before the application service group comes online on the primary site.

Second secondary cluster cannot take over the primary role when primary and 1st-secondary clusters panic [2858187]

If there are three clusters(clus1, clus2, and clus3) in a GCO without a steward, when clus1 loses connection to clus2, it will send the inquiry to clus3 to check the state of clus2:

- If it is able to confirm that clus2 is down, it will mark clus2 as FAULTED.
- If it is not able to send the inquiry to clus3, it will assume that a network disconnect has happened and mark clus2 as UNKNOWN. In this case, automatic failover will not take place even if the ClusterFailoverPolicy is set to Auto. If this happens, users would need to manually failover the global service groups.

Workaround:

Configure the steward at a location geographically distinct from those of the three clusters above.

LLT known issues

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

Cannot configure LLT if full device path is not used in the llttab file (2858159)

(Oracle Solaris 11) On virtual machines ensure that you use the full path of the devices corresponding to the links in llttab. For example, use /dev/net/net1 instead of /dev/net/net:1 in the llttab file, otherwise you cannot configure LLT.

LLT port stats sometimes shows recvcnt larger than recvbytes (1907228)

With each received packet, LLT increments the following variables:

- recvcnt (increment by one for every packet)
- recvbytes (increment by size of packet for every packet)

Both these variables are integers. With constant traffic, recvbytes hits and rolls over MAX_INT quickly. This can cause the value of recvbytes to be less than the value of recvcnt.

This does not impact the LLT functionality.

GAB known issues

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

Cluster panics during reconfiguration (2590413)

While a cluster is reconfiguring, GAB broadcast protocol encounters a race condition in the sequence request path. This condition occurs in an extremely narrow window which eventually causes the GAB master to panic.

Workaround: There is no workaround for this issue.

GAB SMF service sometimes fails to start after reboot (2724565)

In SFRAC environments, sometimes GAB might fail to start because of the race between GAB and LMX in calling add_drv.

Workaround: Start the GAB SMF service and all other dependent services manually using:

```
# svcadm enable gab
# svcadm enable vxfen
# svcadm enable vcs
```

GAB may fail to stop during a phased upgrade on Oracle Solaris 11 (2858157)

While performing a phased upgrade on Oracle Solaris 11 systems, GAB may fail to stop. However, CPI gives a warning and continues with stopping the stack.

Workaround: Reboot the node after the installer completes the upgrade.

Cannot run pfiles or truss files on gablogd (2292294)

When pfiles or truss is run on gablogd, a signal is issued to gablogd. gablogd is blocked since it has called an gab ioctl and is waiting for events. As a result, the pfiles command hangs.

Workaround: None.

(Oracle Solaris 11) On virtual machines, sometimes the common product installer (CPI) may report that GAB failed to start and may exit (2879262)

GAB startup script may take longer than expected to start up. The delay in start up can cause the CPI to report that GAB failed and exits.

Workaround: Manually start GAB and all dependent services.

While deinitializing GAB client, "gabdebug -R GabTestDriver" command logs refcount value 2 (2536373)

After you unregister the gtx port with `-nodeinit` option, the `gabconfig -C` command shows refcount as 1. But when forceful `deinit` option (`gabdebug -R GabTestDriver`) is run to deinitialize GAB client, then a message similar to the following is logged.

```
GAB INFO V-15-1-20239
Client GabTestDriver with refcount 2 forcibly deinited on user request
```

The `refcount` value is incremented by 1 internally. However, the refcount value is shown as 2 which conflicts with the `gabconfig -C` command output.

Workaround: There is no workaround for this issue.

Fail to stop GAB when upgrading the second sub cluster (3066737)

On Solaris 11, in the phased upgrade scenario which includes the Veritas Cluster Server components, the GAB kernel driver may fail to unload on some nodes in some cases. The script based installer will display the following message in such situation:

```
gab failed to stop on sys1
It is recommended to reboot the systems sys1 to resolve
the failures and then retry. If issues persist after reboot,
contact Symantec technical support or refer to
installation guide for further troubleshooting.
Do you want to continue? [y,n,q] (n) y
```

Workaround:

Continue to upgrade the second sub cluster, then execute`/usr/sbin/shutdown -y -i6 -g0` to restart the nodes when the whole upgrade is completed.

I/O fencing known issues

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

Delay in rebooting Solaris 10 nodes due to vxfen service timeout issues (1897449)

When you reboot the nodes using the `shutdown -i6 -g0 -y` command, the following error messages may appear:

```
svc:/system/vxfen:default:Method or service exit
timed out. Killing contract 142
svc:/system/vxfen:default:Method "/lib/svc/method/vxfen stop"
failed due to signal Kill.
```

This error occurs because the vxfen client is still active when VCS attempts to stop I/O fencing. As a result, the vxfen stop service times out and delays the system reboot.

Workaround: Perform the following steps to avoid this vxfen stop service timeout error.

To avoid the vxfen stop service timeout error

1. Stop VCS. On any node in the cluster, run the following command:

   ```
   # hastop -all
   ```

2. Reboot the systems:

   ```
   # shutdown -i6 -g0 -y
   ```

Installer is unable to split a cluster that is registered with one or more CP servers (2110148)

Splitting a cluster that uses server-based fencing is currently not supported.

You can split a cluster into two and reconfigure Veritas High Availability product on the two clusters using the installer. For example, you can split a cluster *clus1* into *clus1A* and *clus1B*.

However, if you use the installer to reconfigure the Veritas High Availability product, the installer retains the same cluster UUID of *clus1* in both *clus1A* and *clus1B*. If both *clus1A* and *clus1B* use the same CP servers for I/O fencing, then the CP server allows registration only from the cluster that attempts to register first. It rejects the registration from the cluster that attempts next. Thus, the installer reports failure during the reconfiguration of the cluster that uses server-based fencing.

Workaround: There is no workaround for this issue.

CoordPoint agent does not report the addition of new disks to a Coordinator disk group [2727672]

The LevelTwo monitoring of the CoordPoint agent does not report a fault even if the constituent of a coordinator disk group changes due to addition of new disks in the cooridnator disk group

Workaround: There is no workaround for this issue.

After upgrading coordination point server in secure mode the cpsadm command may fail with errror - Bus error (core dumped) (2846727)

After upgrading the coordination point server from SFHA 5.0 to the next version on the client system, if you do not remove the VRTSat package that were installed on the system, the cpsadm command fails. The command fails because it loads old security libraries present on the system. The cpsadm command is also run on the coordination point server to add or upgrade client clusters. The command also fails on the server because it loads old security libraries present on the system.

Workaround: Perform the following steps on all the nodes on the coordination point server:

1 Rename cpsadm to cpsadmbin

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

2 Create the /opt/VRTScps/bin/cpsadm file with the following details.

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

3 Give executable permissions to the new file.

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

Fencing may show the RFSM state as replaying for some nodes in the cluster (2555191)

Fencing based on coordination point clients in Campus cluster environment may show the RFSM state as replaying for some nodes in the cluster.

Workaround:

Restart fencing on the node that shows RFSM state as replaying.

Veritas Cluster Server may not come up after rebooting the first node in phased upgrade on Oracle Solaris 11 (2852863)

If any of the kernel level services that depend upon Veritas Cluster Server (VCS) do not come up, then VCS fails to come up. The LLT, GAB, and Vxfen modules may also fail to come up because the `add_drv` command failed to add its driver to the system. On Solaris 11, `add_drv` may fail if there is another `add_drv` command that is being run on the system at the same time.

Workaround:

Check the status of LLT, GAB and Vxfen modules. Ensure that all the three services are online in SMF. Then, retry starting VCS.

After you run the vxfenswap utility the CoordPoint agent may fault (2846389)

After you run the `vxfenswap` utility, if the value of the `FaultTolerance` attribute of the CoordPoint agent is more than the majority (more than 50%) of the coordination points then the Coordination Point agent faults.

Workaround: Manually set the value of the `FaultTolerance` attribute of CoordPoint agent to be less than the majority (more than 50%) of the coordination points.

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

Solaris 10 SMF marks the service status based on the exit code of the start method for that service. The VxFEN start method executes the vxfen-startup script in the background and exits with code 0. Hence, if the vxfen-startup script subsequently exits with failure then this change is not propagated to SMF. This behavior causes the `svcs` command to show incorrect status for VxFEN.

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

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

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

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

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

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

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

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

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

Workaround: Start VxFEN again after some time.

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

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

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

Workaround: You can use any of the following options:

- Before running the configure_cps.pl utility, change the default shell for root user to either KSH or bash.
- Perform the following steps after running the configure_cps.pl utility on each node of the cluster:
  - Manually remove the old credential directory or softlink. For example:

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

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

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

- Start the CPSSG service group:

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

Hostname and username are case sensitive in CP server (2846392)

The hostname and username on the CP server are case sensitive. The hostname and username used by fencing to communicate with CP server must be in same case as present in CP server database, else fencing fails to start.

Workaround: Make sure that the same case is used in the hostname and username on the CP server.

Cannot run the vxfentsthdw utility directly from the install media if VRTSvxfen package is not installed on the system (2858190)

If VRTSvxfen package is not installed on the system, then certain script files that are needed for the vxfentsthdw utility to function are not available. So, without the VRTSvxfen package installed on the system you cannot run the utility from the install media.

Workaround: Install VRTSvxfen package, then run the utility from either the install media or from the `/opt/VRTSvcs/vxfen/bin/` location.

Common product installer cannot setup trust between a client system on release version 5.1SP1 and a server on release version 6.0 or later (2824472)

The issue exists because the 5.1SP1 release version does not support separate directories for truststores. But, release version 6.0 and later support separate directories for truststores. So, because of this mismatch in support for truststores, you cannot set up trust between client systems and servers.

Workaround: Set up trust manually between the coordination point server and client systems using the `cpsat` or `vcsat` command. Now, the servers and client systems can communicate in secure mode.

Server-based fencing may fail to start after reinstalling the stack (2802682)

Server-based fencing may fail to start if you use the existing configuration files after reinstalling the stack.

Workaround:

After reinstalling the stack, add the client cluster information on the coordination point server because the client cluster information is removed when the stack is uninstalled. For more details, see the Setting up server-based I/O Fencing manually section in the Veritas Storage Foundation Installation Guide. Alternatively, you can manually modify the `/etc/vxfenmode` file and the `main.cf` file to start fencing in disable mode and then configure fencing.

Issues related to Intelligent Monitoring Framework (IMF)

Registration error while creating a Firedrill setup [2564350]

While creating the Firedrill setup using the `Firedrill setup` utility, VCS encounters the following error:

```
AMF amfregister ERROR V-292-2-167
Cannot register mount offline event
```

During Firedrill operations, VCS may log error messages related to IMF registration failure in the engine log. This happens because in the firedrill service group, there is a second CFSMount resource monitoring the same MountPoint through IMF. Both the resources try to register for online/offline events on the same MountPoint and as a result, registration of one fails.

Workaround: No workaround.

IMF does not fault zones if zones are in ready or down state [2290883]

IMF does not fault zones if zones are in ready or down state.

IMF does not detect if zones are in ready or down state. In Ready state, there are no services running inside the running zones.

Workaround: Offline the zones and then restart.

IMF does not detect the zone state when the zone goes into a maintenance state [2535733]

IMF does not detect the change in state. However, the change in state is detected by Zone monitor in the next cycle.

Workaround: No workaround.

Engine log gets flooded with messages proportionate to the number of mount offline registration with AMF [2619778]

In a certain error condition, all mount offline events registered with AMF are notified simultaneously. This causes the following message to get printed in the engine log for each registered mount offline event:

```
<Date> <Time> VCS INFO V-16-2-13717
(vcsnode001) Output of the completed operation
(imf_getnotification)
==============================================
Cannot continue monitoring event
Got notification for group: cfsmount221

==============================================
```

This is an expected behavior for this error condition. Apart from the messages there will be no impact on the functionality of the VCS solution.

Workaround: No workaround.

Perl errors seen while using haimfconfig command

Perl errors seen while using `haimfconfig` command:

```
Perl errors seen while using haimfconfig command
```

This error is due to the absolute path specified in main.cf for type-specific configuration files. Currently, `haimfconfig` does not support absolute path for type-specific configuration file in `main.cf`.

Wrokaround: Replace the actual path with the actual file name and copy the file from its absolute location to `/etc/VRTSvcs/conf/config` directory.

For example, if OracleTypes.cf is included in main.cf as:

```
include "/etc/VRTSagents/ha/conf/Oracle/OracleTypes.cf"
```

It should be replaced as follows in main.cf:

```
include "OracleTypes.cf"
```

IMF does not provide notification for a registered disk group if it is imported using a different name (2730774)

If a disk group resource is registered with the AMF and the disk group is then imported using a different name, AMF does not recognize the renamed disk group and hence does not provide notification to DiskGroup agent. Therefore, the DiskGroup agent keeps reporting the disk group resource as offline.

Workaround: Make sure that while importing a disk group, the disk group name matches the the one registered with the AMF.

Direct execution of `linkamf` displays syntax error [2858163]

Bash cannot interpret Perl when executed directly.

Workaround: Run `linkamf` as follows:

```
# /opt/VRTSperl/bin/perl /opt/VRTSamf/imf/linkamf <destination-directory>
```

Error messages displayed during reboot cycles [2847950]

During some reboot cycles, the following message might get logged in the engine log:

```
AMF libvxamf ERROR V-292-2-149 Cannot unregister event: no rid -1 found
AMF libvxamf ERROR V-292-2-306 Unable to unregister all events (errno:405)
```

This does not have any effect on the functionality of IMF.

Workaround: No workaround.

Error message displayed when ProPCV prevents a process from coming ONLINE to prevent concurrency violation does not have I18N support [2848011]

The following message is seen when ProPCV prevents a process from coming ONLINE to prevent concurrency violation. The message is displayed in English and does not have I18N support.

```
Concurrency Violation detected by VCS AMF.
Process <process-details> will be prevented from startup.
```

Workaround: No Workaround.

Error message seen during system shutdown [2954309]

During some system shutdowns, you might see the following message in the syslog.

```
Stopping AMF...
AMF amfconfig ERROR V-292-2-405 AMF_UNCONFIG failed, return value = -1
```

The system continues to proceed with the shutdown.

Workaround: No workaround.

System panics when `getnotification` requests access of groups cleaned by AMF [2848009]

AMF while handling an agent that has faulted due to external or internal activity, cleans up the groups monitored by the agent. Simultaneously, if the agent notification is in progress and the `getnotification` thread requests to access an already deleted group, the system panics.

Workaround: No workaround.

The libvxamf library encounters an error condition while doing a process table scan [2848007]

Sometimes, while doing a process table scan, the libvxamf encounters an error condition. As a result, the process offline registration with AMF fails. In most cases, this registration succeeds when tried again by the agent during the next monitor cycle for this resource. This is not a catastrophic failure as the traditional monitoring continues for this resource.

Workaround: No workaround.

AMF displays StartProgram name multiple times on the console without a VCS error code or logs [2872064]

When VCS AMF prevents a process from starting, it displays a message on the console and in syslog. The message contains the signature of the process that was prevented from starting. In some cases, this signature might not match the signature visible in the PS output. For example, the name of the shell script that was prevented from executing will be printed twice.

Workaround: No workaround.

Terminating the `imfd` daemon orphans the `vxnotify` process [2728787]

If you terminate imfd daemon using the `kill -9` command, the `vxnotify` process created by imfd does not exit automatically but gets orphaned. However, if you stop `imfd` daemon with the `amfconfig -D` command, the corresponding `vxnotify` process is terminated.

Workaround: The correct way to stop any daemon is to gracefully stop it with the appropriate command (which is `amfconfig -D` command in this case), or to terminate the daemon using Session-ID. Session-ID is the -PID (negative PID) of the daemon.

For example:

```
# kill -9 27824
```

Stopping the daemon gracefully stops all the child processes spawned by the daemon. However, using `kill -9 pid` to terminate a daemon is not a recommended option to stop a daemon, and subsequently you must kill other child processes of the daemon manually.

Issues related to the Cluster Manager (Java Console)

This section covers the issues related to the Cluster Manager (Java Console).

Some Cluster Manager features fail to work in a firewall setup [1392406]

In certain environments with firewall configurations between the Cluster Manager and the VCS cluster, the Cluster Manager fails with the following error message:

```
V-16-10-13 Could not create CmdClient. Command Server
may not be running on this system.
```

Workaround: You must open port 14150 on all the cluster nodes.

Unable to log on to secure VCS clusters on Solaris 11 using Java GUI (2718943)

Connecting to secure clusters deployed on Solaris 11 systems using VCS Java GUI is not supported in VCS 6.0PR1. The system displays the following error when you attempt to use the Java GUI:

```
Incorrect username/password
```

Workaround: No workaround.

Issues related to virtualization

Locale message displayed on Solaris 11 system for solaris10 brand zones

When you run the `zlogin` command on a Solaris 11 system, the system logs the following error message:

```
Could not set locale correctly.
```

The default locale for Solaris 11 is en_US.UTF-8 and that of Solaris 10 is C. With solaris10 brand zone, en_US.UTF-8 is not installed inside the zone by default. Therefore, the error message is logged.

Workaround: This message can be safely ignored as there is no functionality issue. To avoid this message, install en_US.UTF-8 locale on solaris10 brand zone.

Veritas Storage Foundation and High Availability known issues

For known issues of Veritas Storage Foundation and High Availability in this release, see Veritas Storage Foundation known issues and Veritas Cluster Server known issues .

Veritas Storage Foundation Cluster File System High Availability known issues

This section describes the Veritas Storage Foundation Cluster File System High Availability known issues in 6.0.3 and 6.0.1.

The vxfsckd resource fails to start when vxfsckd is killed manually and the cluster node is rebooted (2720034)

If you kill the `vxfsckd` resource manually and reboot the node, `vxfsckd` does not come up and the cvm services are faulted.

Workaround:

Use the following commands for this situation:

```
hastop -local
rm /var/adm/cfs/vxfsckd-pid
```

Kill all `vxfsckd` processes:

```
fsclustadm cfsdeinit
hastart
```

NFS issues with VxFS checkpoint (2027492)

NFS clients mounting VxFS checkpoints that are NFS-exported by SFCFS or SFHA cluster nodes using a virtual IP may receive the following error message upon virtual IP failover:

```
Stale NFS file handle
```

This is a result of major numbers of VxFS checkpoints not necessarily being the same on all SFCFS or SFHA cluster nodes.

There is no workaround at this time.

The mount command may hang when there are large number of inodes with extops and a small vxfs_ninode, or a full fsck cannot fix the link count table corruptions (2689326)

You might encounter one of the following issues:

- If there are large number of inodes having extended operations (extops), then the number of inodes used by the `mount` command reaches the maximum number of inodes that can be created in core. As a result, the `mount` command will not get any new inodes, which causes the `mount` command to run slowly and sometimes hang.
  Workaround: Increase the value of vxfs_ninode.
- The link count table (LCT) file can get damaged such that the flag is set, but the attribute inode is already freed. In this case, the mount command tries to free an inode that has been already freed thereby marking the file system for a full structural file system check.
  Workaround: There is no workaround for this issue.

An ENOSPC error may return to the cluster file system application (2867282)

In some cases, when a large number of exclusion zones are set by commands such as `fsadm`, an ENOSPC error may return to the cluster file system application when delegations with free extents are not available.

Workaround: There is no workaround for this issue.

CFS commands might hang when run by non-root (3038283)

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

Workaround

To resolve this issue

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

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

Miscalculated file set usage (2123429)

When file set quotas are enabled, it may be possible for VxFS to get into a state where it thinks a very large number of blocks are allocated to Storage Checkpoints. This issue can be seen using the `fsckptadm` command:

```
# fsckptadm getquotalimit /mnt1
Filesystem    hardlimit    softlimit    usage   action_flag
/mnt1         10000        10000        18446744073709551614
```

This could cause writes to Storage Checkpoints to fail. It could also trigger the removal of removable Storage Checkpoints.

