Symantec™ Storage Foundation and High Availability Solutions 6.1.1 Installation Guide - Solaris

6.1.1 Maintenance Release

August 2015

Symantec

Symantec Storage Foundation and High Availability Installation Guide

Product version: 6.1.1

Document version: 6.1.1 Rev 4

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

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

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

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

Contents

Chapter 1

About Symantec Storage Foundation and High Availability Solutions

This chapter includes the following topics:

About Symantec™ Storage Foundation and High Availability Solutions 6.1.1

Symantec™ Storage Foundation and High Availability Solutions 6.1.1 provides patch updates for the following products:

- Symantec Dynamic Multi-Pathing (DMP)
- Veritas Volume Manager (VxVM)
- Veritas File System (VxFS)
- Symantec Storage Foundation (SF)
- Symantec Cluster Server (VCS)
- Symantec Storage Foundation and High Availability (SFHA)
- Symantec Storage Foundation Cluster File System and High Availability (SFCFSHA)
- Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)
- Symantec Storage Foundation for Sybase ASE CE (SFSYBASECE)

- Symantec ApplicationHA (ApplicationHA)

You can install or upgrade to the patches included in this release by using the `installmr` script. For information on the various options that you can use with the script:

The release supports the following installation and upgrade scenarios:

Table 1-1 Supported installation and upgrade scenarios

Scenario	Install and upgrade process
No product is installed on the target system	Run `installmr` with `-base_path` option to install 6.1.1
The product version before 6.1 is installed on the target system	Run `installmr` with `-base_path` option to upgrade to 6.1.1
The product version 6.1 is installed on the target system	Run `installmr` to upgrade to 6.1.1

To install or upgrade the product to 6.1.1 from releases before 6.1, invoke the `installmr` script with `-base_path` option to install or upgrade 6.1.1.

For installation:

```
./installmr -base_path /tmp/sfha6.1/
```

For upgrade:

```
./installmr -base_path /tmp/sfha6.1/ -upgrade
```

For more information regarding installing 6.1.1 using Install Bundles feature:

See *Using Install Bundles to simultaneously install or upgrade base releases, maintenance patches, and hot fixes* in 6.1 Installation Guides.

Symantec strongly recommends you to use the Install Bundles feature to install or upgrade Symantec Storage Foundation and High Availability Solutions 6.1.1.

Supported operating systems and database software

For information on supported operating systems and database software, see the *Symantec™ Storage Foundation and High Availability Solutions 6.1.1 Release Notes - Solaris*.

Chapter 2

Installing the products for the first time

This chapter includes the following topics:

Supported types of Installation

SFHA Solutions 6.1.1 supports the following types of Installation:

- Installing Symantec products with the script-based installer

  Note: Symantec recommends you to install 6.1.1 with Install Bundles.

- Installing Symantec products with the web-based installer.

Creating a new boot environment on Solaris 11

Before installing SFHA Solutions 6.1.1 on a Solaris 11 host, you can optionally create a backup of the existing active boot environment (BE) and install SFHA Solutions 6.1.1 on the present boot environment. This will help to rollback to the previous state of the operating system in the future if required.

To create a new boot environment as a backup

1 Identify the active boot environment (BE) by looking at the NR tag:

```
# beadm list
```

2 Create the BE:

```
# beadm create bename
```

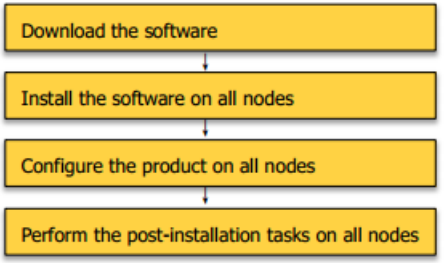
For example,

```
# beadm create pre_sfha_6.1.1
```

Installing the Symantec software using the Install Bundles feature

This section describes how to install a Symantec Storage Foundation and High Availability Solutions product using the Install Bundles feature in one step.

Figure 2-1 Install flow of SFHA Solutions



To install the Symantec software 6.1.1 using Install Bundles:

1 Download Storage Foundation and High Availability Solutions 6.1 from http://fileConnect.symantec.com.

2 Extract the tar ball into the `/tmp/sfha6.1/` directory.

3 Download SFHA Solutions 6.1.1 from https://sort.symantec.com/patches.

4 Extract it to the `/tmp/sfha6.1.1` directory.

5 Change to the `/tmp/sfha6.1.1` directory by entering:

```
# cd /tmp/sfha6.1.1
```

6 Invoke the `installmr` script with `-base_path` option to install 6.1 and 6.1.1. Enter:

```
./installmr -base_path /tmp/sfha6.1/
```

7 In the Task Menu, enter **i** to install a product.

See the 6.1 Installation Guide for configuration steps.