Workaround

If this occurs, disabling and re-enabling file set quotas causes VxFS to recalculate the number of blocks used by Storage Checkpoints:

```
# fsckptadm quotaoff /mnt1
# fsckptadm quotaon /mnt1
# fsckptadm getquotalimit /mnt1
Filesystem    hardlimit    softlimit    usage   action_flag
/mnt1         10000        10000        99
```

Multiple CFSmount resources are in a single service group they may not all come online after a reboot (2164670)

In some cases when multiple CFSmount resources are in a single service group, they all may not come online after a reboot. You will need to manually bring them online after a reboot.

Workaround

Create a resource dependency between the various CFSmount resources.

NFS issues with VxFS Storage Checkpoints (2027492)

NFS clients mounting VxFS Storage Checkpoints that are NFS-exported by SFHA cluster nodes using a Virtual IP may receive the following error message upon Virtual IP failover:

```
Stale NFS file handle
```

This is a result of major numbers of VxFS Storage Checkpoints not necessarily being the same on all SFHA cluster nodes.

Workaround: There is no workaround for this issue.

Panic due to null pointer de-reference in vx_bmap_lookup() (3038285)

A null pointer dereference in the `vx_bmap_lookup`() call can cause a panic.

Workaround: Resize the file system with the `fsadm` command from the primary node of the cluster.

File system check daemon fails to restart after abnormal termination (2720034)

The file system check daemon (`vxfsckd`) fails to update the `vxfsckd-pid` file with the new process ID (pid) of the vxfsckd process after abnormal termination. As a result, the CFSfsckd agent fails to detect the status of the vxfsckd daemon.

Workaround: Perform the following steps to resolve the issue on the node where the `vxfsckd` resource faults:

1. Log into the node as the root user.
2. Kill all `vxfsckd` processes:

```
# kill -9 `ps -ef|grep vxfsckd|awk '{print $2}'`
```

3. Remove the `vxfsckd-pid` file:

   ```
   # rm /var/adm/cfs/vxfsckd-pid
   ```

4. Bring the `vxfsckd` resource online:

   ```
   # hares -online vxfsckd_resname -sys node_name
   ```

Flashsnap clone fails under some unusual archivelog configuration on RAC (2846399)

In a RAC environment, when using FlashSnap, the archive log destination to snapshot must be a shared path, and must be the same across all the nodes. Additionally, all nodes must use the same archive log configuration parameter to specify the archive log destination. Configurations similar to the following are not supported:

```
tpcc1.log_archive_dest_1='location=/tpcc_arch'
tpcc2.log_archive_dest_2='location=/tpcc_arch'
tpcc3.log_archive_dest_3='location=/tpcc_arch'
```

Where tpcc1, tpcc2, and tpcc3 are the names of the RAC instances and /tpcc_arch is the shared archive log destination.

Workaround:

To use FlashSnap, modify the above configuration to *.log_archive_dest_1='location=/tpcc_arch'. For example,

```
tpcc1.log_archive_dest_1='location=/tpcc_arch'
tpcc2.log_archive_dest_1='location=/tpcc_arch'
tpcc3.log_archive_dest_1='location=/tpcc_arch'
```

Veritas Storage Foundation for Oracle RAC known issues

This section describes the Veritas Storage Foundation for Oracle RAC known issues in 6.0.3 and 6.0.1.

- Oracle RAC issues
- SF issues

Oracle RAC issues

This section lists the known issues in Oracle RAC.

Oracle Grid Infrastructure installation may fail with internal driver error

The Oracle Grid Infrastructure installation may fail with the following error:

```
[INS-20702] Unexpected Internal driver error
```

Workaround:

Perform one of the following steps depending on the type of installer you use for the installation:

- Script-based installer

  Export the `OUI_ARGS` environment variable, before you run the SF installation program:

  ```
  export OUI_ARGS=-ignoreInternalDriverError
  ```

  For more information, see the Oracle Metalink document: 970166.1

- Web-based installer

  When you run the Web-based installer, in the **Enter the arguments to be passed to the Oracle installer** text box, enter the value `-ignoreInternalDriverError`.

  For more information, see the *Veritas Storage Foundation for Oracle RAC Installation and Configuration Guide*.

During installation or system startup, Oracle Grid Infrastructure may fail to start

After successful installation of Oracle RAC 11g Release 2 Grid Infrastructure, while executing the `root.sh` script, `ohasd` may fail to start. Similarly, during system startup, Oracle Grid Infrastructure may fail to start though the VCS engine logs may indicate that the cssd resource started Oracle Grid Infrastructure successfully.

The following message may be displayed on running the `strace` command:

```
# /usr/bin/strace -ftt -p pid_of_ohasd.bin
14:05:33.527288 open("/var/tmp/.oracle/npohasd",
O_WRONLY <unfinished ...>
```

For possible causes and workarounds, see the Oracle Metalink document: 1069182.1

Enabling ODM in Oracle RAC 11 Release 2 installations causes errors (1913013)

Enabling ODM in Oracle RAC 11 Release 2 installations causes the following error:

```
'ODM ERROR V-41-4-1-253-12 Not enough space'
Oracle instance may also crash with same error.
```

The error is observed if the DISM (Dynamic Intimate Shared memory) feature is enabled. In Solaris, the Oracle database uses DISM if it is available on the system, and if the value of the `sga_max_size` initialization parameter is larger than the size required for all SGA components combined.

Workaround: Make sure that the file `ORACLE_HOME/bin/oradism` is owned by the root user with "execute" and "setuid" permissions. If the problem persists after correcting the permissions, uncomment the `sga_max_size` and `memory_target` `init.ora` parameters.

Oracle VIP Configuration Assistant fails with an error message (1182220)

During Oracle RAC 10g Release 2 installation, the VIP Configuration Assistant may fail with the following error message:

```
The given interface(s), "" is not public.
Public interfaces should be used to configure virtual IPs.
```

This message appears only when the VIP is not from the regular public IP range (for example, 200.).

Workaround: Invoke the `vipca` utility manually as the superuser.

```
# export DISPLAY=nebula:0.0
# $CRS_HOME/bin/vipca
```

Oracle Cluster Verification utility displays a warning message

During the final stage of Oracle RAC 10g Release 2 installation, you may receive a warning message with the Oracle Cluster Verification utility.

For example:

```
Utility
============================================================
OUI-25031: Some of the configuration assistants failed. It is
strongly recommended that you retry the configuration
assistants at this time. Not successfully running any "
Recommended" assistants means your system will not be correctly
configured.
1. Check the Details panel on the Configuration Assistant Screen
to see the errors resulting in the failures.
2. Fix the errors causing these failures.
3. Select the failed assistants and click the 'Retry' button
to retry them.
============================================================
```

Workaround: You may safely ignore this message if the cluster is operating satisfactorily.

Oracle Database Configuration Assistant displays an error

The Database Configuration Assistant utility displays the following error:

```
SGA size cannot be greater than maximum shared memory
segment size (0).
```

Workaround: Ignore this message and manually configure the database memory parameters for Oracle. In the "Memory" tab of the Oracle Database Creation Assistant (DBCA), select a Custom and Manual shared memory management configuration and enter the appropriate values.

SF issues

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

PrivNIC and MultiPrivNIC agents not supported with Oracle RAC 11.2.0.2 and later versions

The PrivNIC and MultiPrivNIC agents are not supported with Oracle RAC 11.2.0.2 and later versions.

For more information, see the following Technote:

http://www.symantec.com/business/support/index?page=content&id=TECH145261

Issue with format of the last 8-bit number in private IP addresses (1164506)

The PrivNIC/MultiPrivNIC resources fault if the private IP addresses have a leading 0 in any of the octets that comprise the IP address, for example X.X.X.01 or X.X.0X.1. or X.0X.X.1 or 0X.X.X.1, where X is an octet of the IP address.

When you configure private IP addresses for Oracle Clusterware, ensure that the IP addresses have a format as displayed in the following two-node example:

- On galaxy: 192.168.12.1
- On nebula: 192.168.12.2

Confirm the correct format by viewing the PrivNIC or MultiPrivNIC resource in the `/etc/VRTSvcs/conf/config/main.cf` file.

Warning message displayed on taking cssd resource offline if LANG attribute is set to "eucJP" (2123122)

When you take the cssd resource offline using the `hares -offline cssd` command and the LANG attribute is set to "eucJP", the following message may be observed in the `hamsg engine_A` command output:

```
VCS INFO V-16-2-13716 Could not find message V-16-2-13716
```

You may ignore the message.

PrivNIC resource faults in IPMP environments on Solaris 11 systems (2838745)

The PrivNIC resource faults on Solaris 11 systems when private interfaces used by IPMP are configured under PrivNIC resource.

Workaround: Avoid using PrivNIC or MultiPrivNIC agents in IPMP environments.

Error displayed on removal of VRTSjadba language package (2569224)

Removal of the VRTSjadba language package displays the following error on the screen:

```
Executing postremove script.
Generating BMC map file...
bmcmap ERROR V-33-1000-10001 Unable to create BMC map
```

You may ignore the error.

Veritas Volume Manager can not identify Oracle Automatic Storage Management (ASM) disks (2771637)

Veritas Volume Manager (VxVM) commands can not identify disks that are initialized by ASM. Administrators must use caution when using the VxVM commands to avoid accidental overwriting of the ASM disk data.

Oracle Universal Installer fails to start on Solaris 11 systems (2784560)

The Oracle Universal Installer (OUI) fails to start when the SF Oracle RAC installer invokes the OUI for the installation of Oracle Clusterware/Grid Infrastructure software.

Workaround: Install the following packages before installing Oracle Clusterware/Grid Infrastructure.

```
SUNWxwplt
SUNWmfrun
```

For instructions, see the Oracle documentation.

Veritas Storage Foundation for Sybase ASE CE known issues

This section describes the Veritas Storage Foundation for Sybase ASE CE known issues in 6.0.3 and 6.0.1.

SF issues

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

Sybase Agent Monitor times out (1592996)

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

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

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

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

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

Installer warning (151550)

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

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

The above warning may be safely ignored.

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

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

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

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

Unexpected node reboot when invalid attribute is given (2567507)

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

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

AutoFailOver = 0 attribute absent in the sample files at `/etc/VRTSagents/ha/conf/Sybase` (2615341)

Problem: AutoFailOver = 0 attribute is not present in the sample files at `/etc/VRTSagents/ha/conf/Sybase`.

Resolution: If you copy the main.cf file from the `/etc/VRTSagents/ha/conf/Sybase` location, add the AutoFailOver = 0 attribute to the binmnt and sybasece service groups.

Symantec VirtualStore known issues

This section describes the Symantec VirtualStore known issues in 6.0.3.

Symantec VirtualStore issues

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

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

```
iscsitadm: Error Requested size is too large for system
```

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

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

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

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

This makes the target unusable.

Workaround

To resolve this issue

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

2. Go to the configuration directory for the TargetID:

   ```
   # cd /etc/iscsi/TargetID .
   ```

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

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

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

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

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

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

Workaround

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

Cloning may not work (2348628)

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

Workaround

To disable the vAPP

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

2. Click **Disable**.

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

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

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

Workaround

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

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

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

For example, if you do the following:

- Right-click wingoldvm1 and invoke the wizard.
- Then soon after, right-click slesgoldvm1 and invoke the wizard.

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

Workaround

To resolve this issue:

- Close both instances of the wizard.
- Reopen a new instance of the wizard.

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

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

- FileStore nodes
- ESX host on which the clones are being created
- vCenter Server

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

Workaround

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

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

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

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

Workaround

There is no workaround for this issue.

Cloning issue in a Japanese environment (2623471)

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

Workaround

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

To resolve this issue

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

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

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

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

3 Restart the services from step 1.

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

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

The Virtual machine's local Administrator password may be set to blank (2676078, 2676079)

When clones are made of a Windows 2008 Virtual Machine and Guest OS Customization is enabled, the Virtual Machine's local Administrator password is set to blank.

Workaround: There is no workaround for this issue.

Software limitations

This section covers the software limitations in 6.0.3 and 6.0.1.

- Veritas Dynamic Multi-pathing software limitations
- Veritas Storage Foundation software limitations
- Veritas Cluster Server software limitations
- Veritas Storage Foundation and High Availability software limitations
- Veritas Storage Foundation Cluster File System High Availability software limitations
- Veritas Storage Foundation for Oracle RAC software limitations
- Veritas Storage Foundation for Sybase ASE CE software limitations
- Symantec VirtualStore software limitations

Veritas Dynamic Multi-pathing software limitations

This section describes the Veritas Dynamic Multi-pathing software limitations in 6.0.3 and 6.0.1.

DMP support for the Solaris format command (2043956)

When DMP is enabled to support Solaris ZFS pools, the Solaris `format` command displays either a path or the corresponding dmpnode. The result depends on the order in which the `format` command parses the entries in the `/dev/rdsk` directory.

DMP settings for NetApp storage attached environment

To minimize the path restoration window and maximize high availability in the NetApp storage attached environment, set the following DMP tunables:

Table 1-12

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

The change is persistent across reboots.

To change the tunable parameters

1 Issue the following commands:

```
# vxdmpadm settune dmp_restore_interval=60
```

```
# vxdmpadm settune dmp_path_age=120
```

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

```
# vxdmpadm gettune dmp_restore_interval
```

```
# vxdmpadm gettune dmp_path_age
```

ZFS pool in unusable state if last path is excluded from DMP (1976620)

When a DMP device is used by a ZFS pool, do not exclude the last path to the device. This can put the ZFS pool in an unusable state.

DMP does not support devices in the same enclosure that are configured in different modes (2643506)

DMP does not support the configuration where two devices in the same enclosure are configured in different modes. For example, if one device is configured as ALUA and another one is configured as Active/Passive (A/P).

Veritas Storage Foundation software limitations

This section describes the Veritas Storage Foundation software limitations in 6.0.3 and 6.0.1.

Veritas Volume Manager software limitations

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

Converting a multi-pathed disk

When converting a multi-pathed disk that is smaller than 1 TB from a VTOC label to an EFI label, you must issue the `format -e` command for each path. For example, if a node has two paths, `c1t2d0s2` and `c2tsd0s2`, you must run the `format -e` command on each of the two paths.

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

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

You are unable to specify units in the tunables file

The CPI displays an error when you set the unit type, such as MB or GB, for tunable parameters in the tunables file that you specify with the `-tunablesfile` *`file`* option. To avoid the error, you must set the unit type manually.

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

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

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

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

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

```
# vxdisk -o full reclaim dg1
Reclaiming storage on:
Disk xiv0_617 : Done.
Disk xiv0_616 : Done.
Disk xiv0_618 : Done.
Disk xiv0_612 : Done.
Disk xiv0_613 : Done.
Disk xiv0_614 : Done.
Disk xiv0_615 : Done
```

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

```
# vxdisk -o thin list
DEVICE    SIZE(MB) PHYS_ALLOC(MB) GROUP TYPE
xiv0_612  19313    2101           dg1   thinrclm
xiv0_613  19313    2108           dg1   thinrclm
xiv0_614  19313    35             dg1   thinrclm
xiv0_615  19313    32             dg1   thinrclm
xiv0_616  19313    31             dg1   thinrclm
xiv0_617  19313    31             dg1   thinrclm
xiv0_618  19313    31             dg1   thinrclm
```

SF does not support thin reclamation of space on a linked mirror volume (2729563)

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

DR Tool is not supported in Solaris x86 machine (2951032)

I386 is not a supported architecture of the Dynamic Reconfiguration (DR) script, the pre check for the DR Tool fails.

Veritas File System software limitations

The following are software limitations in the 6.0.3 release of Veritas Storage Foundation.

Recommended limit of number of files in a directory

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

Limitations with delayed allocation for extending writes feature

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

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

FlashBackup in NetBackup 7.1 and prior does not support disk layout Version 8 and 9

The FlashBackup feature of NetBackup 7.1 or prior does not support a VxFS file system with disk layout Version 8 or 9.

Compressed files that are backed up using NetBackup 7.1 or prior become uncompressed when you restore the files

The NetBackup 7.1 release and prior does not support the file compression feature. If you back up compressed files using NetBackup 7.1 or a prior release, the files become uncompressed when you restore the files.

Veritas Storage Foundation for Databases (SFDB) tools software limitations

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

Oracle Data Guard in an Oracle RAC environment

Database snapshots and Database Storage Checkpoints are not supported in a Data Guard with Oracle RAC environment.

Upgrading to Oracle 10.2.0.5 is required if using SFDB tools

If you are running Oracle version 10.2.0.4 and upgrading a Storage Foundation product with SFDB tools to 6.0.3, you must upgrade the Oracle binaries and database to version 10.2.0.5, before upgrading to 6.0.3.

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

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

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

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

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

Veritas Cluster Server software limitations

This section describes the Veritas Cluster Server software limitations in 6.0.3 and 6.0.1.

Limitations related to bundled agents

Volumes in a disk group start automatically irrespective of the value of the StartVolumes attribute in VCS

Volumes in a disk group are started automatically when the disk group is imported, irrespective of the value of the StartVolumes attribute in VCS. This behavior is observed if the value of the system-level attribute `autostartvolumes` in Veritas Volume Manager is set to On.

Workaround: If you do not want the volumes in a disk group to start automatically after the import of a disk group, set the autostartvolumes attribute to Off at the system level.

Programs using networked services may stop responding if the host is disconnected

Programs using networked services (for example, NIS, NFS, RPC, or a TCP socket connection to a remote host) can stop responding if the host is disconnected from the network. If such a program is used as an agent entry point, a network disconnect can cause the entry point to stop responding and possibly time out.

For example, if the host is configured to use NIS maps as a client, basic commands such as `ps -ef` can hang if there is network disconnect.

Symantec recommends creating users locally. To reflect local users, configure:

```
/etc/nsswitch.conf
```

Volume agent clean may forcibly stop volume resources

When the attribute FaultOnMonitorTimeouts calls the Volume agent clean entry point after a monitor time-out, the `vxvol -f stop` command is also issued. This command forcibly stops all volumes, even if they are still mounted.

False concurrency violation when using PidFiles to monitor application resources

The PID files created by an application contain the PIDs for the processes that are monitored by Application agent. These files may continue to exist even after a node running the application crashes. On restarting the node, the operating system may assign the PIDs listed in the PID files to other processes running on the node.

Thus, if the Application agent monitors the resource using the PidFiles attribute only, the agent may discover the processes running and report a false concurrency violation. This could result in some processes being stopped that are not under VCS control.

Online for LDom resource fails [2517350]

Online of LDom resource fails when the boot disk configured in the guest domain that is a part of the virtual disk multi-pathing group (mpgroup) and also the primary path to the virtual disk is not available.

This is due to the limitations in Oracle VM Server that do not allow retrying of other device paths that exist for the virtual disks, which are part of a virtual disk multi-pathing group, when booting a guest domain.

Workaround: None.

Zone agent registered to IMF for Directory Online event

The Directory Online event monitors the Zone root directory. If the parent directory of the Zone root directory is deleted or moved to another location, AMF does not provide notification to the Zone agent. In the next cycle of the zone monitor, it detects the change and reports the state of the resource as offline.

LDom resource calls clean entry point when primary domain is gracefully shut down

LDom agent sets failure policy of the guest domain to stop when primary domain stops. Thus when primary domain is shut down, guest domain is stopped. Moreover, when primary domain is shutdown, ldmd daemon is stopped abruptly and LDom configuration cannot be read. These operations are not under VCS control and VCS may call clean entry point.

Workaround: No workaround.

Application agent limitations

- ProPCV fails to prevent execution of script-based processes configured under MonitorProcesses.

Interface object name must match net<*x*>/v4static for VCS network reconfiguration script in Solaris 11 guest domain [2840193]

If the Solaris 11 guest domain is configured for DR and its interface object name does not match the `net<x>/v4static` pattern then the VCS guest network reconfiguration script (VRTSvcsnr) running inside the guest domain adds a new interface object and the existing entry will remain as is.

Share agent limitation (2717636)

If the Share resource is configured with VCS to share a system directory (for example, /usr) or Oracle Solaris 11 which gets mounted at boot time, the VCS share resource detects it online once VCS starts on the node after a panic or halt. This can lead to a concurrency violation if the share resource is a part of a failover service group, and the group has failed over to another node in the cluster. VCS brings down the Share resource subsequently. This is due to the share command behavior or Oracle Solaris 11, where a directory shared with share command remains persistently on the system across reboots.

Agent directory base name must be type name for an agent using out-of-the-box imf_init IMF entry point to get IMF support [2858160]

To get IMF support for an agent which uses the out-of-the-box imf_init IMF entry point, the base name of agent directory must be the type name. When AgentFile is set to one of the out-of-the-box agents like Script51Agent, that agent will not get IMF support.

Workaround:

1. Create the following symlink in agent directory (for example in `/opt/VRTSagents/ha/bin/WebSphereMQ6` directory).

   ```
   # cd /opt/VRTSagents/ha/bin/<ResourceType>
   # ln -s /opt/VRTSvcs/bin/Script51Agent <ResourceType>Agent
   ```

2. Run the following command to update the AgentFile attribute based on value of VCS_HOME.

   - If VCS_HOME is /opt/VRTSvcs:

     ```
     # hatype -modify <ResourceType> AgentFile
     /opt/VRTSvcs/bin/<ResourceType>/<ResourceType>Agent
     ```

   - If VCS_HOME is /opt/VRTSagents/ha:

```
# hatype -modify <ResourceType> AgentFile
/opt/VRTSagents/ha/bin/<ResourceType>/<ResourceType>Agent
```

Limitations related to the VCS database agents

The Db2udb agent does not support DB2 9.8

The Db2udb agent does not support DB2 version 9.8. This is because DB2 9.8 is designed especially for DB2 PureScale feature and it doesn't support some of the features in DB2 9.7 temporarily.

See
http://www.ibm.com/developerworks/data/library/techarticle/dm-0909db2whichedition/
for more information.

DB2 RestartLimit value [1234959]

When multiple DB2 resources all start at the same time with no dependencies, they tend to interfere or race with each other. This is a known DB2 issue.

The default value for the DB2 agent RestartLimit is 3. This higher value spreads out the re-start of the DB2 resources (after a resource online failure), which lowers the chances of DB2 resources all starting simultaneously.

Limitation with intentional offline functionality of VCS agent for Oracle

The Oracle resource never faults after an intentional offline.

Intentional offline functionality of VCS agent for Oracle requires you to enable health check monitoring. The agent uses Oracle's Health Check API to find the state of the database. If the API returns a graceful shutdown for the database, then the agent marks the resource state as INTENTIONAL OFFLINE. Later if the Oracle agent's online function does not succeed, the agent does not mark the resource as FAULTED. The state remains as INTENTIONAL OFFLINE because the agent receives the database state from the API as graceful shutdown during each monitor cycle. [1805719]

Sybase agent does not perform qrmutil based checks if Quorum_dev is not set (2724848)

If you do not set the Quorum_dev attribute for Sybase Cluster Edition, the Sybase agent does not perform the qrmutil-based checks. This error in configuration may lead to undesirable results. For example, if qrmutil returns failure pending, the agent does not panic the system. Thus, the Sybase agent does not perform qrmutil-based checks because the Quorum_dev attribute is not set.

Therefore, setting Quorum_Dev attribute is mandatory for Sybase cluster edition.

Engine hangs when you perform a global cluster upgrade from 5.0MP3 in mixed-stack environments [1820327]

If you try to upgrade a mixed stack VCS environment (where IPv4 and IPv6 are in use), from 5.0MP3 to 5.1SP1, HAD may hang.

Workaround: When you perform an upgrade from 5.0MP3, make sure no IPv6 addresses are plumbed on the system..

Use VCS installer to install or upgrade VCS when the zone root is on VxFS shared storage [1215671]

You must use the VCS installer program to install or upgrade VCS when the zone root is on Veritas File System (VxFS).

Systems in a cluster must have same system locale setting

VCS does not support clustering of systems with different system locales. All systems in a cluster must be set to the same locale.

Limitations with DiskGroupSnap agent [1919329]

The DiskGroupSnap agent has the following limitations:

- The DiskGroupSnap agent does not support layered volumes.
- If you use the Bronze configuration for the DiskGroupSnap resource, you could end up with inconsistent data at the secondary site in the following cases:
  - After the fire drill service group is brought online, a disaster occurs at the primary site during the fire drill.
  - After the fire drill service group is taken offline, a disaster occurs at the primary while the disks at the secondary are resynchronizing.

  Symantec recommends that you use the Gold configuration for the DiskGroupSnap resource.

Cluster Manager (Java console) limitations

This section covers the software limitations for Cluster Manager (Java Console).

Cluster Manager (Java Console) version 5.1 and lower cannot manage VCS 6.0 secure clusters

Cluster Manager (Java Console) from versions lower than VCS 5.1 cannot be used to manage VCS 6.0 secure clusters. Symantec recommends using the latest version of Cluster Manager.

See the *Veritas Cluster Server Installation Guide* for instructions on upgrading Cluster Manager.

Cluster Manager does not work if the `hosts` file contains IPv6 entries

VCS Cluster Manager fails to connect to the VCS engine if the `/etc/hosts` file contains IPv6 entries.

Workaround: Remove IPv6 entries from the `/etc/hosts` file.

VCS Simulator does not support I/O fencing

When running the Simulator, be sure the UseFence attribute is set to the default, “None”.

Limited support from Cluster Manager (Java console)

Features introduced in VCS 6.0 may not work as expected with Java console. However, CLI option of the simulator supports all the VCS 6.0 features. You are recommended to use Veritas Operations Manager (VOM) since all new features are already supported in VOM. However, Java console may continue to work as expected with features of releases prior to VCS 6.0.

Port change required to connect to secure cluster [2615068]

In order to connect to secure cluster, the default port must be changed from 2821 to 14149. You must choose **Advanced settings** in the **Login** dialog box and change **IP**: **2821** to **IP**: **14149** for secure cluster login.

Limitations related to I/O fencing

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

Preferred fencing limitation when VxFEN activates RACER node re-election

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

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

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

Stopping systems in clusters with I/O fencing configured

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

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

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

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

Limitations related to global clusters

- Cluster address for global cluster requires resolved virtual IP.
  The virtual IP address must have a DNS entry if virtual IP is used for heartbeat agents.
- Total number of clusters in a global cluster configuration can not exceed four.
- Cluster may not be declared as faulted when Symm heartbeat agent is configured even when all hosts are down.
  The Symm agent is used to monitor the link between two Symmetrix arrays. When all the hosts are down in a cluster but the Symm agent is able to see the replication link between the local and remote storage, it would report the

heartbeat as ALIVE. Due to this, DR site does not declare the primary site as faulted.

- Configuring Veritas Volume Replicator for Zone Disaster Recovery is not supported for zone root replication. Oracle Solaris 11 supports zone root only on ZFS file system.
- Configuring a cluster of mixed nodes such as a cluster between systems running on Solaris 10 and Solaris 11 versions is not supported in SF 6.0.3. The configuration is not supported through manual as well as CPI configuration.

Veritas Storage Foundation and High Availability software limitations

This section describes the Veritas Storage Foundation and High Availability software limitations in 6.0.3 and 6.0.1.

Replication software limitations

The following are replication software limitations in this release of Veritas Storage Foundation.

VVR Replication in a shared environment

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

VVR IPv6 software limitations

VVR does not support the following Internet Protocol configurations:

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

VVR support for replicating across Storage Foundation versions

VVR supports replication between Storage Foundation 6.0 and the prior major releases of Storage Foundation (5.1 and 5.1SP1). Replication between versions is supported for disk group versions 150, 160, and 170 only. Both the Primary and Secondary hosts must be using a supported disk group version.

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

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

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

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

Veritas Storage Foundation Cluster File System High Availability software limitations

This section describes the Veritas Storage Foundation Cluster File System High Availability software limitations in 6.0.3 and 6.0.1.

cfsmntadm command does not verify the mount options (2078634)

You must confirm the mount options are correct which are then passed to the `cfsmntadm` command. If the mount options are not correct, the mount fails and the CFSMount resource will not come online. You can check the VCS engine log file for any mount failure messages.

Stale SCSI-3 PR keys remain on disk after stopping the cluster and deporting the disk group

When all nodes present in the SF cluster are removed from the cluster, the SCSI-3 Persistent Reservation (PR) keys on the data disks may not get preempted. As a result, the keys may be seen on the disks after stopping the cluster or after the nodes have booted up. The residual keys do not impact data disk fencing as they will be reused or replaced when the nodes rejoin the cluster. Alternatively, the keys can be cleared manually by running the `vxfenclearpre` utility.

For more information on the `vxfenclearpre` utility, see the *Veritas Storage Foundation Administrator's Guide*.

Veritas Storage Foundation for Oracle RAC software limitations

This section describes the Veritas Storage Foundation for Oracle RAC software limitations in 6.0.3 and 6.0.1.

Oracle Clusterware/Grid Infrastructure installation fails if the cluster name exceeds 14 characters

Setting the cluster name to a value that exceeds 14 characters during the installation of Oracle Clusterware/Grid Infrastructure causes unexpected cluster membership issues. As a result, the installation may fail.

Workaround: Restart the Oracle Clusterware/Grid Infrastructure installation and set the cluster name to a value of maximum 14 characters.

Web installation program does not support phased upgrade and native operating system upgrade mechanisms

The Web installation program does not support phased upgrade and native operating system upgrade mechanisms such as Live Upgrade.

Policy-managed databases not supported by CRSResource agent

The CRSResource agent supports only admin-managed database environments in this release. Policy-managed databases are not supported.

Health checks may fail on clusters that have more than 10 nodes

If there are more than 10 nodes in a cluster, the health check may fail with the following error:

```
vxgettext ERROR V-33-1000-10038
Arguments exceed the maximum limit of 10
```

The health check script uses the `vxgettext` command, which does not support more than 10 arguments.[2142234]

Cached ODM not supported in SF environments

Cached ODM is not supported for files on Veritas local file systems and on Cluster File System.

Veritas Storage Foundation for Sybase ASE CE software limitations

This section describes the Veritas Storage Foundation for Sybase ASE CE software limitations in 6.0.3 and 6.0.1.

Only one Sybase instance is supported per node

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

SF Sybase CE is not supported in the Campus cluster environment

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

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

See the *Installation Guide* for more information.

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

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

SF Sybase CE installation is not supported by Web installer

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

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

See the *Installation Guide* for more information.

Symantec VirtualStore software limitations

This section describes the Symantec VirtualStore software limitations in 6.0.3 and 6.0.1.

VMware vSphere extension for VirtualStore limitations

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

F5 usage is not supported for wizard refreshing (2362940)

F5 usage is not supported for wizard refreshing.

Workaround

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

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

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

Documentation errata

There are no documentation errata updates.

List of patches

This section lists the patches and packages for 6.0.3.

Note: You can also view the following list using the `installmr` command, type:

```
./installmr -listpatches
```

Table 1-13 Patches and packages for Solaris SPARC

Patch ID	Package Name	Products Affected	Patch Size	Solaris 10
148481-02	VRTSvxfs	FS,SF,SFCFSHA, SFHA,SFSYBASECE,SVS	37 MB	X

Table 1-13 Patches and packages for Solaris SPARC *(continued)*

Patch ID	Package Name	Products Affected	Patch Size	Solaris 10
148490-02	VRTSvxvm	DMP,SF,SFCFSHA, SFHA,SFSYBASECE,SVS,VM	204 MB	X
148492-01	VRTSvcs	SFCFSHA,SFHA, SFSYBASECE,SVS,VCS	221 MB	X
148496-01	VRTSvcsag	SFCFSHA,SFHA, SFSYBASECE,SVS,VCS	6.2 MB	X
148497-01	VRTSvcsea	SFCFSHA,SFHA, SFSYBASECE,SVS,VCS	17 MB	X
148498-01	VRTSamf	SFCFSHA,SFHA, SFSYBASECE,SVS,VCS	4.9 MB	X
149691-01	VRTScavf	SFCFSHA, SFSYBASECE,SVS	881 KB	X
149695-01	VRTSvxfen	SFCFSHA,SFHA, SFSYBASECE,SVS,VCS	2.7 MB	X
149696-01	VRTSdbed	SF,SFCFSHA,SFHA, SFSYBASECE,SVS	116 MB	X
149699-01	VRTSperl	DMP,FS,SF,SFCFSHA,SFHA, SFSYBASECE,SVS,VCS,VM	57 MB	X
149702-01	VRTSsfcpi601	DMP,FS,SF,SFCFSHA,SFHA, SFSYBASECE,SVS,VCS,VM	5.0 MB	X

Table 1-14 Patches and packages for Solaris x64

Patch ID	Package Name	Products Affected	Patch Size	Solaris 10
148482-02	VRTSvxfs	FS,SF,SFCFSHA, SFHA,SVS	32 MB	X

Table 1-14 Patches and packages for Solaris x64 *(continued)*

Patch ID	Package Name	Products Affected	Patch Size	Solaris 10
148491-02	VRTSvxvm	DMP,SF,SFCFSHA, SFHA,SVS,VM	209 MB	X
148493-01	VRTSvcsag	SFCFSHA,SFHA,SVS,VCS	6.5 MB	X
148494-01	VRTSvcs	SFCFSHA,SFHA,SVS,VCS	229 MB	X
148495-01	VRTSamf	SFCFSHA,SFHA,SVS,VCS	4.8 MB	X
149692-01	VRTScavf	SFCFSHA,SVS	913 KB	X
149693-01	VRTSvcsea	SFCFSHA,SFHA,SVS,VCS	20 MB	X
149694-01	VRTSvxfen	SFCFSHA,SFHA,SVS,VCS	2.6 MB	X
149697-01	VRTSdbed	SF,SFCFSHA,SFHA,SVS	122 MB	X
149698-01	VRTSperl	DMP,FS,SF,SFCFSHA, SFHA,SVS,VCS,VM	54 MB	X
149703-01	VRTSsfcpi601	DMP,FS,SF,SFCFSHA, SFHA,SVS,VCS,VM	4.8 MB	X

Downloading the 6.0.3 archive

The patches that are included in the 6.0.3 release are available for download from the Symantec website. After downloading the 6.0.3 rolling patch, use gunzip and tar commands to uncompress and extract it.

For the 6.0.3 download archive and instructions, see the following TechNote on the Symantec Technical Support website:

http://www.symantec.com/docs/TECH164885

Chapter 2

Installing the products for the first time

This chapter includes the following topics:

Creating a new boot environment

Before installing SFHA 6.0.3 on a Solaris 11 host, you can optionally create a boot environment (BE) and install SFHA 6.0.3 on the new boot environment. This will help to rollback to previous version in future if required.

To create a new boot environment

1. Identify the active boot environment (BE) by looking at the NR tag:

   ```
   # beadm list
   ```

2. Create the BE:

   ```
   # beadm create bename
   ```

   For example,

   ```
   # beadm create sfha_603
   ```

3 Activate the BE:

```
# beadm activate bename
```

For example,

```
# beadm activate sfha_603
```

4 Reboot the node so that new be is active now.

```
# reboot
```

Installing the Veritas software using the script-based installer

This section describes how to install a 6.0.3 Veritas Storage Foundation and High Availability Solutions product for the first time on a host. Follow these instructions to make sure that you have the latest patches for the installer before you install or upgrade the product.

See the 6.0.1 *Installation Guide* and *Release Notes* for your product for more information.

If you already have 6.0.1 installed, you must upgrade to 6.0.3.

See "Upgrading to 6.0.3" on page 164.

To install the Veritas software for the first time

1 Download Storage Foundation and High Availability Solutions 6.0.1 from http://fileConnect.symantec.com.

2 Extract the tar ball into a directory called `/tmp/sfha601`.

3 Check http://sort.symantec.com/patches to see if there are any patches available for the 6.0.1 Installer. Download applicable P-patches and extract them to the `/tmp` directory.

4 Change the directory to `/tmp/sfha601`:

```
# cd /tmp/sfha601
```

5 Run the installer to install SFHA 6.0.1. See the Installation Guide for instructions on installing the 6.0.1 version of this product.

```
# ./installer -require complete_path_to_601_installer_patch
```

6 Download SFHA 6.0.3 from http://sort.symantec.com/patches.

7 Extract it to a directory called /tmp/sfha603.

8 Check http://sort.symantec.com/patches to see if there are patches available for the 6.0.3 installer. Download applicable P-patches and extract them to the /tmp directory.

9 Change the directory to /tmp/sfha603:

```
# cd /tmp/sfha603
```

10 On Solaris 11, before installing SFHA 6.0.3, you can optionally create a boot environment (BE) and install SFHA 6.0.3 on the new boot environment. This will help to rollback to previous version in future if required.

See "Creating a new boot environment" on page 149.

11 Invoke the installmr script to install 6.0.3:

```
# installmr -require complete_path_to_603_installer_patch
```

See "About the installmr and the uninstallmr scripts" on page 12.

12 If you did not configure the product after the 6.0.1 installation, the installer prompts you to configure the product during RP installation. If you do not want to configure the product now, answer **n** when prompted. To configure the product in the future, run the product installation script from the 6.0.1 installation media or from /opt/VRTS/install directory with the -configure option

Installing Veritas software using the Web-based installer

This section describes how to install a Veritas Storage Foundation and High Availability Solutions product for the first time on a host and then to install 6.0.3 using the Web-based installer. For detailed instructions on how to install 6.0.1 using the Web-based installer, follow the procedures in the 6.0.1 Installation Guide and Release Notes for your products.

See "Upgrading to 6.0.3" on page 164.

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

1 Start the Veritas XPortal Server process `xprtlwid`, on the installation server:

```
# ./webinstaller start
```

The webinstaller script displays a URL.

2 Start the Web browser on the system from which you want to perform the installation.

3 Navigate to the URL displayed from step 1.

4 The browser may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

5 When prompted, enter `root` and root's password of the installation server.

Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.

To obtain a security exception

1 Click **Or you can add an exception** link.

2 Click **Add Exception** button.

3 Click **Get Certificate** button.

4 Uncheck **Permanently Store this exception checkbox (recommended)**.

5 Click **Confirm Security Exception** button.

6 Enter root in User Name field and root password of the web server in the Password field.

Installing 6.0.3 with the Veritas Web-based installer

This section describes installing SF with the Veritas Web-based installer.

To install SF

1 The 6.0.1 version of the Veritas product must be installed before upgrading to 6.0.3.

See "Prerequisites for upgrading to 6.0.3" on page 163.

2 On the **Select a task and product** page, select **Install 6.0.3** from the **Task** drop-down list, and click **Next.**

3 Indicate the systems on which to install. Enter one or more system names, separated by spaces. Click **Validate**.

4 You have the option to let the installer configure SSH or RSH communications between the systems. If you choose to allow this configuration, select the shell and provide the root passwords for each system.

5 After the validation completes successfully, click **Next** to install 6.0.3 patches on the selected system.

6 Select the checkbox to specify whether you want to send your installation information to Symantec.

```
Would you like to send the information about this installation
to Symantec to help improve installation in the future?
```

Click **Finish**.

Installing the products using JumpStart

This chapter includes the following topics:

Generating the finish scripts

Perform these steps to generate the finish script to install SF.

To generate the finish script

1 Mount the 6.0.3 media and run the `installmr` program to generate the scripts.

```
# installmr -jumpstart directory_to_generate_scripts
```

where the *directory_to_generate_scripts* is the location where you want to put the scripts.

For example:

```
# ./installmr -jumpstart /js_scripts
```

2 When you are prompted to encapsulate the root disk automatically, choose **yes** to do so. If you do not want to encapsulate it automatically, choose **no** and go to step 6.