Installing the Symantec software using the script-based installer

This section describes how to install a 6.1.1 Symantec Storage Foundation and High Availability Solutions product for the first time on a host. Download the latest patches for the installer before you install or upgrade the product.

See "Installing the Symantec software for the first time" on page 15.

See the 6.1 *Installation Guide* and *Release Notes* for your product for more information.

Installing the Symantec software for the first time

1 Download Storage Foundation and High Availability Solutions 6.1 from http://fileConnect.symantec.com.

2 Extract the tar ball into a directory called `/tmp/sfha6.1`.

3 Check https://sort.symantec.com/patches to see if there are any patches available for the 6.1 Installer. Download applicable P-patches and extract them to the `/tmp` directory.

4 Change to the `/tmp/sfha6.1` directory:

```
# cd /tmp/sfha6.1
```

5 Run the installer to install SFHA Solutions 6.1.

See the *Installation Guide* for instructions on installing the 6.1 version of this product.

```
#./installer -require complete_path_to_61_installer_patch
```

Note: If the P-patch is not available for 6.1 installer, use the `installer` script without `-require` option.

---

6 Download SFHA Solutions 6.1.1 from https://sort.symantec.com/patches.

7 Extract it to a directory called `/tmp/sfha6.1.1`.

8 Check https://sort.symantec.com/patches to see if there are patches available for the 6.1.1 installer. Download applicable P-patches and extract them to the `/tmp` directory.

9 Change to the `/tmp/sfha6.1.1` directory:

```
# cd /tmp/sfha6.1.1
```

10 Invoke the `installmr` script to install 6.1.1:

```
# ./installmr -require complete_path_to_611_installer_patch
```

Note: If the P-patch is not available for 6.1.1 installer, use the `installmr` script without `-require` option.

11 If you did not configure the product after the 6.1 installation, the installer prompts you to configure the product during MR 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 `/opt/VRTS/install` directory with the `-configure` option.

For configuration procedures, refer to *6.1 Installation Guide* for your product.

Installing the Symantec software using the Web-based installer

This section describes how to install a Symantec Storage Foundation and High Availability Solutions product for the first time on a host and then to install 6.1.1 using the Web-based installer. For detailed instructions on how to install 6.1 using the Web-based installer, follow the procedures in the 6.1 Installation Guide and Release Notes for your products.

See Upgrading to 6.1.1 from 6.1 for upgrade procedures.

You need to configure SF Oralce RAC before you upgrade it from 6.1 to 6.1.1. For more information, refer to Software Limitations in 6.1.1 *Release Notes*.

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 6.1.1 with the Veritas Web-based installer

This section describes installing SFHA with the Veritas Web-based installer.

To install SFHA

1. The 6.1 version of the Symantec product must be installed before upgrading to 6.1.1.
2. On the **Select a task and a product** page, select **Install 6.1.1** 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 **Next**.

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 communication type and provide the root passwords for each system.

5 After the validation completes successfully, click **Next** to install 6.1.1 patches on the selected system.

6 For Storage Foundation, click **Next** to complete the patch installation.

For Storage Foundation High Availability, if the product is not yet configured, the installer prompts you to configure the cluster.

If you select **n**, you can exit the installer. You must configure the product before you can use Storage Foundation High Availability.

For configuration procedures, refer to *6.1 Installation Guide* for your product.

After the installation completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.

7 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**.

Chapter 3

Installing SFHA Solutions using operating system-specific methods

This chapter includes the following topics:

Installing SFHA Solutions using JumpStart

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 20.
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 24.

6 On each client node, run the following command to install the Symantec product packages and patches:

For Solaris SPARC:

```
Ok> boot net -  install
```

7 Click **Upload finish.sh**, then continue with the operating systsem installation.

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.

---

8 After the reboot, run the `installprod` command from the `/opt/VRTS/install` directory to configure the Symantec software.

```
# /opt/VRTS/install/installprod61 -configure
```

where *`installprod61`* is the product's installation command.

Generating the finish scripts

Perform these steps to generate the finish script to install SFHA.