3. Specify a disk group name for the root disk.

   ```
   Specify the disk group name of the root disk to be encapsulated:
   rootdg
   ```

4. Specify private region length.

   ```
   Specify the private region length of the root disk to be
   encapsulated: (65536)
   ```

5. Specify the disk's media name of the root disk to encapsulate.

   ```
   Specify the disk media name of the root disk to be encapsulated:
   (rootdg_01)
   ```

6 JumpStart finish scripts of Veritas products, and encapsulation scripts are generated in the directory you specified in step 1. Output resembles:

```
The finish scripts for DMP is generated at \
/tmp/js_scripts/jumpstart_dmp.fin
The finish scripts for FS is generated at \
/tmp/js_scripts/jumpstart_fs.fin
The finish scripts for SF is generated at \
/tmp/js_scripts/jumpstart_sf.fin
The finish scripts for SFCFSHA is generated at \
/tmp/js_scripts/jumpstart_sfcfsha.fin
The finish scripts for SFHA is generated at
/tmp/js_scripts/jumpstart_sfha.fin
The finish scripts for SF Oracle RAC is generated at \
/tmp/js_scripts/jumpstart_sfrac.fin
The finish scripts for SFSYBASECE is generated at \
/tmp/js_scripts/jumpstart_sfsybasece.fin
The finish scripts for SVS is generated at \
/tmp/js_scripts/jumpstart_svs.fin
The finish scripts for VCS is generated at \
/tmp/js_scripts/jumpstart_vcs.fin
The finish scripts for VM is generated at \
/tmp/js_scripts/jumpstart_vm.fin
The encapsulation boot disk script for VM is generated at \
/tmp/js_scripts/encap_bootdisk_vm.fin
```

List the js_scripts directory.

```
# ls /js_scripts
```

You could select scripts according to the products you want to install and copy them to the `BUILDSRC NFS` shared location. For example, `/export/config` where you mounted the `BUILDSRC`.

For SF:

```
encap_bootdisk_vm.fin jumpstart_sf.fin
```

For SFHA:

```
encap_bootdisk_vm.fin jumpstart_sfha.fin
```

For SFCFS:

```
encap_bootdisk_vm.fin jumpstart_sfcfs.fin
```

For SF Oracle RAC:

```
encap_bootdisk_vm.fin jumpstart_sfrac.fin
```

For VCS:

```
encap_bootdisk_vm.fin jumpstart_vcs.fin
```

For DMP:

```
encap_bootdisk_vm.fin jumpstart_dmp.fin
```

For SVS:

```
encap_bootdisk_vm.fin jumpstart_svs.fin
```

For SF Sybase CE:

```
encap_bootdisk_vm.fin jumpstart_sfsybasece.fin
```

For FS:

```
encap_bootdisk_vm.fin jumpstart_fs.fin
```

For VM:

```
encap_bootdisk_vm.fin jumpstart_vm.fin
```

For AT:

```
encap_bootdisk_vm.fin jumpstart_at.fin
```

7 Copy the install and uninstall scripts of Veritas product that you are installing on to `BUILDSRC` shared location `/export/config` from 5.1 SP1 media.

For example:

```
# cp -p /dvd_mount/product_name/installprod  /export/config
# cp -p /dvd_mount/product_name/uninstallprod  /export/config
```

Here *prod* is one of /dmp/fs/sf/sfcfsha/sfsybasece/sfha/sfrac/svs/vcs/vm.

8 Modify the JumpStart script according to your requirements. You must modify the BUILDSRC and ENCAPSRC values. Keep the values aligned with the resource location values.

```
BUILDSRC="hostname_or_ip:/path_to_pkgs_patches_scripts"
```

Example: **BUILDSRC=10.209.100.100:/export/config**

```
// If you don't want to encapsulate the root disk automatically
// comment out the following line.
ENCAPSRC="hostname_or_ip:/path_to_encap_script"
```

9
- If you want to install other products packages in the Storage Foundation and High Availability suite, then use the product-specific install command with one of the following options to get a list of packages in the order to be installed:
  - minpkgs
  - recpkgs
  - allpkgs

    Use the list of packages that is generated to replace the package list in the finish scripts.
- If you want to install other products patches in the Storage Foundation and High Availability suite, then use the product-specific install command with one of the following options to get a list of patches in the order to be installed:

  ```
  # ./installmr -listpatches
  ```

  See "About the installmr and the uninstallmr scripts" on page 12.
  See "The installmr script options" on page 12.

10 Once the installation is complete, refer to installation and configuration guide for the respective product from 6.0.1 to proceed with the configuration.

Overview of JumpStart installation tasks

Review the summary of tasks before you perform the JumpStart installation.

Summary of tasks

1 Add a client (register to the JumpStart server). See the JumpStart documentation that came with your operating system for details.

2 Read the JumpStart installation instructions.

3 Generate the finish scripts.

See "Generating the finish scripts" on page 155.

4 Modify the rules file for JumpStart.

See the JumpStart documentation that came with your operating system for details.

5 Prepare installation resources.

See "Preparing installation resources" on page 160.

6 On each client node, run the following command to install the Veritas product packages and patches:

For Solaris SPARC:

```
Ok> boot net -  install
```

For Solaris x64:

Press **F12** and select the network boot mode.

Note: The system is restarted after the packages are installed. If you choose to encapsulate the root disk on your systems, the systems start with an encapsulated root disk.

7 Run the `installer` command from the disc or from directory `/opt/VRTS/install` directory to configure the Veritas software.

```
# /opt/VRTS/install/installprod vers -configure
```

where `installprod vers` is the product's installation command.

Preparing installation resources

Prepare resources for the JumpStart installation.

To prepare the resources

1 Copy the contents of 6.0.1 disk and 6.0.3 disk both to buildsrc.

```
# cd /cdrom/cdrom0
# cp -r * BUILDSRC
```

Note: After you copied the patches, you must uncompress them using the gunzip and tar commands.

2 Generate the response file for the package and patch list that you found when you generated the finish script.

See "Generating the finish scripts" on page 155.

To view the patches, packages and operating systems for your Veritas product use the `installmr -listpatches` command, type:

```
# ./installmr -listpatches
```

```
# cd BUILDSRC/pkgs/
# pkgask -r package_name.response -d /BUILDSRC/pkgs/packages_name.pkg
```

3 Create the adminfile file under *BUILDSRC*/pkgs/ directory. The adminfile file's contents follow:

```
mail=
instance=overwrite
partial=nocheck
runlevel=quit
idepend=quit
rdepend=nocheck
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

4 Copy the install and uninstall scripts that you created when you generated the finish script to *BUILDSRC* if you want to configure or uninstall from `/opt/VRTS/install`. Otherwise, you need to configure and uninstall from disc.

See "Generating the finish scripts" on page 155.

5. If you want to encapsulate the root disk automatically when perform the JumpStart installation, copy the scripts `encap_bootdisk_vm.fin` created when you generated the finish script to *ENCAPSRC*.

6. Modify the rules file as required.

   For example:

   ```
   any - - profile_sf jumpstart_sf51.fin
   ```

   For detailed instructions, see the *Oracle's JumpStart* documentation.

Adding language pack information to the finish file

For the language pack, copy the language packages from the language pack installation disc to the shared storage.

```
# cd /cdrom/cdrom0/pkgs
# cp -r * BUILDSRC/pkgs
```

Add lines for the language packages in the finish script. If the finish file resembles:

```
. . .
for PKG in VRTSperl VRTSvlic VRTSicsco . . .

do
...
done
```

Add the following lines for the language pack after the patch information for VCS. Copy the command syntax between the "do" and "done" lines and add that for the language pack lines as well. Note that the line that starts "for PKG" is on three lines in this guide, but should be on a single line in the file.

```
. . .
for PKG in VRTSmulic VRTSatJA VRTSjacav VRTSjacs VRTSjacse
VRTSjacsu VRTSjadba VRTSjafs VRTSjavm VRTSjadbe VRTSjaodm
VRTSatZH VRTSzhvm

do
.
.
.
done
```

Upgrading to 6.0.3

This chapter includes the following topics:

Prerequisites for upgrading to 6.0.3

The following list describes prerequisites for upgrading to the 6.0.3 release:

- For any product in the Veritas Storage Foundation stack, you must have the 6.0.1 installed before you can upgrade that product to the 6.0.3 release.
- Each system must have sufficient free space to accommodate patches.
- See http://www.symantec.com/docs/TECH202397 before upgrading to Oracle Solaris 11.1.
- The full list of prerequisites can be obtained by running `./installmr -precheck`.
- Make sure to download the latest patches for the installer.
  See "Downloading required software to upgrade to 6.0.3 " on page 163.

Downloading required software to upgrade to 6.0.3

This section describes how to download the latest patches for the installer.

To download required software to upgrade to 6.0.3

1. Download SFHA 6.0.3 from http://sort.symantec.com/patches.
2. Extract it to a directory such as `/tmp/sfha603`.
3. Check http://sort.symantec.com/patches to see if there are patches available for the 6.0.3 installer. Download applicable P-patches and extract them to the `/tmp` directory.
4. When you run the `installmr` script, use the `-require` option and specify the location where you downloaded the 6.0.3 installer patches.

Supported upgrade paths

This section describes the supported upgrade paths for this release.

- 6.0.1 to 6.0.3

You can use this installation option to upgrade to the following releases:

Upgrading to 6.0.3

This section describes how to upgrade from 6.0.1 to 6.0.3 on a cluster or a standalone system.

For Solaris 11:

See "Creating a new boot environment" on page 149.

- Performing a full upgrade to 6.0.3 on a cluster
  Use the procedures to perform a full upgrade to 6.0.3 on a cluster that has Veritas Cluster Server (VCS), Veritas Storage Foundation and High Availability Solutions (SFHA), Veritas Storage Foundation Cluster File System High Availability(SFCFSHA), Veritas Storage Foundation for Oracle RAC (SFRAC), Veritas Storage Foundation for Sybase ASE CE (SF Sybase CE), or Symantec VirtualStore (SVS) installed and configured.
- Upgrading to 6.0.3 on a standalone system
  Use the procedure to upgrade to 6.0.3 on a system that has SF installed.
- Upgrading Veritas products using Live Upgrade
  Use the procedure to upgrade your Veritas product with a Live Upgrade.
- Performing a rolling upgrade using the `installmr` script
  Use the procedure to upgrade your Veritas product with a rolling upgrade.
- Manually installing packages on Solaris brand non-global zones

Use the procedure to install packages on Solaris brand non-global zones manually.

See "Installing the Veritas software using the script-based installer" on page 150.

Performing a full upgrade to 6.0.3 on a cluster

Performing a full upgrade on a cluster requires stopping cluster failover functionality during the entire procedure. However, if you use Veritas Storage Foundation Cluster File System High Availability (SFCFSHA) and Cluster Volume Manager (CVM), the SFCFSHA and CVM services remain available.

Depending on your cluster's configuration, select one of the following procedures to upgrade to 6.0.3:

- Performing a full upgrade to 6.0.3 on a Veritas Cluster Server
- Performing a full upgrade to 6.0.3 on an SFHA cluster
- Performing a full upgrade to 6.0.3 on an SFCFSHA cluster
- Performing a full upgrade to 6.0.3 on an SF Oracle RAC cluster
- Performing a full upgrade to 6.0.3 on an SF Sybase ASE CE cluster
  See "Downloading required software to upgrade to 6.0.3 " on page 163.

Performing a full upgrade to 6.0.3 on a Veritas Cluster Server

The following procedure describes performing a full upgrade on a Veritas Cluster Server (VCS) cluster.

To upgrade VCS

1. Make sure you have downloaded the latest software required for the upgrade.

   See "Downloading required software to upgrade to 6.0.3 " on page 163.

2. Log in as superuser.

   Note: Upgrade the Operating System and reboot the systems if required.

   See "System requirements" on page 26.

3 Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.0.3 rolling patch binaries, change to the directory that contains the installmr script. Start the pre-upgrade check:

```
# ./installmr -precheck node1 node2 ... nodeN
```

See "About the installmr and the uninstallmr scripts" on page 12.

4 Resolve any issues that the precheck finds.

5 Start the upgrade:

```
# ./installmr node1 node2 ... nodeN
```

See "About the installmr and the uninstallmr scripts" on page 12.

6 After the upgrade, review the log files for any issues.

Performing a full upgrade to 6.0.3 on an SFHA cluster

The following procedure describes performing a full upgrade on an SFHA and VCS cluster.

To perform a full upgrade to 6.0.3 on an SFHA cluster

1 Make sure you have downloaded the latest software required for the upgrade.

See "Downloading required software to upgrade to 6.0.3 " on page 163.

2 Log in as superuser.

3 Verify that `/opt/VRTS/bin` and `/opt/VRTSvcs/bin` is in your `PATH` so that you can execute all product commands.

4 If you install VCS on Solaris 10 systems that run non-global zones, make sure that all non-global zones are booted and in the running state on each node before you upgrade the SFHA stack in the global zone.

5 On any node in the cluster, make the VCS configuration read only:

```
# haconf -dump -makero
```

6 Stop VCS.

To stop applications, unmount VxFS file systems and stop VxVM volumes managed by VCS.

```
# hastop -all
```

7 Stop all the applications that are using VxFS files systems and VxVM volumes which are not managed by VCS.

Use application's native commands to stop applications.

8 On each node, enter the following command to check if any Storage Checkpoints are mounted:

```
# df -F vxfs
```

If any Storage Checkpoints are mounted, on each node in the cluster, unmount all Storage Checkpoints.

```
# umount /checkpoint_name
```

9 On each node, enter the following command to check if any VxFS file systems are mounted.

Unmount the VxFS file systems that are not managed by VCS.

```
# df -F vxfs
```

If any VxFS file systems are present, on each node in the cluster, stop IOs on the file systems, unmount all of the VxFS file systems:

```
# umount /filesystem
```

10 If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vxrvg stop` command to stop each RVG individually:

  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

  Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

11 Stop activity to all VxVM volumes that are not managed by VCS.

For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.Use application specific commands to stop the applications.

12 On each node, stop all VxVM volumes by entering the following command for each disk group, which are not managed by VCS:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

13 Deport all the disk groups which are not managed under VCS.

```
# vxdg deport diskgroup
```

14 If required, apply the OS kernel patches.

See “System requirements” on page 26.

See Oracle's documentation for the procedures.

15 On each node, check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

16 Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.0.3 rolling patch binaries, change to the directory that contains the `installmr` script. Start the pre-upgrade check:

```
# ./installmr -precheck node1 node2 ... nodeN
```

where *node1* and *node2* are nodes which are to be upgraded.

See “About the installmr and the uninstallmr scripts” on page 12.

Resolve any issue that the precheck finds.

17 Start the upgrade.

```
# ./installmr [-rsh]  node1 node2 ... nodeN
```

Review the output.

18 Enter the following command on each node to take service groups online:

```
# hagrp -online service_group -sys nodename
```

19 If necessary, reinstate any missing mount points in the /etc/vfstab file on each node.

20 Import all the diskgroups that are not managed by VCS:

```
# vxdg import diskgroup
```

21 Restart all the volumes by entering the following command for each disk group that are not managed by VCS:

```
# vxvol -g diskgroup startall
```

22 If you stopped any RVGs in step 10, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

23 Remount all VxFS file systems on all nodes, which are not managed by VCS:

```
# mount -F vxfs blockdevice mountpoint
```

24 Remount all Storage Checkpoints on all nodes:

```
# mount -F vxfs -o ckpt=name blockdevice checkpoint_name
```

25 Start all applications which are using VxFS files systems that are not managed by VCS.

Use application native commands to start the applications.

Performing a full upgrade to 6.0.3 on an SFCFSHA cluster

The following procedure describes performing a full upgrade on an SFCFSHA cluster.

To perform a full upgrade to 6.0.3 on an SFCFSHA cluster

1 Make sure you have downloaded the latest software required for the upgrade.

See “Downloading required software to upgrade to 6.0.3 ” on page 163.

2 Log in as superuser.

3 Verify that /opt/VRTS/bin and /opt/VRTSvcs/bin is in your PATH so that you can execute all product commands.

4 If you install VCS on Solaris 10 systems that run non-global zones, make sure that all non-global zones are booted and in the running state on each node before you install or upgrade the SFCFSHA stack in the global zone.

5 On any node in the cluster, make the VCS configuration read only:

```
# haconf -dump -makero
```

6 Stop VCS.

To stop applications, unmounts VxFS/CFS file systems and stop VxVM/CVM volumes managed under VCS.

```
# hastop -all
```

7 Stop all applications which are using CFS files systems and VxVM volumes that are not managed by VCS.

Use application native commands to stop applications.

8 On each node, enter the following command to check if any Storage Checkpoints are mounted:

```
# df -F vxfs
```

If any Storage Checkpoints are mounted, on each node in the cluster unmount all Storage Checkpoints.

```
# cfsumount /checkpoint_name
```

9 On each node, enter the following command to check if any VxFS/CFS file systems are mounted not manage by VCS:

Unmount the VxFS/CFS file systems that are not managed by VCS.

```
# df -F vxfs
```

If any VxFS/CFS file systems are present, on each node in the cluster, stop IOs on the file systems, unmount all of the VxFS/CFS file systems:

```
# cfsumount /filesystem
or
# umount /filesystem
```

10 If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.

- Use the `vxrvg stop` command to stop each RVG individually:

  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

  Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

11 Stop activity to all VxVM/CVM volumes that are not managed by VCS.

For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

12 On each node, stop all VxVM/CVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

13 Deport all the disk groups which are not managed under VCS.

```
# vxdg deport diskgroup
```

14 If required, apply the OS kernel patches.

See “System requirements” on page 26.

See Oracle’s documentation for the procedures.

15 On each node, check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

16 Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.0.3 rolling patch binaries, change to the directory that contains the `installmr` script.

Start the pre-upgrade check:

```
# ./installmr -precheck node1 node2 ... nodeN
```

where *node1* and *node2* are nodes which are to be upgraded.

See "About the installmr and the uninstallmr scripts" on page 12.

Resolve any issue that the precheck finds.

17 Start the upgrade.

```
# ./installmr [-rsh] node1 node2 ... nodeN
```

Review the output.

18 Enter the following command on each node to take service groups online:

```
# hagrp -online service_group -sys nodename
```

19 If necessary, reinstate any missing mount points in the `/etc/vfstab` file on each node.

20 Import all the diskgroups that are not managed by VCS:

```
# vxdg import diskgroup
```

21 Restart all the volumes by entering the following command for each disk group that are not managed by VCS:

```
# vxvol -g diskgroup startall
```

22 If you stopped any RVGs in step 10, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

23 Remount all CFS/VxFS file systems on all nodes:

```
# cfsmount mountpoint
or
# mount -F fstype blockdevice mountpoint
```

24 Remount all Storage Checkpoints on all nodes:

```
# cfsmount /checkpoint_name
or
# mount -F vxfs -o ckpt=name blockdevicemountpoint
```

25 Start all applications which are using VxFS/CFS files systems that are not managed by VCS. Use the application native commands to start the applications.

Performing a full upgrade to 6.0.3 on an SF Oracle RAC cluster

The following procedure describes performing a full upgrade on an SF for Oracle RAC cluster.

To upgrade to 6.0.3 on an SF Oracle RAC cluster

1 Make sure you have downloaded the latest software required for the upgrade.

See “Downloading required software to upgrade to 6.0.3 ” on page 163.

2 Log in as superuser.

3 Verify that `/opt/VRTSvcs/bin` is in your `PATH` so that you can execute all product commands.

4 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

5 Enter the following command to freeze HA service group operations on each node:

```
# hasys -freeze -persistent nodename
```

6 Make the configuration read-only:

```
# haconf -dump -makero
```

7 If Oracle Clusterware is not controlled by VCS, enter the following command on each node of the cluster to stop Oracle Clusterware:

```
# $CRS_HOME/bin/crsctl stop crs
```

8 Stop VCS.