To generate the finish script

1 Download the SFHA Solutions 6.1.1 patch from SORT 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 Symantec products, and encapsulation scripts are generated in the directory you specified in step 1. Output resembles:

```
The finish scripts for DMP is generated at
/js_scripts/jumpstart_dmp.fin
The finish scripts for FS is generated at
/js_scripts/jumpstart_fs.fin
The finish scripts for SF is generated at
/js_scripts/jumpstart_sf.fin
The finish scripts for SFCFSHA is generated at
/js_scripts/jumpstart_sfcfsha.fin
The finish scripts for SFHA is generated at
/js_scripts/jumpstart_sfha.fin
The finish scripts for SF Oracle RAC is generated at
/js_scripts/jumpstart_sfrac.fin
The finish scripts for SFSYBASECE is generated at
/js_scripts/jumpstart_sfsybasece.fin
The finish scripts for SVS is generated at
/js_scripts/jumpstart_svs.fin
The finish scripts for VCS is generated at
/js_scripts/jumpstart_vcs.fin
The finish scripts for VM is generated at
/js_scripts/jumpstart_vm.fin
The encapsulation boot disk script for VM is generated at
/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 SFCFSHA:

```
encap_bootdisk_vm.fin jumpstart_sfcfs.fin
```

For SF Oracle RAC:

```
jumpstart_sfrac.fin
```

For VCS:

```
encap_bootdisk_vm.fin jumpstart_vcs.fin
```

For DMP:

```
encap_bootdisk_vm.fin jumpstart_dmp.fin
```

For SFSYBASECE:

```
jumpstart_sfsybasece.fin
```

For SVS:

```
encap_bootdisk_vm.fin jumpstart_svs.fin
```

For FS:

```
encap_bootdisk_vm.fin jumpstart_fs.fin
```

For VM:

```
encap_bootdisk_vm.fin jumpstart_vm.fin
```

7 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"
```

8
- 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
```

9 Once the installation is complete, refer to installation and configuration guide for the respective product from 6.1 to proceed with the configuration.

Preparing installation resources

Prepare resources for the JumpStart installation.

To prepare the resources

1 Copy the contents of SFHA Solutions6.1 to buildsrc:

```
# cd /tmp/sfha6.1
# cp -r pkgs BUILDSRC
```

Note: The VRTSaslapm package of 6.1 should be replaced with the 6.1.1 VRTSaslspm package.

2 Copy the contents of 6.1.1 patch to buildsrc:

```
# cd /tmp/sfha6.1.1
# cp -r patches BUILDSRC
```

Note: After you copied the patches, you must uncompress them using the gunzip and tar commands.

3 Generate the response file for the package list that you found when you generated the finish script.

See "Generating the finish scripts" on page 20.

To view the patches, packages and operating systems for your Symantec product use the `installmr -listpatches` command, type:

```
# ./installmr -listpatches
```

```
# cd BUILDSRC/pkgs/
# pkgask -r package_name.response -d /BUILDSRC/pkgs/packages_name.pkg
```

4 Create the adminfile file named admin 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
```

5 If you want to encapsulate the root disk automatically when perform the JumpStart installation, copy the scripts `encap_bootdisk_vm61.fin` created when you generated the finish script to *ENCAPSRC*.

See 3 on page 25.

Adding language pack information to the finish file

For the language pack, copy the language packages from the SFHA Solutions 6.1 to the shared storage.

```
# cd /tmp/sfha6.1/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 VRTSspt . . .
```

```
do
...
done
```

Installing SFHA Solutions on Solaris 11 using Automated Installer

You can use the Oracle Solaris Automated Installer (AI) to install the Solaris 11 operating system and Storage Foundation product on multiple client systems in a network. AI performs a hands-free installation (automated installation without manual interactions) of SPARC systems. You can also use AI media to install the Oracle Solaris OS on a single SPARC platform. Oracle provides the AI bootable image and it can be downloaded from the Oracle website. All cases require access to a package repository on the network to complete the installation.

Using Automated Installer

To use Automated Installer to install systems over the network, set up DHCP and set up an AI service on an AI server. The DHCP server and AI server can be the same system or two different systems.

Make sure that the systems can access an Oracle Solaris Image Packaging System (IPS) package repository. The IPS package repository can reside on the AI server, on another server on the local network, or on the Internet.