```
# hastop -all
```

9 If required, apply the OS kernel patches.

See "System requirements" on page 26.

See *Oracle's* documentation for the procedures.

10 From the directory that contains the extracted and untarred 6.0.3 rolling patch binaries, change to the directory that contains the installmr script. If ssh key authentication is configured then enter:

```
# ./installmr  node1 node2
```

If ssh is not configured then enter:

```
# ./installmr -rsh node1 node2
```

where node1 and node2 are nodes which are to be upgraded.

11 After the entire cluster is upgraded, follow the installer instructions to proceed further.

12 If necessary, reinstate any missing mount points in the /etc/vfstab file on each node.

13 Manually mount the VxFS and CFS file systems that are not managed by VCS.

14 Start all applications on the cluster that are not configured under VCS. Use native application commands to start the application.

15 Relink the SF Oracle RAC libraries with Oracle.

Refer to *Veritas Storage Foundation for OracleRAC 6.0.1 or later Installation and Configuration Guide* for more information.

16 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

17 Enter the following command on each node to unfreeze HA service group operations:

```
# hasys -unfreeze -persistent nodename
```

18 Make the configuration read-only:

```
# haconf -dump -makero
```

19 Enter the following command on each node to take service groups online:

```
# hagrp -online service_group -sys nodename
```

20 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

21 Remount all VxFS file systems on all nodes:

```
# mount /filesystem
```

22 If Oracle Clusterware is not controlled by VCS, enter the following command on each node to start Oracle Clusterware.

```
# $CRS_HOME/bin/crsctl start crs
```

23 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

Performing a full upgrade to 6.0.3 on an SF Sybase ASE CE cluster

The following procedure describes performing a full upgrade on an SF for Oracle RAC cluster.

To upgrade to 6.0.3 on an SF Sybase ASE CE cluster

1 Make sure you have downloaded the latest software required for the upgrade.

See “Downloading required software to upgrade to 6.0.3 ” on page 163.

2 Log in as superuser.

3 Verify that `/opt/VRTSvcs/bin` is in your `PATH` so that you can execute all product commands.

4 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

5 Enter the following command to freeze HA service group operations on each node:

```
# hasys -freeze -persistent nodename
```

6 Make the configuration read-only:

```
# haconf -dump -makero
```

7 Take the Sybase database group offline:

```
# hagrp -offline sybasece -sys node_name
```

8 Stop VCS.

```
# hastop -all
```

9 If required, apply the OS kernel patches.

See "System requirements" on page 26.

See *Sybase* documentation for the procedures.

10 From the directory that contains the extracted and untarred 6.0.3 rolling patch binaries, change to the directory that contains the installmr script. If ssh key authentication is configured then enter:

```
# ./installmr  node1 node2
```

If ssh is not configured then enter:

```
# ./installmr -rsh node1 node2
```

where `node1` and `node2` are nodes which are to be upgraded.

11 After the entire cluster is upgraded, follow the installer instructions to proceed further.

12 If necessary, reinstate any missing mount points in the `/etc/vfstab` file on each node.

13 Manually mount the VxFS and CFS file systems that are not managed by VCS.

14 Start all applications on the cluster that are not configured under VCS. Use native application commands to start the application.

15 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

16 Enter the following command on each node to unfreeze HA service group operations:

```
# hasys -unfreeze -persistent nodename
```

17 Make the configuration read-only:

```
# haconf -dump -makero
```

18 Enter the following command on each node to take service groups online:

```
# hagrp -online service_group -sys nodename
```

19 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

20 Remount all VxFS file systems on all nodes:

```
# mount /filesystem
```

21 Bring the Sybasece resource group online.

```
# hagrp -online sybasece -sys node_name
```

22 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

Upgrading to 6.0.3 on a standalone system

You can use this procedure to upgrade on a standalone system that runs SF.

To upgrade to 6.0.3 on a standalone system

1 Make sure you have downloaded the latest software required for the upgrade.

See "Downloading required software to upgrade to 6.0.3 " on page 163.

2 Log in as superuser.

3 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

4 If required, apply the OS kernel patches.

See "System requirements" on page 26.

See Oracle's documentation for the procedures.

5 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -F vxfs
```

6 Unmount all Storage Checkpoints and file systems:

```
# cfsumount /checkpoint_name
# cfsumount /filesystem
```

7 If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vxrvg stop` command to stop each RVG individually:

  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

  Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

8 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

9 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

10 Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

11 Copy the patch archive downloaded from the patch central to temporary location, untar the archive and browse to the directory containing the installmr installer script. Enter the `installmr` script:

```
# ./installmr nodename
```

12 If necessary, reinstate any missing mount points in the `/etc/vfstab` file.

13 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

14 If you stopped any RVGs in step 7, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

15 Remount all VxFS file systems and Storage Checkpoints:

```
# mount /filesystem
# mount /checkpoint_name
```

16 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

Upgrading Veritas products using Live Upgrade

This section describes how to upgrade 6.0.1 to 6.0.3 using Live Upgrade.

Supported live upgrade paths:

- Upgrading Veritas Products without Solaris OS upgrade:
  - Upgrading Solaris 10 Update x 6.0.1 to Solaris 10 Update x 6.0.3

- Upgrading Veritas Products with Solaris OS upgrade
  - Upgrading Solaris 10 Update x 6.0.1 to Solaris 10 Update y 6.0.3

Prerequisites to upgrade to 6.0.3 using Live Upgrade:

- The node should have an alternate boot disk that is identical to the primary boot disk.
- Installation disc for 6.0.1 and 6.0.3 to be installed on the ABE.
- Installation disc for target OS to be installed on ABE.
- The latest list of required patches is available in the Oracle Solaris Live Upgrade Software:

  Patch Requirements (Doc ID 1004881.1) document in My Oracle Support (https://support.oracle.com/).
- If OS upgrade is involved, then remove the currently installed SUNWluu, SUNWlur and SUNWlucfg packages and install SUNWluu, SUNWlur, SUNWlucfg packages from target OS. Also replace SUNWluzone if zones are involved.
- The `vxlustart` script takes around 2-3 hours to complete uninterrupted. Symantec recommends to have a network connection that does not time out in the interim.

Upgrading Veritas products using Live Upgrade from 6.0.1 to 6.0.3 without OS upgrade

This section describes how to upgrade SF, SFHA, SFCFSHA, SFSYBASECE, or SF for Oracle RAC from 6.0.1 to 6.0.3 using Live Upgrade where OS upgrade is not involved.

To upgrade your Veritas product using Live Upgrade

1. Ensure that 6.0.1 is installed and configured on PBE.

   See your Veritas product 6.0.1 Installation Guide for more information.

2. Run the `vxlustart -V` command to ensure there are no problems before beginning the Live Upgrade process.

   If the `vxlustart -V` command reports success, proceed with running the `vxlustart` command.

   If the `vxlustart -V` command reports errors, correct the problem, and run the `vxlustart -V` command again.

   Note: This `vxlustart -V` command does not catch failures that are reported by Solaris Live Upgrade commands.

   ---

3. Run the `installmr` command to upgrade your Veritas product:

   ```
   # ./installmr -rootpath /altroot_path
   ```

4. Run the `vxlufinish` command to complete the Live Upgrade:

   - If the primary root disk is not encapsulated, run the following command:

     ```
     # ./vxlufinish -u target_os_version
     ```

   - If the primary root disk is encapsulated by VxVM, run the following command:

     ```
     # ./vxlufinish -u target_os_version -g diskgroup
     ```

5. Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

   ```
   # shutdown -g0 -y -i6
   ```

6. Verify that the alternate boot environment is active.

   ```
   # lustatus
   ```

7. In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

   ```
   # gabconfig -a
   ```

Upgrading Veritas products using Live Upgrade from 6.0.1 to 6.0.3 with OS upgrade

This section describes how to upgrade SF, SFHA, SFCFSHA, SFSYBASECE, or SF for Oracle RAC from 6.0.1 to 6.0.3 using Live Upgrade where OS upgrade is involved.

To upgrade your Veritas product using Live Upgrade

1. Ensure that 6.0.1 is installed and configured on PBE.

   See your Veritas product 6.0.1 Installation Guide for more information.

2. Run the `vxlustart -V` command to ensure there are no problems before beginning the Live Upgrade process.

   If the `vxlustart -V` command reports success, proceed with running the `vxlustart` command.

   If the `vxlustart -V` command reports errors, correct the problem, and run the `vxlustart -V` command again.

   Note: This `vxlustart -V` command does not catch failures that are reported by Solaris Live Upgrade commands.

   ---

3. Run the `vxlustart` command to start the Live Upgrade for your Veritas product:

   ```
   # ./vxlustart -v -u target_os_version -s osimage_path -d disk_name
   ```

4. If you are upgrading from Solaris 9 Update x to Solaris 10 Update y, uninstall Veritas products on ABE, else go to Step 6.

   ```
   # ./installprod -rootpath /altroot_path
   ```

5. Install Veritas products again on ABE.

   ```
   # ./installprod -rootpath /altroot_path
   ```

6. Run the `installmr` command to upgrade your Veritas product:

   ```
   # ./installmr -rootpath  /altroot_path
   ```

7 In case of SFRAC, refer to the “Completing the Live upgrade” section in SFRAC 6.0.1 Installation and Configuration guide. For other products, go to the next step.

8 Run the `vxlufinish` command to complete the Live Upgrade:

- If the primary root disk is not encapsulated, run the following command:

  ```
  # ./vxlufinish -u target_os_version
  ```

- If the primary root disk is encapsulated by VxVM, run the following command:

  ```
  # ./vxlufinish -u target_os_version -g diskgroup
  ```

9 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

```
# shutdown -g0 -y -i6
```

10 Verify that the alternate boot environment is active.

```
# lustatus
```

11 In a cluster environment, make sure that all the GAB ports are up. Note that different ports appear for different products.

```
# gabconfig -a
```

12 In case of SFRAC, refer to the “Performing post-upgrade Tasks” section to relink Oracle RAC libraries with SF Oracle RAC from 6.0.1 Installation and Configuration guide.

Performing a rolling upgrade using the `installmr` script

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

- About rolling upgrades
- Prerequisites for a rolling upgrades
- Performing a rolling upgrade using the installer

About rolling upgrades

You can use rolling upgrades to upgrade one product from a release to the next. Rolling upgrades require less downtime.

Rolling upgrades take two discrete phases. In the first, you upgrade the kernel packages with exception of VCS packages and agent packages. In the second, you upgrade the non-kernel packages, which are VCS packages and agents packages.

You can perform a rolling upgrade for the following products:

- Veritas Cluster Server
- Storage Foundation and High Availability
- Storage Foundation Cluster File System and High Availability
- Storage Foundation for Oracle RAC
- Symantec VirtualStore
- Storage Foundation for Sybase CE

You can perform a rolling upgrade from 6.0.1 to 6.0.3.

Prerequisites for a rolling upgrades

Meet the following prerequisites before performing a rolling upgrade:

- Make sure that the product you want to upgrade supports rolling upgrade.
- Split up your cluster into sub-clusters for the purpose of upgrade. A sub-cluster can include one or more nodes. This division helps to keep service groups running during the upgrade.
- Make sure you are logged in as superuser and have the media mounted.
- VCS must be running before performing the rolling upgrade.
- For SF Oracle RAC, stop Oracle Clusterware before upgrading Kernel packages on any node, which is not managed by VCS.
- Make sure you have downloaded the latest software required for the upgrade.

  See "Downloading required software to upgrade to 6.0.3 " on page 163.

Limitation: During VCS and agents upgrade, you must bring down the application High Availability (HA) for several minutes. This does not affect the application running on the cluster. You can restore the application's high availability after VCS and the agent packages are upgraded.

Performing a rolling upgrade using the installer

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

Performing a rolling upgrade on kernel packages for VCS, SFHA, SFSYBASECE, SVS and SFCFSHA: phase 1

Note that in the following instructions a sub-cluster can represent one or more nodes in a full cluster, but is represented by nodeA.

To perform the rolling upgrade on kernel packages: phase 1

1. Stop all the applications that access volumes which are not under VCS control in the sub-cluster to be upgraded.
2. Unmount all the file systems managed by SF which are not under VCS control in the sub-cluster to be upgraded.
3. On the first sub-cluster, start the installer for the rolling upgrade with the `-rollingupgrade_phase1` option.

   ```
   # ./installmr -rollingupgrade_phase1 nodeA
   ```

4. Note that if the boot-disk is encapsulated, then you do not need to perform an unencapsulation for upgrades.
5. The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type **y** to continue.
6. The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type **y** to continue. If you choose to specify the nodes, type **n** and enter the names of the nodes.
7. The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type **y** to continue or quit the installer and address the precheck's warnings.
8. After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:

   - Manually switch service groups
   - Use the CPI to automatically switch service groups

   The downtime is the time that it normally takes for the service group's failover.

9. After switching failover service group, installer detects if there are online parallel service groups on the node to be upgraded. If there are online parallel service groups, installer will ask user to use CPI to automatically offline parallel service groups.

10. The installer stops relevant processes, uninstalls old kernel packages, and installs the new packages. When prompted, enable replication or global cluster capabilities, if required, and register the software.

11. The installer performs the upgrade configuration and re-starts processes.

    If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.

12. If the boot disk is encapsulated, reboot the first sub-cluster's system. Otherwise go to step 13.

13. Before you proceed to phase 2, complete step 1 to step 11 on the second subcluster.

Performing a rolling upgrade on non-kernel packages for VCS, SFHA, SFSYBASECE, SVS and SFCFSHA: phase 2

In this phase installer installs all non-kernel patches on all the nodes in cluster and restarts VCS cluster.

To perform the rolling upgrade on non-kernel packages: phase 2

1. When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type **y** to continue.

2. Reboot the nodes if the installer requires.

3. The installer determines the remaining packages to upgrade. Press **Enter** to continue.

4. The installer stops Veritas Cluster Server (VCS) processes but the applications continue to run. Type **y** to continue.

   The installer performs prechecks, uninstalls old packages, and installs the new packages. It performs post-installation tasks, and the configuration for the upgrade.

5. Type **y** or **n** to help Symantec improve the automated installation.

6. If you have network connection to the Internet, the installer checks for updates.

7. A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.

8 Verify the cluster's status:

```
# hastatus -sum
```

9 If you want to upgrade CP server systems that use VCS or SFHA to 6.0.3, make sure that you upgraded all application clusters to version 6.0.3. Then, upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA installation guide.

Preparing to perform a rolling upgrade for SFRAC

Perform the preparatory steps in this section if you are performing a rolling upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.

Note: Perform the steps on the first subcluster.

To prepare to upgrade SF Oracle RAC:

1 Log in as superuser to one of the nodes in the cluster.

2 Back up the following configuration files on your system: `main.cf`, `types.cf`, `CVMTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`

For example:

```
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.save
# cp /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/config/types.cf.save
# cp /etc/VRTSvcs/conf/config/OracleTypes.cf \
/etc/VRTSvcs/conf/config/OracleTypes.cf.save
# cp /etc/VRTSvcs/conf/config/PrivNIC.cf \
/var/VRTSvcs/conf/config/PrivNIC.cf.save
# cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
/var/VRTSvcs/conf/config/MultiPrivNIC.cf.save
```

3 Stop the applications that use VxFS or VxVM disk groups on each node, whether local or CFS.

If the applications are under VCS control:

```
# hagrp -offline grp_name -sys node_name
```

If the applications are not under VCS control, use native application commands to stop the application.

4 For Oracle RAC 10g and Oracle RAC 11g

Stop the Oracle RAC resources on each node.

- If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

```
# hagrp -offline grp_name -sys node_name
```

- If the database instances are not managed by VCS, then run the following on one node:

```
$ srvctl stop instance -d db_name -i instance_name
```

5
- If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts. Failing to perform this step results in the database attempting to come online after the upgrade; the attempt fails due to the presence of old libraries on the system.

```
# haconf -makerw
# hagrp -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:

```
$ srvctl modify database -d db_name -y manual
```

6 Take all the VCS service groups offline:

```
# hagrp -offline grp_name -sys sys_name
```

7 Unmount all the VxFS file system which is not under VCS control.

```
# mount -v |grep vxfs
```

```
# fuser -c /mount_point
```

```
# umount /mount_point
```

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```
# fuser -cu /mount_point
```

Performing a rolling upgrade on kernel packages for SFRAC: phase 1

Note that in the following instructions that a sub-cluster can represent one or more nodes in a full cluster, but is represented by nodeA.

To perform the rolling upgrade on kernel packages: phase 1

1 On the first subcluster, start the installer for the rolling upgrade with the `-rollingupgrade_phase1` option.

```
 # ./installmr -rollingupgrade_phase1 nodeA
```

2 Note that if the boot disk is encapsulated, then you do not need to perform an unencapsulation for upgrades.

3 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type **y** to continue.

4 The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type **y** to continue. If you choose to specify the nodes, type **n** and enter the names of the nodes.

5 The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type **y** to continue or quit the installer and address the precheck's warnings.

6 After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:

- Manually switch service groups

- Use the CPI to automatically switch service groups

  The downtime is the time that it normally takes for the service group's failover.

7 After switching failover service group, installer detects if there are online parallel service groups on the node to be upgraded. If there are online parallel service groups, installer will ask user to use CPI to automatically offline parallel service groups.

8 The installer stops relevant processes, uninstalls old kernel packages, and installs the new packages. When prompted, enable replication or global cluster capabilities, if required, and register the software.

9 The installer performs the upgrade configuration and re-starts processes.

  If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.

  Note: The Oracle service group is offline as the AutoStart attribute is set to 0 to prevent the service group from starting automatically. The service group is started later in the process.

10 In case of SFRAC, refer to the “Performing post-upgrade Tasks” section to relink Oracle RAC libraries with SF Oracle RAC from 6.0.1 Installation and Configuration guide.

11 Bring the Oracle database service group online.

- If VCS manages the Oracle database:

```
# hagrp -online oracle_group -sys node_name
```

- If VCS does not manage the Oracle database:

```
# srvctl start database -d db_name
```

12 Manually mount the VxFS and CFS file systems that are not managed by VCS.

13 Start all applications that VCS does not manage. Use native application commands to start the applications.

14 If the boot disk is encapsulated, reboot the first sub-cluster's system.

15 Before you proceed to phase 2, complete step 1 to 14 on the second subcluster.

16 - If VCS manages the Oracle database, reset the AutoStart value to 1 to enable VCS to bring the database service group online when VCS starts:

```
# haconf -makerw
# hagrp -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If VCS does not manage the Oracle database, change the management policy for the database to automatic:

  ```
  $ srvctl modify database -d db-name -y AUTOMATIC
  ```

Performing a rolling upgrade on non-kernel packages for SFRAC: phase 2

In this phase installer installs all non-kernel packages on all the nodes in cluster and restarts VCS cluster.

To perform the rolling upgrade on non-kernel packages: phase 2

1. When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type **y** to continue.
2. Reboot the nodes if the installer requires.
3. The installer determines the remaining packages to upgrade. Press **Enter** to continue.
4. The installer stops Veritas Cluster Server (VCS) processes but the applications continue to run. Type **y** to continue.

   The installer performs prechecks, uninstalls old packages, and installs the new packages. It performs post-installation tasks, and the configuration for the upgrade.
5. Type **y** or **n** to help Symantec improve the automated installation.
6. If you have network connection to the Internet, the installer checks for updates.
7. A prompt message appears to ask if the user would like to read the summary file. You can choose **y** if you want to read the install summary file.
8. Verify the cluster's status:

   ```
   # hastatus -sum
   ```
9. If you want to upgrade CP server systems that use VCS or SFHA to 6.0.3, make sure that you upgraded all application clusters to version 6.0.3. Then, upgrade VCS or SFHA on the CP server systems.

   For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA installation guide.

Manually installing packages on Solaris brand non-global zones

With Oracle Solaris 11, you must manually install SFHA packages inside non-global zones. The native non-global zones are called Solaris brand zones.

To install packages manually on Solaris brand non-global zones:

1 Ensure that the SMF service svc:/application/pkg/system-repository:default is online on the global zone.

```
# svcs svc:/application/pkg/system-repository
```

2 Log on to the non-global zone as a superuser.

3 Copy the VRTSpatches.p5p package from the pkgs directory from the installation media to the non-global zone (for example at `/tmp/install` directory).

4 Disable the publishers that are not reachable, as package install may fail if any of the already added repositories are unreachable.

```
#pkg set-publisher --disable <publisher name>
```

5 Add a file-based repository in the non-global zone.

```
# pkg set-publisher -p/tmp/install/VRTSpatches.p5p Symantec
```

6 Install the required packages.

```
# pkg install --accept VRTSperl VRTSvlic VRTSvxfs VRTSvcs VRTSvcsag
VRTSvcsea VRTSodm
```

7 Remove the publisher on the non-global zone.

```
#pkg unset-publisher Symantec
```

8 Clear the state of the SMF service, as setting the file-based repository causes SMF service svc:/application/pkg/system-repository:default to go into maintenance state.

```
# svcadm clear svc:/application/pkg/system-repository:default
```

9 Enable the publishers that were disabled earlier.

```
# pkg set-publisher --enable <publisher>
```

Note: Perform steps 2 through 9 on each non-global zone.

Verifying software versions

To verify the version of the software, enter the following command:

On Solaris 10:

```
# pkginfo -l  pkgname
```

On Solaris 11:

```
# pkg info pkgname
```

Chapter 5

Uninstalling version 6.0.3

This chapter includes the following topics:

About removing Veritas Storage Foundation and High Availability Solutions 6.0.3

This section describes how to roll back either by using the `uninstallmr` script or manually for Solaris 10.

See See “Rolling back to previous boot environment on Solaris 11” on page 196.

Roll back of version 6.0.3 to the 6.0.1 release is supported for the following products:

- Dynamic Multi-Pathing (DMP)
- Veritas Cluster Server (VCS)
- Storage Foundation and High Availability (SFHA)
- Veritas Storage Foundation Cluster File System High Availability (SFCFSHA)
- Veritas Storage Foundation for Oracle RAC (SF for Oracle RAC)
- Veritas Storage Foundation for Sybase ASE CE (SFSYBASECE)
- Symantec VirtualStore (SVS)

Rolling back to previous boot environment on Solaris 11

On Solaris 11, SFHA solutions 6.0.3 contains only packages so removing 6.0.3 is not supported. Instead if you have already created a boot environment for installing 6.0.3, you can roll back to the previous boot environment available before installing 6.0.3.

To roll back to previous boot environment

1 Activate the boot environment available before installing 6.0.3:

```
# beadm activate bename
```

2 Reboot the node so that new be is active now:

```
# reboot
```

3 You may optionally destroy the boot environment on which 6.0.3 is installed:

```
# beadm destroy bename
```

For example,

```
# beadm destroy sfha_603
```

Rolling back using the uninstallmr script

Use the following procedure to roll back from any Veritas product to the previous version using the `uninstallmr` script.

Note: If any of the systems that you plan to roll back have encapsulated boot disks, you must reboot them after rollback.

To roll back

1 Stop the applications that use CVM or CFS that are not under VCS control.

- Using native application commands, stop the applications that use CVM or CFS on all nodes.
- Verify that no processes use the CFS mount point:

```
# fuser -c mount_point
```

2 Unmount CFS file systems that are not under VCS control.

- Determine the file systems that need to be unmounted by checking the output of mount command.

  ```
  # mount -v | grep vxfs | grep cluster
  ```

- Unmount each file system that is not controlled by VCS on each node:

  ```
  # umount mount_point
  ```

3 Stop VCS to take the service groups on all nodes offline.

On any node execute following command to stop VCS:

```
# hastop -all
```

4 Stop the applications that use VxVM or VxFS that are not under VCS control.

- Using native application commands, stop the applications that use VxVM or VxFS.
- Verify that no processes use the VxFS mount point:

  ```
  # fuser -c mount_point
  ```

5 Unmount VxFS file systems that are not under VCS control.

- Determine the file systems that need to be unmounted by checking the output of mount command.

  ```
  # mount -v | grep vxfs
  ```

- Unmount each file system that is not controlled by VCS on each node:

  ```
  # umount mount_point
  ```

6 Run the `uninstallmr` command from the directory that contains the `installmr` script, type::

```
# ./uninstallmr nodeA nodeB nodeC...
```

7 If you performed a roll back on a system that has an encapsualted boot disk, you must reboot the system. After reboot, you may need to run `hagrp -list Frozen=1` to get the frozen SG list . Then run `hagrp -unfreeze <group> -persistent` to unfreeze all the frozen SGs manually.

Rolling back manually

Use one of the following procedures to roll back to 6.0.1 manually.

- Rolling back Storage Foundation or Storage Foundation and High Availability manually
- Rolling back Storage Foundation Cluster File System High Availability manually
- Rolling back Storage Foundation for Oracle RAC manually
- Rolling back Veritas Cluster Server manually
- Rolling back Symantec VirtualStore manually
- Rolling back Dynamic Multi-Pathing manually

Note: You must reboot systems that you roll back manually at the end of the roll back procedure.

Rolling back Storage Foundation or Storage Foundation and High Availability manually

Use the following procedure to roll back to 6.0.1 manually.

To roll back SF or SFHA

1 Log in as superuser.

2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

4 Check if the root disk is under VxVM control by running this command:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootvol` is listed as being mounted as the root (/) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:

- Use the `vxplex` command to remove all the plexes of the volumes `rootvol`, `swapvol`, `usr`, `var`, `opt` and `home` that are on disks other than the root disk.

  For example, the following command removes the plexes `mirrootvol-01`, and `mirswapvol-01` that are configured on a disk other than the root disk:

  ```
  # vxplex -o rm dis mirrootvol-01  mirswapvol-01
  ```

  Note: Do not remove the plexes on the root disk that correspond to the original disk partitions.

- Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices. There must be at least one other disk in the rootdg disk group in addition to the root disk for vxunroot to succeed.

  ```
  # /etc/vx/bin/vxunroot
  ```

  Following the removal of encapsulation, the system is restarted from the unencapsulated root disk.

5 Enter the following command to check if any VxFS file systems are mounted:

```
# df -F vxfs
```

If any VxFS file systems are present, unmount all of the VxFS file systems that are not under VCS control:

```
# umount /filesystem
```

6 If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the vxrvg stop command to stop each RVG individually:

```
# vxrvg -g diskgroup stop rvg_name
```

- On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

  Note: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

7 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

8 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

9 Stop VCS along with all its resources. Then, stop the remaining resources manually:

```
# svcadm disable -t vcs
```

10 If cluster fencing was originally configured in enabled mode, type the following on all the nodes:

```
# rm /etc/vxfenmode
```

11 Unmount `/dev/odm`:

```
# umount /dev/odm
```

12 Unload the ODM module:

```
# svcadm disable -t odm
# modinfo | grep odm
# modunload -i odm_mod_id
```

13 Unload the cluster fencing (`vxfen`) module:

```
# svcadm disable -t vxfen
# modinfo | grep vxfen
# modunload -i vxfen_mod_id
```

14 Stop GAB and LLT in the following order:

```
# svcadm disable -t gab
# svcadm disable -t llt
```

15 Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

16 Remove the SF 6.0.3 patches.

- Get the list of 6.0.3 patches, type:

  ```
  # ./installmr -listpatches
  ```

- Remove each patch from the patch list. For example:

  ```
  # patchrm 143287-07
  ```

Rolling back Storage Foundation Cluster File System High Availability manually

Use the following procedure to roll back to 6.0.1 manually.

To roll back SFCFSHA manually

1 Log in as superuser.

2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

4 Check if the root disk is under VxVM control by running this command:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootvol` is listed as being mounted as the root (/) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:

- Use the `vxplex` command to remove all the plexes of the volumes `rootvol`, `swapvol`, `usr`, `var`, `opt` and `home` that are on disks other than the root disk.

  For example, the following command removes the plexes `mirrootvol-01`, and `mirswapvol-01` that are configured on a disk other than the root disk:

  ```
  # vxplex -o rm dis mirrootvol-01 \
  mirswapvol-01
  ```

  Note: Do not remove the plexes on the root disk that correspond to the original disk partitions.

- Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices. There must be at least one other disk in the rootdg disk group in addition to the root disk for vxunroot to succeed.

  ```
  # /etc/vx/bin/vxunroot
  ```

  Following the removal of encapsulation, the system is restarted from the unencapsulated root disk.

5 Enter the following command to check if any VxFS file systems are mounted:

```
# df -F vxfs
```

If any VxFS file systems are present, unmount all of the VxFS file systems that are not under VCS control:

```
# umount /filesystem
```

6 If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the vxrvg stop command to stop each RVG individually:

  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

  Note: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

7 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

8 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

9 Stop VCS along with all its resources. Then, stop the remaining resources manually:

```
# svcadm disable -t vcs
```

10 If cluster fencing was originally configured in enabled mode, type the following on all the nodes:

```
# rm /etc/vxfenmode
```

11 Unmount `/dev/odm`:

```
# umount /dev/odm
```

12 Unload the ODM module:

```
# svcadm disable -t odm
# modinfo | grep odm
# modunload -i odm_mod_id
```

13 Unload the cluster fencing (`vxfen`) module:

```
# svcadm disable -t vxfen
# modinfo | grep vxfen
# modunload -i vxfen_mod_id
```

14 Stop GAB and LLT in the following order:

```
# svcadm disable -t gab
# svcadm disable -t llt
```

15 Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

16 Remove the SFCFSHA 6.0.3 patches.

- Get the list of 6.0.3 patches, type:

  ```
  # ./installmr -listpatches
  ```

- Remove each patch from the patch list. For example:

  ```
  # patchrm 143287-07
  ```

Rolling back Storage Foundation for Oracle RAC manually

Use the following procedure to roll back to 6.0.1 manually.

To roll back SF for Oracle RAC manually

1 On each node, take the Oracle resources in the VCS configuration file (main.cf) offline.

```
# hagrp -offline oracle_group -sys node_name
```

If the database is not managed by VCS, stop the Oracle database as follows:

```
$ srvctl stop database -d db_name
```

2 If CRS is not under VCS Control, then enter the following command on each node of the cluster to stop CRS.

- For 10gR2 or 11gR1:

  ```
  # /etc/init.d/init.crs stop
  ```

- For 11gR2:

  ```
  # /etc/init.d/ohasd stop
  ```

3 Stop the applications that use CVM or CFS that are not under VCS control.

- Using native application commands, stop the applications that use CVM or CFS on all nodes.
- Verify that no processes use the CFS mount point:

```
# fuser -c mount_point
```

4 Unmount CFS file systems that are not under VCS control.

- Determine the file systems that need to be unmounted by checking the output of mount command.

  ```
  # mount -v | grep vxfs | grep cluster
  ```

- Unmount each file system that is not controlled by VCS on each node:

  ```
  # umount mount_point
  ```

5 Stop VCS to take the service groups on all nodes offline

On any node execute following command to stop VCS:

```
# hastop -all
```

6 Stopping the applications that use VxVM or VxFS that are not under VCS control

- Using native application commands, stop the applications that use VxVM or VxFS.
- Verify that no processes use the VxFS mount point:

  ```
  # fuser -c mount_point
  ```

7 Unmounting VxFS file systems that are not under VCS control.

- Determine the file systems that need to be unmounted by checking the output of mount command.

```
# mount -v | grep vxfs
```

- Unmount each file system that is not controlled by VCS on each node:

  ```
  # umount mount_point
  ```

8 To stop the process, type:

```
# ./installsfrac -stop <node1> <node2> ... <nodeN>
```

9 Remove the SF for Oracle RAC 6.0.3 patches.

- Get the list of 6.0.3 patches, type:

  ```
  # ./installmr -listpatches
  ```

- Remove each patch from the patch list. For example:

  ```
  # patchrm 143287-07
  ```

10 Verify that the patches have been remove on all the nodes.

11 Reboot the nodes point.

```
# /usr/sbin/shutdown -g0 -y -i6
```

Rolling back Veritas Cluster Server manually

Use the following procedure to roll back VCS 6.0.3 to VCS 6.0.1 on your cluster manually. To uninstall VCS, see the *Veritas Cluster Server Installation Guide*.

Note: Use this procedure only when rolling back VCS. Do not roll back VCS when it is part of other products that rely on VCS, for example Storage Foundation Clustered File System or Storage Foundation for Oracle RAC.

To roll back VCS manually

1 List the service groups in your cluster and their status. On any node, type:

```
# hagrp -state
```

2 Take the ClusterService service group offline if it is running. On any node, type:

```
# hagrp -offline -force ClusterService -sys system
```

3 Make the VCS configuration writable. On any node, type:

```
# haconf -makerw
```

4 Freeze all service groups. On any node, type:

```
# hagrp -freeze service_group -persistent
```

where `service_group` is the name of the service group. Note that the ClusterService group cannot be frozen.

5 Save the configuration (`main.cf`) file with the groups frozen. On any node, type:

```
# haconf -dump -makero
```

6 Make a backup copy of the current `main.cf` and all `types.cf` configuration files. For example, on one node in the cluster, type:

```
#  cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/main.cf.save
# cp /etc/VRTSvcs/conf/config/types.cf \
/etc/VRTSvcs/conf/types.cf.save
```

7 Shut down VCS. On any node, type:

```
# /opt/VRTSvcs/bin/hastop -all -force
```

8 Shut down CmdServer. On each node, type:

```
# /opt/VRTSvcs/bin/CmdServer -stop
```

9 Verify that VCS has shut down. On any node, type:

```
# /sbin/gabconfig -a
```

The output resembles: GAB Port Memberships Port a gen 23dc0001 membership 01. The output shows no membership for port h.

10 For Solaris 10, on nodes that run non-global zones, check if the non-global zones are in the running state. Boot the non-global zones that are not in the running state.

- Check the zone’s state. On each node, type:

  ```
  # zoneadm list -icv
  ```

- Boot the zone if it is not in the running state. On each node, type:

  ```
  # zoneadm -z zone boot
  ```

  where *zone* is the name of the non-global zone.

Note: Do not configure one or more Solaris zones to boot from the shared storage.

11 Unconfigure vxfen if the VCS cluster uses the fencing option. On each node, type:

```
# /sbin/vxfenconfig -U
```

12 Unload vxfen. On each node, perform the following steps:

- Identify the vxfen kernel module, for example:

  ```
  # modinfo|grep vxfen
  ```

- Unload vxfen using the module number.

  ```
  # modunload -i 210
  ```

13 Unconfigure GAB. On each node, type:

```
# /sbin/gabconfig -U
```

14 Unload GAB. On each node, perform the following steps:

- Identify the GAB kernel module. For example:

  ```
  # modinfo | grep gab
  ```

- Unload GAB using the module number:

  ```
  # modunload -i 149
  ```

15 Unconfigure LLT. On each node, perform the following steps:

- Type:

  ```
  # /sbin/lltconfig -U
  ```

- Type **y** on each node in response to the message.

16 Unload LLT. On each node, perform the following steps:

- Identify the LLT kernel module. For example:

  ```
  # modinfo | grep llt
  ```

- Unload LLT using the module number:

  ```
  # modunload -i 147
  ```

17 Remove the VCS 6.0.3 patches. On each node, perform the following steps:

- Get the list of 6.0.3 patches, type:

  ```
  # ./installmr -listpatches
  ```

- Remove each patch from the patch list. For example:

  ```
  # patchrm 143287-07
  ```

18 Verify that the patches have been removed. On each node, type:

```
# showrev -p | grep VRTS
```

19 If the LLT, GAB, or VXFEN modules cannot be stopped or unloaded following the patch removal, reboot all nodes in the cluster.

20 If you do not perform step 19, start the VCS components manually. On each node, type:

```
# /sbin/lltconfig -c
# /sbin/gabconfig -cx
# /sbin/vxfenconfig -c
# /opt/VRTSvcs/bin/hastart
```

You do not have to start vxfen unless you use the fencing option.

21 After VCS has started, perform the following steps:

- Verify all resources have been probed. On any node, type:

  ```
  # hastatus -summary
  ```

- Unfreeze all service groups. On any node, type:

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

where *service_group* is the name of the service group.

22 Bring online the ClusterService service group, if necessary. On any node type:

```
# hagrp -online ClusterService -sys system
```

where *system* is the node name.

Rolling back Symantec VirtualStore manually

Use the following procedure to roll back to 6.0.1 manually.

To roll back SVS manually

1 Log in as superuser.

2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

4 Check if the root disk is under VxVM control by running this command:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootvol` is listed as being mounted as the root (`/`) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:

- Use the `vxplex` command to remove all the plexes of the volumes `rootvol`, `swapvol`, `usr`, `var`, `opt` and `home` that are on disks other than the root disk.

  For example, the following command removes the plexes `mirrootvol-01`, and `mirswapvol-01` that are configured on a disk other than the root disk:

  ```
  # vxplex -o rm dis mirrootvol-01\  mirswapvol-01
  ```

  Note: Do not remove the plexes on the root disk that correspond to the original disk partitions.

- Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices. There must be at least one other disk in the rootdg disk group in addition to the root disk for vxunroot to succeed.

  ```
  # /etc/vx/bin/vxunroot
  ```

  Following the removal of encapsulation, the system is restarted from the unencapsulated root disk.

5. Enter the following command to check if any VxFS file systems are mounted:

   ```
   # df -F vxfs
   ```

   If any VxFS file systems are present, unmount all of the VxFS file systems that are not under VCS control:

   ```
   # umount /filesystem
   ```

6. If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

   - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
   - Use the vxrvg stop command to stop each RVG individually:

     ```
     # vxrvg -g diskgroup stop rvg_name
     ```

   - On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:

     ```
     # vxrlink -g diskgroup status rlink_name
     ```

     Note: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

7. Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

8 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

9 Stop VCS along with all its resources. Then, stop the remaining resources manually:

```
# svcadm disable -t vcs
```

10 If cluster fencing was originally configured in enabled mode, type the following on all the nodes:

```
# rm /etc/vxfenmode
```

11 Unmount `/dev/odm`:

```
# umount /dev/odm
```

12 Unload the ODM module:

```
# svcadm disable -t odm
# modinfo | grep odm
# modunload -i odm_mod_id
```

13 Unload the cluster fencing (`vxfen`) module:

```
# svcadm disable -t vxfen
# modinfo | grep vxfen
# modunload -i vxfen_mod_id
```

14 Stop GAB and LLT in the following order:

```
# svcadm disable -t gab
# svcadm disable -t llt
```

15 Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

16 Remove the SVS 6.0.3 patches.

- Get the list of 6.0.3 patches, type:

  ```
  # ./installmr -listpatches
  ```

- Remove each patch from the patch list. For example:

  ```
  # patchrm 143287-07
  ```

Rolling back Dynamic Multi-Pathing manually

Use the following procedure to roll back to 6.0.1 manually.

To roll back DMP manually

1 Log in as superuser.

2 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

4 Check if the root disk is under VxVM control by running this command:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootvol` is listed as being mounted as the root (`/`) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:

- Use the `vxplex` command to remove all the plexes of the volumes `rootvol`, `swapvol`, `usr`, `var`, `opt` and `home` that are on disks other than the root disk.

  For example, the following command removes the plexes `mirrootvol-01`, and `mirswapvol-01` that are configured on a disk other than the root disk:

```
# vxplex -o rm dis mirrootvol-01 \
mirswapvol-01
```

Note: Do not remove the plexes on the root disk that correspond to the original disk partitions.

- Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices. There must be at least one other disk in the rootdg disk group in addition to the root disk for vxunroot to succeed.