An AI service is associated with an AI install image and one or more sets of installation instructions. The installation instructions specify one or more IPS package repositories from where the system retrieves the packages that are needed to complete the installation. The installation instructions also include the names of additional packages to install and information such as target device and partition information. You can also specify instructions for post-installation configuration of the system.

Consider the operating systems and packages you want to install on the systems. Depending on your configuration and needs, you may want to do one of the following:

- If two systems have different architectures or need to be installed with different versions of the Oracle Solaris OS, create two AI services. Then, associate each AI service with a different AI image
- If two systems need to be installed with the same version of the Oracle Solaris OS but need to be installed differently in other ways, create two sets of installation instructions for the AI service. The different installation instructions can specify different packages to install or a different slice as the install target.

The installation begins when you boot the system. DHCP directs the system to the AI install server, and the system accesses the install service and the installation instructions within that service.

For more information, see the *Oracle® Solaris 11 Express Automated Installer Guide*.

Using AI to install the Solaris 11 operating system and SFHA Solutions products

Use the following procedure to install the Solaris 11 operating system and SFHA Solutions products using AI.

To use AI to install the Solaris 11 operating system and SFHA Solutions products

1. Follow the Oracle documentation to set up a Solaris AI server and DHCP server.

   You can find the documentation at http://docs.oracle.com.

2. Set up the Symantec package repository by running the following commands to startup necessary SMF services and create directories:

   ```
   # svcadm enable svc:/network/dns/multicast:default
   # mkdir /ai
   # zfs create -o compression=on -o mountpoint=/ai rpool/ai
   ```

3. Run the following commands to set up IPS repository for Symantec SPARC packages:

   ```
   # mkdir -p /ai/repo_symc_sparc
   # pkgrepo create /ai/repo_symc_sparc
   # pkgrepo add-publisher -s /ai/repo_symc_sparc Symantec
   ```

   - For 6.1:

     ```
     # pkgrecv -s base_release_media/pkgs/VRTSpkgs.p5p -d
     /ai/repo_symc_sparc '*'
     ```

   - For 6.1.1:

     ```
     # pkgrecv -s base_release_media/pkgs/VRTSpkgs.p5p -d
     /ai/repo_symc_sparc '*'
     ```

```
# pkgrecv -s patch_release_media/patches/VRTSpatches.p5p -d
/ai/repo_symc_sparc '*'
```

Set service property and enable it:

```
# svccfg -s pkg/server list
# svcs -a | grep pkg/server
# svccfg -s pkg/server add symcsparc
# svccfg -s pkg/server:symcsparc addpg pkg application
# svccfg -s pkg/server:symcsparc setprop pkg/port=10003
# svccfg -s pkg/server:symcsparc setprop pkg/inst_root=
/ai/repo_symc_sparc
# svccfg -s pkg/server:symcsparc addpg general framework
# svccfg -s pkg/server:symcsparc addpropvalue general/complete
astring: symcsparc
# svccfg -s pkg/server:symcsparc addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcsparc
# svcadm enable application/pkg/server:symcsparc
```

Or run the following commands to set up the private depot server for testing purposes:

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_sparc -p 10003 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://*host*:10003

4 Set up the install service on the AI server.

Run the following command:

```
# mkdir /ai/iso
```

Download the AI image from the Oracle website and place the `iso` in the `/ai/iso` directory.

Create an install service.

For example:

To set up the AI install service for SPARC platform::

```
# # installadm create-service -n sol11sparc -s\
 /ai/iso/sol-11-1111-ai-sparc.iso -d /ai/aiboot/
```

5 Run the installer to generate manifest XML files for all the SFHA Solutions products that you plan to install.

```
# mkdir /ai/manifests
# media/installmr -ai /ai/manifests
```

6 For each system, generate the system configuration and include the host name, user accounts, and IP addresses. For example, enter one of the following:

```
# mkdir /ai/profiles
# sysconfig create-profile -o /ai/profiles/profile_client.xml
```

or

```
# cp /ai/aiboot/auto-install/sc_profiles/sc_sample.xml
/ai/profiles/profile_client.xml
```

7 Add a system and match it to the specified product manifest and system configuration.

Run the following command to add a SPARC system, for example:

```
# installadm create-client -e "client_MAC" -n sol11sparc
# installadm add-manifest -n sol11sparc -f \
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n sol11sparc -f \
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n sol11sparc -m \
vrts_sfha -p profile_sc -c mac="client_MAC"
# installadm list -m -c -p -n sol11sparc
```

8 For SPARC system, run the following command to restart the system and install the operating system and Storage Foundation products:

```
# boot net:dhcp - install
```

Chapter 4

Upgrading to 6.1.1 from releases earlier than 6.1

This chapter includes the following topics:

Planning to upgrade to SFHA Solutions 6.1.1

This section includes the following topics:

Supported upgrade types

SFHA Solutions supports various ways of upgrading your cluster to the latest version. Choose a method that best suits your environment and supports your planned upgrade path.