  ```
  # /etc/vx/bin/vxunroot
  ```

  Following the removal of encapsulation, the system is restarted from the unencapsulated root disk.

5 Enter the following command to check if any VxFS file systems are mounted:

```
# df -F vxfs
```

If any VxFS file systems are present, unmount all of the VxFS file systems that are not under VCS control:

```
# umount /filesystem
```

6 If you have created any Veritas Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the vxrvg stop command to stop each RVG individually:

  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

Note: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

7 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

8 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

To verify that no volumes remain open, enter the following command:

```
# vxprint -Aht -e v_open
```

9 Stop VCS along with all its resources. Then, stop the remaining resources manually:

```
# svcadm disable -t vcs
```

10 If cluster fencing was originally configured in enabled mode, type the following on all the nodes:

```
# rm /etc/vxfenmode
```

11 Unmount `/dev/odm`:

```
# umount /dev/odm
```

12 Unload the ODM module:

```
# svcadm disable -t odm
# modinfo | grep odm
# modunload -i odm_mod_id
```

13 Unload the cluster fencing (`vxfen`) module:

```
# svcadm disable -t vxfen
# modinfo | grep vxfen
# modunload -i vxfen_mod_id
```

14 Stop GAB and LLT in the following order:

```
# svcadm disable -t gab
# svcadm disable -t llt
```

15 Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

16 Remove the DMP 6.0.3 patches.

- Get the list of 6.0.3 patches, type:

  ```
  # ./installmr -listpatches
  ```

- Remove each patch from the patch list. For example:

  ```
  # patchrm 143287-07
  ```

Rolling back Veritas Storage Foundation for Sybase CE

You can use the following procedure to roll back SF Sybase CE from 6.0.3 to 6.0.1.

To roll back Veritas Storage Foundation for Sybase CE

1 Log in as the superuser on one of the nodes in the cluster.

2 On each node, take the Sybase resources in the VCS configuration file (`main.cf`) offline.

```
# hagrp -offline Sybase_group -sys node_name
```

For example:

```
# /opt/VRTSvcs/bin/hagrp -offline sybasece -sys sys1

# /opt/VRTSvcs/bin/hagrp -offline sybasece -sys sys2
```

These commands stop the Sybase resources under VCS control.

3 Verify that the state of the Sybase and CVM service groups are offline and online respectively.

```
# /opt/VRTSvcs/bin/hagrp -state
Group Attribute System Value
binmnt State sys1 |ONLINE|
binmnt State sys2 |ONLINE|
cvm State sys1 |ONLINE|
cvm State sys2 |ONLINE|
sybasece State sys1 |OFFLINE|
sybasece State sys2 |OFFLINE|
```

4 Backing up the Sybase database.

If you plan to retain the Sybase database, you must back up the Sybase database. For instructions on backing up the Sybase database, see the Sybase documentation.

5 Stop the applications that use CVM volumes or CFS mount points not controlled by VCS.

To stop the applications that use CVM or CFS (outside of VCS control):

- Stop the applications that use a CFS mount point. The procedure varies for different applications. Use the procedure appropriate for the application.
- Verify that no processes use the CFS mount point:

  ```
  # fuser -c mount_point
  ```

6 Unmount CFS file systems that are not under VCS control on all nodes.

To unmount CFS file systems not under VCS control:

- Determine the file systems that need to be unmounted by checking the output of the mount command. The command lists all the mounted clustered file systems. Consult the main.cf file for identifying the files that are under VCS control.

  ```
  # mount -v | grep vxfs | grep cluster
  ```

- Unmount each file system that is not controlled by VCS:

  ```
  # umount mount_point
  ```

7 Stop VCS to take the service groups on all nodes offline.

```
# hastop -all
```

8 Verify the output of the `gabconfig -a` command to ensure that VCS has been stopped. In this command output, the VCS engine or high availability daemon (HAD) port h is not displayed. This output indicates that VCS has been stopped.

```
# /sbin/gabconfig -a
GAB Port Memberships
===============================================================
Port a gen 5c3d0b membership 01
Port b gen 5c3d10 membership 01
```

9 Stop all applications that use VxVM volumes or VxFS mount points not under VCS control.

To stop the applications that use VxVM or VxFS (outside of VCS control):

- Stop the applications that use a VxFS mount point. The procedure varies for different applications. Use the procedure that is appropriate for your application.
- Verify that no processes use the VxFS mount point:

  ```
  # fuser -c mount_point
  ```

10 Unmount VxFS file systems that are not under VCS control on all nodes.

Note: To avoid issues on rebooting, you must remove all entries of VxFS from the `/etc/vfstab` directory.

To unmount VxFS file systems not under VCS control:

- Determine the file systems that need to be unmounted by checking the output of the mount command. The command lists all the mounted file systems.

  ```
  # mount -v | grep vxfs
  ```

- Unmount each file system that is not under VCS control:

  ```
  # umount mount_point
  ```

11 Remove the SF Sybase CE 6.0.3 packages:

- If you manually uninstall SF Sybase CE 6.0.3 packages:

  ```
  # ./installsfsybasece -stop node1 node2 ... nodeN
  ```

  Get the list , type:

  ```
  # ./installmr -listpatches
  ```

  Remove each patch from the patch list. For example:

  ```
  # patchrm patchnumber
  ```

  Bring up entire stack:

  ```
  # ./installsfsybasece -start  node1 node2 ... nodeN
  ```

- If you use the `uninstallmr` command to uninstall SF Sybase CE 6.0.3 packages:

  ```
  # ./uninstallmr node1 node2 ... nodeN
  ```

12 If you remove the SF Sybase CE packages on a system that has an encapsualted boot disk, you must reboot the system. After reboot, you may need to run hagrp -list Frozen=1 to get the frozen SG list . Then run `hagrp -unfreeze` *`group`*`-persistent` to unfreeze all the frozen SGs manually.

Appendix A

Configuring VCS to manage a Logical Domain using services from multiple I/O domains

This appendix includes the following topics:

Configuring VCS to manage a Logical Domain using services from multiple I/O domains

VCS provides high availability to Logical Domains using I/O services from multiple I/O domains. When I/O services from the control domain and alternate I/O domain fail, VCS fails over the LDom from one system to another system. LDom continues to be functional on the same system and does not need a fail over if one of the I/O domain continues to provide service.

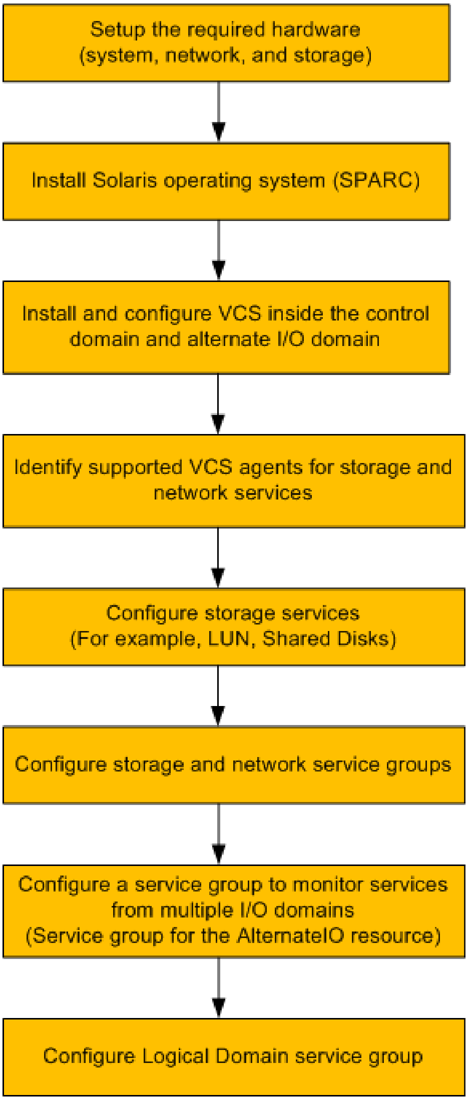
VCS uses service groups and resources to manage the storage and network services that are provided to a Logical Domain. These service groups are monitored by the AlternateIO resource. The AlternateIO service group provides the information about the state of the storage and network services to the LDom agent. VCS fails over the Logical Domain when services from both the I/O domains fail.

Perform the following tasks to configure VCS to manage a Logical Domain:

- Identify supported storage and network services

- Determine the number of nodes to form VCS cluster
- Install and configure VCS inside the control domain and alternate I/O domain
- Configuring storage services
- Configure storage service groups
- Configure network service groups
- Configure a service group to monitor services from multiple I/O domains
- Configure the AlternateIO resource
- Configure the service group for a Logical Domain

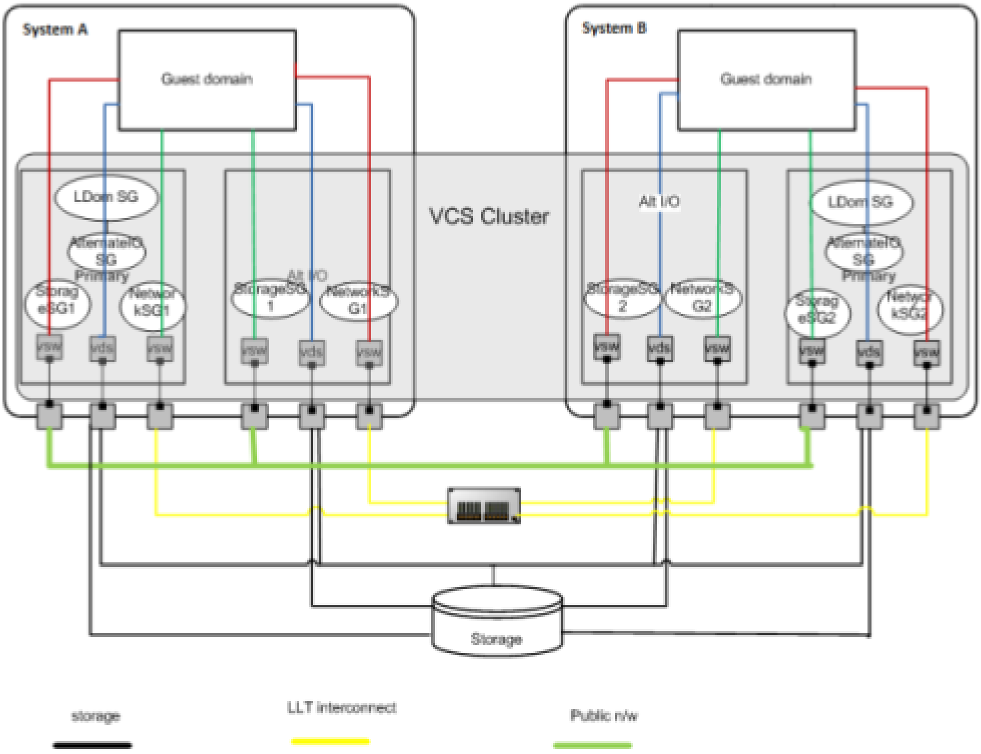
Figure A-1 Workflow to configure VCS on a physical system to manage a Logical Domain


Setup the required hardware
(system, network, and storage)
Install Solaris operating system (SPARC)
Install and configure VCS inside the control domain and alternate I/O domain
Identify supported VCS agents for storage and network services
Configure storage services
(For example, LUN, Shared Disks)
Configure storage and network service groups
Configure a service group to monitor services from multiple I/O domains
(Service group for the AlternateIO resource)
Configure Logical Domain service group

A typical setup for a Logical Domain with multiple I/O services

Guest logical domain using I/O services from multiple I/O domains.

Figure A-2 shows VCS configuration to monitor a logical domain using I/O services from multiple I/O domains



System A, System B - T5440 servers

LDom SG - Logical Domain service group

AlternateIO SG - AlternateIO service group

Storage SG - Storage service group

Network SG - Network service group

Identify supported storage and network services

The following back-end storage and network services can be exported to Logical Domains.

I/O services	Back-end device	VCS agents to be used
Storage	LUN, shared disk	Disk
	Flat file	Mount
	zpool	Zpool
	Veritas CVM volume	CVMVolDG
Network	NIC	NIC

Determine the number of nodes to form VCS cluster

The total number of nodes that form a VCS cluster depends on the number of physical systems times the the control domain and alternate I/O domain on each physical system.

For example, if you have two physical systems, each having a control domain and an alternate I/O domain, you need to configure VCS as a four node cluster.

Install and configure VCS inside the control domain and alternate I/O domain

Install and configure VCS inside the control domain and alternate I/O domain

For more details, refer to the *Veritas™ Cluster Server Installation Guide*.

Configuring storage services

Depending upon the storage service, the configuration procedure differs.

- LUN, Shared Disk, or CVM volume
  See "About virtual disk multipathing for storage services" on page 226.
  See "Configuring virtual disk multipathing for LUN, Shared Disk, or CVM Volume" on page 226.

- ZFS volume
  See "Configuring storage services when back-end device is a ZFS volume" on page 228.

- Flat file
  For more information, refer to the LDom Administrator's guide.

- Zpool
  For more information, refer to the LDom Administrator's guide.

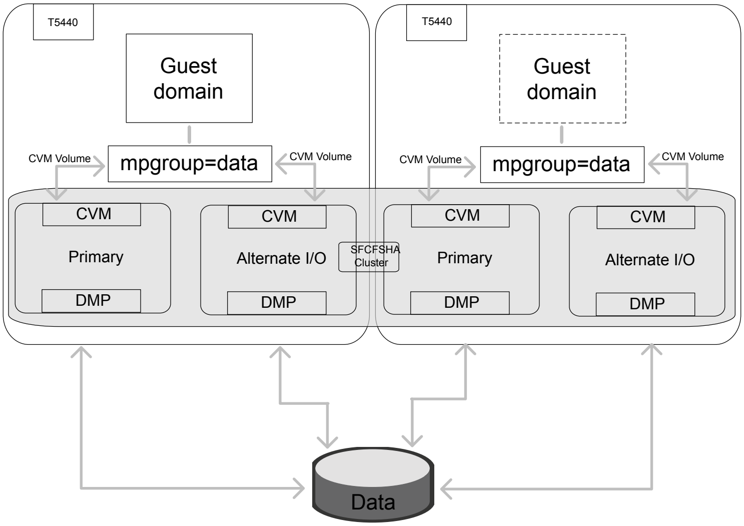
About virtual disk multipathing for storage services

Virtual disk multipathing (`mpgroup`) enables you to configure virtual disk on a guest logical domain to access its back-end storage path through more than one I/O domain. This feature ensures that the virtual disk accessed by the guest logical domain remains accessible as long as services from one of the I/O domain are available.

For example, if you set up a virtual disk multipathing (`mpgroup`) to access a physical disk from a shared storage (SAN) which is connected to more than one I/O domains, when the guest domain accesses that virtual disk, the virtual disk driver goes through one of the I/O domains to access the back-end storage. If the virtual disk driver cannot connect to an I/O domain, then the virtual disk attempts to reach the back-end storage through a different I/O domain.

You must configure virtual disk multipathing (`mpgroup`) only if the storage back-end device exported to the guest domain is a LUN, Shared Disk, or CVM volume.

Figure A-3 shows a sample diagram for mpgroup with CVM Volume



Configuring virtual disk multipathing for LUN, Shared Disk, or CVM Volume

To enable virtual disk multipathing (`mpgroup`), you must export a virtual disk back-end path from each I/O domain and add the virtual disks to a multipathing group (also known as `mpgroup`). The `mpgroup` is identified by a name and is configured when you export the virtual disk back-end path.

To configure virtual disk multipathing

1 Add the physical disk back-end path of the disk service to the primary domain.

```
# ldm add-vdsdev mpgroup=data backend_path1 volume@primary-vds0
```

where *backend_path1* is the path to the virtual disk back-end from the primary domain.

2 Add the physical disk back-end path of the disk service to the alternate I/O domain for disk added in step 1.

```
# ldm add-vdsdev mpgroup=data backend_path2 volume@alternate-vds0
```

where *backend_path2* is the path to the virtual disk back-end from the alternate I/O domain.

3 Export the virtual disk to the guest domain.

```
# ldm add-vdisk disk_name volume@primary-vds0 ldom_name
```

where *disk_name* is the name of the virtual storage device.

where *ldom_name* is the name of the Logical Domain.

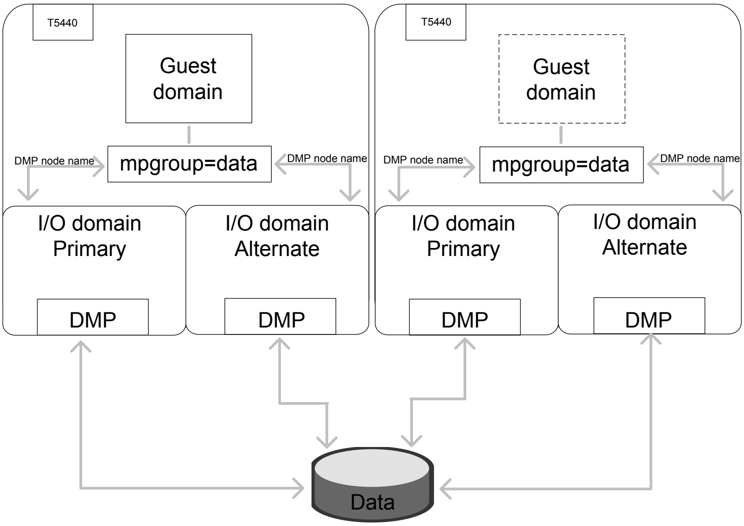
Note: Do not set the value of the **Options** attribute to exclusive; **excl**. If set to exclusive, Logical Domain cannot use the multipathing functionality.

For more details on configuring virtual disk multipathing, refer to the *Oracle VM server for SPARC Administration Guide*.

Virtual disk multi-pathing (mpgroup) configurations with DMP

If the disk exported to guest domain has more than one I/O path from each I/O domain, install Veritas Dynamic Multi-pathing (DMP) in each I/O domain. Use the DMP node name to configure the virtual disk multi-pathing (`mpgroup`) to the disk exported to the guest domain.

Figure A-4 shows how mpgroup and DMP works together



Configuring storage services when back-end device is a ZFS volume

If you export ZFS volume as a back-end storage to Logical Domain, you need to

1. Export ZFS volume created in the control domain.

   You do not need to configure mpgroup.

2. Export ZFS volume created in the alternate I/O domain.

   You do not need to configure mpgroup.

   Note: Ensure the ZFS volume size created in both domains matches.

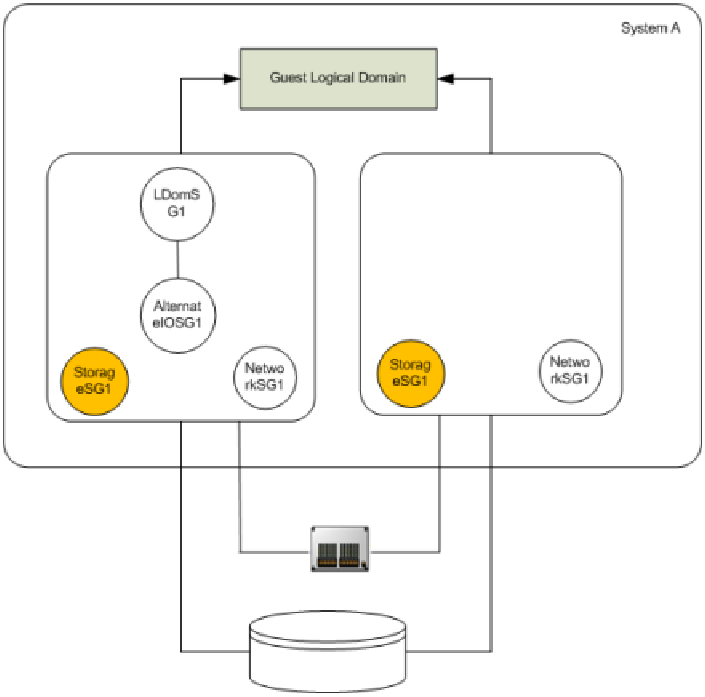
3. Create ZFS root pool mirror inside the Logical Domain from the volumes exported from control domain and alternate I/O domain.

Configure storage service groups

VCS agents manage storage services that are made available to a guest Logical Domain. Depending on the back-end storage device, use the appropriate VCS agent. For more information on supported VCS agents, see Identify supported storage and network services.

Note: You must configure a storage service group on each physical system in the cluster.

Figure A-5 shows storage service groups in the control domain and alternate I/O domain on a physical system



Configuration parameter	Description

Localize resource attribute value	You may need to localize VCS resource attributes depending on the type of back-end storage device.
	For example, for Disk resource, if the back-end storage paths from the control and alternate I/O domains are different, you need to localize the partition attribute.
	`Disk disk1`
	` (`
	`   Partition @primary =`
	`   "/dev/rdsk/c3t50060E8000C46C50d2s2"`
	`   Partition @alternate =`
	`   "/dev/rdsk/c1t50060E8000C46C50d2s2"`
	` )`

Service group type	Service groups that manage storage services in the control domain and alternate I/O domain must be configured as a parallel service group.
Configure the SystemList attribute	Modify the SystemList attribute of the service group to add hostnames of the control domain and alternate I/O domain configured on the physical system.
Configure Phantom resource	If all the resources are of the type Disk, configure a Phantom resource. The Disk resource is of the type OnOnly and does not contribute to determine the state of the service group. The Phantom resource enables VCS to determine the state of parallel service groups that do not include OnOff resources. For more information on the Phantom agent, refer to the Veritas™ Cluster Server Bundled Agents Reference Guide.

An example of storage service group configuration from main.cf configuration (for a setup that has two physical systems)

Control domain host names – primary1, primary2

Alternate domain host names – alternate1, alternate2

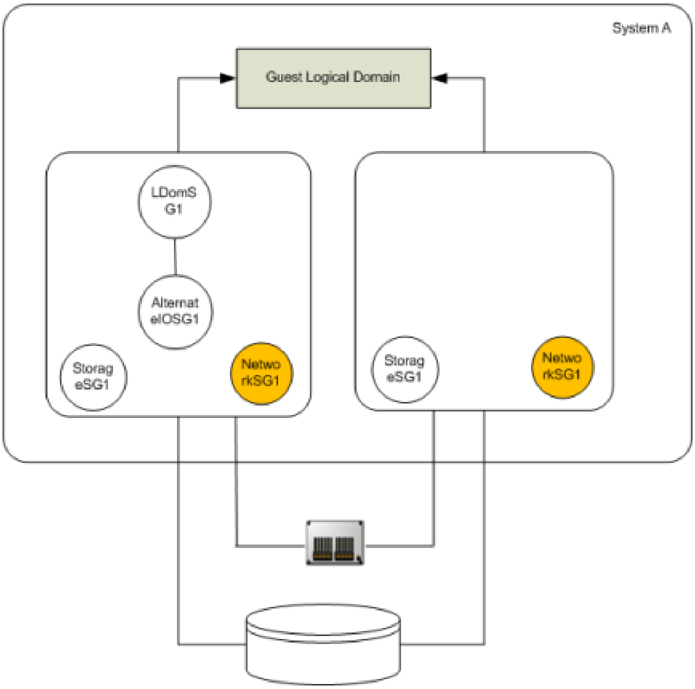
```
group primary1-strsg (
        SystemList = { primary1 = 0, alternate1 = 1 }
        AutoStartList = { primary1, alternate1 }
        Parallel = 1
        )