Table 4-1 lists the supported types of upgrade.

Table 4-1 Supported types of upgrade

Type of upgrade	Abstract
Full upgrade	A full upgrade involves upgrading all the nodes in the cluster at the same time. All components are upgraded during the process. The cluster remains unavailable for the duration of the upgrade.
Phased upgrade	The phased upgrade methodology involves upgrading half of the nodes in the cluster at a time.
Rolling upgrade	The rolling upgrade minimizes downtime for highly available clusters to the amount of time that it takes to perform a service group failover.
Automated upgrade using response files	You can upgrade from SFHA Solutions using a response file.
Solaris Live Upgrade or Boot Environment upgrade (On Solaris 10 and Solaris 11 systems)	Solaris Live Upgrade or Boot Environment upgrade provides a method of upgrading a system while the system continues to operate.

Supported upgrade paths for SFHA Solutions 6.1.1 from releases earlier than 6.1

You can run the `installmr` script with Install Bundles to upgrade SFHA Solutions to 6.1.1 from releases earlier than 6.1.

For information on operating systems that are supported for 6.1.1, see *System requirments* in *Symantec™ Storage Foundation and High Availability Solutions 6.1.1 Release Notes*.

Table 4-2 lists the supported upgrade paths for Solaris SPARC.

Table 4-2 Supported upgrade paths for Solaris SPARC from releases earlier than 6.1

Current version	Solaris 8 or older	Solaris 9	Solaris 10	Solaris 11
5.1 5.1 RPs 5.1 SP1 5.1 SP1 RPs	Not applicable.	Upgrade OS to Solaris 10 or above. Upgrade to 6.1.1 using the `installmr` script with Install Bundles.	Upgrade directly to 6.1.1 using the `installmr` script with Install Bundles.	Not applicable.
6.0 6.0 RPs	Not applicable.	Not applicable.	Upgrade directly to 6.1.1 using the `installmr` script with Install Bundles.	Not applicable.
6.0 PR1	Not applicable.	Not applicable.	Not applicable.	Upgrade OS to Sol11 U1. Upgrade to 6.1.1 using the `installmr` script with Install Bundles.
6.0.1 6.0.3 6.0.5	Not applicable.	Not applicable.	Upgrade directly to 6.1.1 using the `installmr` script with Install Bundles.	Upgrade OS to Sol11 U1. Upgrade to 6.1.1 using the `installmr` script with Install Bundles.

About using the installer to upgrade from releases earlier than 6.1 when the root disk is encapsulated

Upgrading a system with an encapsulated root disk to 6.1.1 requires a reboot after upgrade.

Table 4-3 Upgrading using the installer from releases earlier than 6.1 when the root disk is encapsulated

Starting version	Ending version	Action required
5.1 5.1 RP1	6.1.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.1 SP1 5.1 SP1 RP1 5.1 SP1 RP2 5.1 SP1 RP3 5.1 SP1 RP4	6.1.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
6.0 6.0 RP1	6.1.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
6.0.1 6.0.3 6.0.5	6.1.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.

Preparing to upgrade Volume Replicator

Before installing or upgrading Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.
- If replication using VVR is configured, Symantec recommends that the disk group version is at least 110 prior to upgrading.
  You can check the Disk Group version using the following command:

  ```
  # vxdg list diskgroup
  ```

- If replication using VVR is configured, make sure the size of the SRL volume is greater than 110 MB.
  Refer to the *Symantec™ Storage Foundation and High Availability Solutions Replication Administrator's Guide*.
- If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date on all the hosts.

```
# /usr/sbin/vxrlink -g diskgroup status rlink_name
```

Note: Do not continue until the primary RLINKs are up-to-date.

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.
- Make sure that you have worked out all terminal emulation issues. Make sure that the terminal you use is fully functional for OpenBoot prompts and single-user and multi-user run levels.

See the *Symantec™ Storage Foundation and High Availability Solutions Replication Administrator's Guide* for more information.

See the *Getting Started Guide* for more information on the documentation.