        Disk disk1
        (
        Partition @primary1 = "/dev/rdsk/c3t50060E8000C46C50d2s2"
        Partition @alternate1 = "/dev/rdsk/c1t50060E8000C46C50d2s2"
        )

        Phantom ph1 (
                )
group primary2-strsg (
        SystemList = { primary2 = 0, alternate2 = 1 }
        AutoStartList = { primary2, alternate2 }
        Parallel = 1
        )

        Disk disk2
        (
        Partition @primary2 = "/dev/rdsk/c3t50060E8000C46C50d2s2"
        Partition @alternate2 = "/dev/rdsk/c1t50060E8000C46C50d2s2"
        )

        Phantom ph2 (
                )
```

Configure network service groups

VCS agents manage network resources that are made available to a guest Logical Domain. Depending on the back-end storage device, use appropriate VCS agent. For more information, see Identify supported storage and network services.

Note: You must configure a network service group on each physical system in the cluster.

Figure A-6 shows network service groups in the control domain and alternate I/O domain



Perform the configuration steps for the network service group on each physical system.

Configuration parameter	Description
Localize network resource attribute	You may need to localize VCS resources depending on the back-end network device. For example, for disk agent, if the network device exported from control and alternate I/O domain are different, you need to localize the Device attribute.

```
NIC primary1-network
      (
          Device @primary = nxge3
          Device @alternate = nxge4
      )
```

Configuration parameter	Description
Service group type	Service groups that manage network services in the control domain and alternate I/O domain must be configured as a parallel service group.
Configure the SystemList attribute	Modify the SystemList attribute in the service group to add host names of the control domain and alternate I/O domain configured on the physical system.
Configure Phantom resource	If all the resources are of the type NIC, configure a Phantom resource. The NIC resource is of the type OnOnly and does not contribute to determine the state of the service group. The Phantom resource enables VCS to determine the state of parallel service groups that do not include OnOff resources. For more information on the Phantom agent, refer to the Veritas™ Cluster Server Bundled Agents Reference Guide.

An example of network service group configuration from main.cf (for a setup that has two physical systems)

Control domain host names – primary1, primary2

Alternate domain host names – alternate1, alternate2

```
group primary1-nwsg (
        SystemList = { primary1 = 0, alternate1 = 1 }
        AutoStartList = { primary1, alternate1 }
        Parallel = 1
        )

        NIC nicres1 (
                Device @primary1 = nxge3
                Device @alternate1 = nxge1
                )

        Phantom ph3 (
                )
group primary2-nwsg (
        SystemList = { primary2= 0, alternate2 = 1 }
        AutoStartList = { primary2, alternate2 }
        Parallel = 1
        )
```

```
NIC  nicres2(
     Device @primary2= nxge3
     Device @alternate2 = nxge1
     )

Phantom ph4 (
     )
```

Configure a service group to monitor services from multiple I/O domains

Configure a service group for the AlternateIO resource to monitor storage and network services that are exported from back-end devices to a Logical Domain.

Configuration notes for the service group:

- Configure the service group as a parallel or a failover service group. See, Type of service group configuration for the AlternateIO resource.
- If multiple storage services are exported to a Logical Domain, you can configure separate service groups to monitor each of the storage services. For example, you can configure separate service groups to monitor LUN and ZFS volume storage services.
- The SystemList attribute of the service group must contain only host names of the control domains present on each physical system in the cluster.
- Localize the StorageSG attribute of the service group with the list of the storage service groups configured for each node.
- Enable preonline trigger for a fail over type service group

  ```
  # hagrp -modify aiosg TriggerPath bin/AlternateIO
  ```

  where aiosg is the name of the service group

  ```
  # hagrp -modify aiosg TriggersEnabled PREONLINE
  ```

Type of service group configuration for the AlternateIO resource

Service group type	Condition

Parallel

If storage services are simultaneously accessible to all nodes in the cluster, the service group of the AlternateIO resource must be configured as a parallel service group.

For example, shared LUNs, shared Disks, CVM Volume.

Fail over

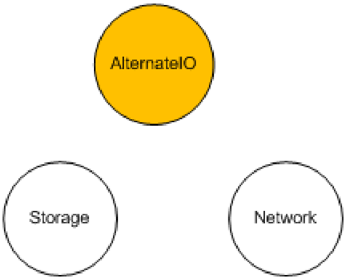
If storage services must be accessible only on one physical system (control domain and alternate I/O domain) in the cluster, configure the service group of the AlternateIO resource as a failover service group.

For example, zpool.

Configure the AlternateIO resource

The AlternateIO resource monitors storage and network services that are exported to a guest Logical Domain. The AlternateIO resource is not dependent on storage or network resources. However, its state depends upon the state of storage or network service groups.

Figure A-7 shows that the AlternateIO resource does not have any dependency on storage or network resources.



Configuration parameter | **Description**

StorageSG attribute

This attribute is a key value pair. A storage service group is the key and the value of the key can either be 0 or 1.

Set the value of the key to 1 to bring the service group online when the AlternateIo resource comes online and to take the service group offline when the AlternateIo resource goes offline.

Localize the StorageSG attribute of the AlternateIO resource with the list of storage service groups that are configured on each node.

```
AlternateIO altiores1
 (
 StorageSG @primary1 = { primary1-strsg1 = 1 }
 StorageSG @primary2 = { primary2-strsg1 = 1 }
  )
```

NetworkSG attribute

This attribute is a key value pair. A network service group is the key and the value of the key can either be 0 or 1.

Set the value of the key to 1 to bring the service group online when the AlternateIo resource comes online and to take the service group offline when the AlternateIo resource goes offline.

Localize the NetworkSG attribute of the AlternateIO resource with the list of network service groups that are configured on each node.

```
AlternateIO altiores1
 (
 NetworkSG @primary1 = { primary1-nwsg = 0 }
 NetworkSG @primary2 = { primary2-nwsg = 0 }
 )
```

Configuration parameter	Description
Preonline trigger	For any of the service groups configured in the StorageSG or NetworkSG attributes, if you set the value to 1, configure the preonline trigger at the service group level. Configuring the preonline trigger ensures that service groups listed in the StorageSG attributes are offline on all systems except onto the system where failover or a manual switch over is initiated. For information on enabling the preonline trigger, see Configure service group to monitor services from multiple I/O domains.

Sample service group configuration for the AlternateIO resource

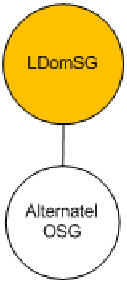
Assumption – Storage and network service groups are of the type parallel.

```
group aiosg (
        SystemList = { primary1 = 0, primary2 = 1 }
        AutoStartList = { primary1, primary2 }
        Parallel = 1
         )

        AlternateIO aiores1 (
         StorageSG @primary1 = { primary1-strsg = 0 }
         StorageSG @primary2 = { primary2-strsg = 0 }
         NetworkSG @primary1 = { primary1-nwsg = 0 }
         NetworkSG @primary2 = { primary2-nwsg = 0 }
          )
```

Configure the service group for a Logical Domain

VCS uses the LDom agent to manage a guest logical domain. The Logical Domain resource has an online local hard dependency on the AlternateIO resource.

Figure A-8 shows the dependency of LDom service group on the AlternateIO service group.



Configuration notes:

- Configure the service group as a fail over type service group.
- The SystemList attribute in the LDom service group must contain only host names of the control domains from each physical system in the cluster.
- The LDom service group must have online local hard dependency with the AlternateIO service group.

If the guest domain needs to be made available even when the primary domain is rebooted or shut down for planned maintenance.

To make the guest domain available

1 Set the LDom resource attribute DomainFailurePolicy to { primary=ignore, alternate1=stop } for all the LDom resources in the cluster which are critical and needs to be available during primary/control domain maintenance. This setting ensure that guest domain will not be brought down when primary/control domain is taken down for planned maintenance.

```
# hares -modify DomainFailurePolicy ldmres primary ignore \
alternate1 stop
```

2 Set the LDom service group attribute SysDownPolicy to AutoDisableNoOffline This setting ensures that VCS will not fail-over the service group even when the primary/control domain where the service group is online is taken down.

```
# hagrp -modify ldmsg SysDownPolicy AutoDisableNoOffline
```

3 The service group will be auto-disabled in the cluster when the control domain is taken down for maintenance. Once the control domain is brought online again, clear the auto disabled system by executing the following command:

```
# hagrp -autoenable ldmsg -sys primary1
```

4 Once the maintenance for the control domain is completed, set the DomainFailurePolicy attribute to it’s original values (default: {primary = stop}). Also reset the service group attribute SysDownPolicy:

```
# hares -modify ldmres DomainFailurePolicy primary stop
# hagrp -modify ldmsg SysDownPolicy -delete AutoDisableNoOffline
```

Sample configuration for LDom service group

The LDom service group must have online local hard dependency with the AlternateIO service group.

```
group ldmsg (
        SystemList = { primary1 = 0, primary2 = 1 }
        AutoStartList = { primary1, primary2 }
        SysDownPolicy = { AutoDisableNoOffline }
        )

        LDom ldmres (
                LDomName = ldg1
                DominFailurePolicy={ primary=ignore, alternate1="stop"}
                )
```

Failover scenarios

Scenario	Control domain	Alternate I/O domain	VCS behavior
State of each storage service group	Online	Online	No fail over
	Offline/FAULT	Online	No fail over
	Online	Offline/FAULT	No fail over
	Offline/FAULT	Offline/FAULT	Fail over

Scenario	Control domain	Alternate I/O domain	VCS behavior
State of each network service group	Online	Online	No fail over
	Offline/FAULT	Online	No fail over
	Online	Offline/FAULT	No fail over
	Offline/FAULT	Offline/FAULT	Fail over
Domain state	Up	Up	No fail over
	Up	down	No fail over
	Down	Up	Fail over *
	Down	down	Fail over **

* VCS behavior would be “No fail over” with service group in auto-disabled state if the LDom resource attribute DomainFailurePolicy for the control domain is set to “ignore” and the LDom service group attribute SysDownPolicy is set to “AutoDisableNoOffline”.

** VCS behavior would be “No fail over” with service group in auto-disabled state if the LDom resource attribute DomainFailurePolicy for the control and other I/O domain is set to “ignore” and the LDom service group attribute SysDownPolicy is set to “AutoDisableNoOffline”

Recommendations while configuring VCS and Oracle VM Server for SPARC with multiple I/O domains

- Online and offline operations for service groups in the StorageSG attribute
  To manually bring online or take offline service groups that are configured in the StorageSG attribute do not use the AlternateIO resource or its service group
  Instead, use service groups configured in the StorageSG attribute.
- Freeze the service group for the AlternateIO resource
  Freeze the AlternateIO service group before you bring online or take offline service groups configured in the StorageSG attribute of the AlternateIO resource. If you do not freeze the service group, the behavior of the Logical Domain is unknown as it is dependent on the AlternateIO service group.
- Configuring preonline trigger for storage service groups
  You must configure preonline trigger in the following scenario:

When the service groups configured in the StorageSG attribute of the AlternateIO resource are of fail over type, and if you accidentally bring storage service groups online on another physical system in the cluster.

It is possible to bring the storage service groups online on another physical system because resources configured to monitor back-end storage services are present in different service groups on each physical system. Thus, VCS cannot prevent resources coming online on multiple systems. This may cause data corruption.

Note: Perform this procedure for storage service groups on each node.

To configure preonline trigger for each service group listed in the StorageSG attribute

- Run the following commands:

  ```
  # hagrp -modify stg-sg TriggerPath bin/AlternateIO/StorageSG
  # hagrp -modify stg-sg TriggersEnabled PREONLINE
  ```

  where *stg-sg* is the name of the storage service group

- Set connection time out period for virtual disks

  When a disk device is not available, I/O services from the guest domain to the virtual disks are blocked.

  Symantec recommends to set a connection time out period for each virtual disk so that applications times out after the set period instead of waiting indefinitely. Run the following command:

  ```
  # ldm add-vdisk timeout=seconds disk_name \
  volume_name@service_name ldom
  ```

- Fail over of LDom service group when all the I/O domains are down. When the attribute SysDownPolicy is set to AutoDisableNoOffline for a service group, the service group state would be changed to OFFLINE|AutoDisabled when the system on which the service group online goes down. Before auto-enabling the service group and online the service group on any other nodes, it is mandatory to ensure that guest domain is stopped on the system (control domain) that is down. This is particularly important when failure-policy of the master-domains is set to ignore.

Consider the following scenario: The DomainFailurePolicy of the LDom resource is set to {primary=”stop”} by default.

If the guest domain need to be made available even when primary domain is rebooted or shut down for maintenance.

- The DomainFailurePolicy attribute would be changed to {primary=ignore, alternate1=stop} or {primary=ignore, alternate1=ignore}.

  Guest domain will not be stopped even when primary domain is rebooted or shutdown
- The SysDownPolicy attribute would be set to AutoDisableNoOffline for planned maintenance. VCS will not fail-over the service group when the node is down instead the group would be put in to auto-disabled state.

The guest domain can continue to function normally with the I/O services available through alternate I/O domain when the control domain is taken down for maintenance.

When the control domain is under maintenance, and if the alternate I/O domain fails due one of the following:

- DomainFailurePolicy attribute is set to {primary=ignore, alternate1=stop} and only the I/O services from alternate I/O domain are unavailable (i/o domain is active, but n/w or storage loss).
- DomainFailurePolicy attribute is set to {primary=ignore, alternate1=ignore} and if the alternate I/O domain is down (domain is in-active).

In this situation guest domain will not be functioning normally and it is not possible to bring down the guest domain as there is no way to access the guest domain. In such scenarios, you must perform the following steps to online the LDom service group on any other available nodes.

To online the LDom service group

1. If the primary domain can be brought up, then bring up the primary domain and stop the guest domain:

   ```
   # ldm stop ldom_name
   ```

   If this is not possible, power off the physical system from the console so that the guest domain stops.

2. Auto enable the service group:

   ```
   # hagrp -autoenable group -sys system
   ```

3. Online the LDom service group:

   ```
   # hagrp -online group -any
   ```

Sample VCS configuration for AlternateIO resource configured as a fail over type

```
include "types.cf"
cluster altio-cluster (
 UserNames = { admin = XXXXXXXXXXX }
 Administrators = { admin }
 HacliUserLevel = COMMANDROOT
 )

system primary1 (
 )

system alternate1 (
 )

system primary2 (
 )

system alternate2 (
 )

group aiosg (
 SystemList = { primary1 = 0, primary2 = 1 }
 AutoStartList = { primary1 }
 TriggerPath = "bin/AlternateIO"
 TriggersEnabled @primary1 = { PREONLINE }
 TriggersEnabled @primary2 = { PREONLINE }
 )

 AlternateIO altiores (
  StorageSG @primary1 = { primary1-strsg = 1 }
  StorageSG @primary2 = { primary2-strsg  = 1 }
  NetworkSG @primary1 = { primary1-nwsg = 0 }
  NetworkSG @primary2 = { primary2-nwsg  = 0 }
  )



 // resource dependency tree
 //
 // group aiosg
 // {
```

```
 // AlternateIO altiores
 // }


group ldomsg (
 SystemList = { primary1 = 0, primary2 = 1 }
 AutoStartList = { primary1 }
 SysDownPolicy = { AutoDisableNoOffline }
 )

 LDom ldmguest (
  LDomName = ldg1
  )

 requires group aiosg online local hard


 // resource dependency tree
 //
 // group ldomsg
 // {
 // LDom ldg1
 // }


group primary1-strsg (
  SystemList = { primary1 = 0, alternate1 = 1  }
        AutoStart = 0
        Parallel = 1
        TriggerPath = "bin/AlternateIO/StorageSG"
        TriggersEnabled @primary1 = { PREONLINE }
        TriggersEnabled @alternate1 = { PREONLINE }
        AutoStartList = { primary1, alternate1 }
        )

        Zpool zpres1 (
                PoolName @primary1= zfsprim
                PoolName @alternate1 = zfsmirr
                ForceOpt = 0
                )
        // resource dependency tree
        //
        //      group primary1-strsg
        //      {
        //      Zpool zpres1
        //      }



group primary1-nwsg (
 SystemList = { primary1 = 0, alternate1 = 1 }
 Parallel = 1
 )

 Phantom ph1 (
  )

 NIC nicres1 (
                Device @primary1 = nxge3
                Device @alternate1 = nxge4
                )



 // resource dependency tree
 //
 // group primary1-nwsg
 // {
 // Phantom ph1
 // Proxy nicres1
 // }


group primary2-strsg (
  SystemList = { primary2 = 0, alternate2 = 1  }
        Parallel = 1
        TriggerPath = "bin/AlternateIO/StorageSG"
        TriggersEnabled @primary2 = { PREONLINE }
        TriggersEnabled @alternate2 = { PREONLINE }
        )

        Zpool zpres2 (
                PoolName @ primary2  = zfsprim
                PoolName @ alternate2 = zfsmirr
                ForceOpt = 0
                )



   // resource dependency tree
   //
   //      group primary2-strsg
   //      {
   //      Zpool zpres2
   //      }


group primary2-nwsg (
 SystemList = { primary2 = 0, alternate2 = 1 }
 Parallel = 1
 )

 Phantom ph2 (
  )

 NIC nicres2 (
                Device @primary2 = nxge3
                Device @alternate2 = nxge4
                )



 // resource dependency tree
 //
 // group primary2-nwsg
 // {
 // Phantom ph2
 // Proxy nicres2
 // }
```