Planning an upgrade from the previous VVR version

If you plan to upgrade VVR from the previous VVR version, you can upgrade VVR with reduced application downtime by upgrading the hosts at separate times. While the Primary is being upgraded, the application can be migrated to the Secondary, thus reducing downtime. The replication between the (upgraded) Primary and the Secondary, which have different versions of VVR, will still continue. This feature facilitates high availability even when the VVR upgrade is not complete on both the sites. Symantec recommends that the Secondary hosts be upgraded before the Primary host in the Replicated Data Set (RDS).

See the *Symantec™ Storage Foundation Release Notes* for information regarding VVR support for replicating across Storage Foundation versions.

Replicating between versions is intended to remove the restriction of upgrading the Primary and Secondary at the same time. VVR can continue to replicate an existing RDS with Replicated Volume Groups (RVGs) on the systems that you want to upgrade. When the Primary and Secondary are at different versions, VVR does not support changing the configuration with the `vradmin` command or creating a new RDS.

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in Table 4-4, if either the Primary or Secondary are running a version of VVR prior to 6.1.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.1.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

Table 4-4 VVR versions and checksum calculations

VVR prior to 6.1.1 (DG version <= 140)	VVR 6.1.1 (DG version >= 150)	VVR calculates checksum TCP connections?
Primary	Secondary	Yes
Secondary	Primary	Yes
Primary and Secondary		Yes
	Primary and Secondary	No

Note: When replicating between versions of VVR, avoid using commands associated with new features. The earlier version may not support new features and problems could occur.

If you do not need to upgrade all the hosts in the RDS simultaneously, you can use replication between versions after you upgrade one host. You can then upgrade the other hosts in the RDS later at your convenience.

Note: If you have a cluster setup, you must upgrade all the nodes in the cluster at the same time.

Additional settings for using VVR in a localized environment

If the language packages for VVR are installed, VVR displays localized messages, if the client locale is a supported non-English locale. The client locale is the locale from which you are accessing the VVR command line or GUI. For example, if the Japanese version of VVR is installed, then the messages are displayed in the Japanese locale, if the client locale is Japanese.

Make sure that the appropriate locale has been installed on all the hosts that are intended to be a part of the VVR RDS setup. Otherwise, some VVR error messages will be displayed in English, because it is the default locale. Make sure the following settings are done on all hosts that are intended to be part of the RDS:

- Install the required client locale from the Operating System disc.
- Install the required Volume Manager and VVR localized packages.
- Set the client locale, before using any of the VVR interfaces:
  - For the VVR command line, set the locale using the appropriate method for your operating system.
  - For VRW, select the locale from the VRW login page.

Downloading SFHA Solutions 6.1.1

The following procedure describes how to upgrade to 6.1.1 with Install Bundles from releases earlier than 6.1.

Note: If you are upgrading from releases earlier than 6.1, Symantec suggests you upgrade with Install Bundles.

1. Download Storage Foundation and High Availability Solutions 6.1 from http://fileConnect.symantec.com.
2. Extract the tar ball into a directory called /tmp/sfha6.1
3. Download SFHA Solutions 6.1.1 from https://sort.symantec.com/patches.
4. Extract it to a directory called /tmp/sfha6.1.1

Performing a full upgrade with Install Bundles

Performing a full upgrade of VCS using Install Bundles

You can use the installer to upgrade VCS.

To upgrade VCS using the product installer

1. Log in as superuser.
2. Change to the `/tmp/sfha6.1.1` directory.
3. Invoke the `installmr` script with `-base_path` option to upgrade to 6.1.1:

   ```
   # ./installmr -base_path /tmp/sfha6.1/
   ```

4. From the opening Selection Menu, choose: **G** for "Upgrade a Product."
5. Choose **1** for Full Upgrade.
6. Enter the names of the nodes that you want to upgrade. Use spaces to separate node names. Press the Enter key to proceed.

   The installer runs some verification checks on the nodes.

7 When the verification checks are complete, the installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.

The installer lists the packages to upgrade.

8 The installer asks if you want to stop VCS processes. Press the Enter key to continue.

The installer stops VCS processes, uninstalls packages, installs or upgrades packages, configures, and startsVCS.

The installer lists the nodes that Symantec recommends you to restart, if needed.

9 The installer asks if you would like to send the information about this installation to Symantec to help improve installation in the future. Enter your response.

The installer displays the location of log files, summary file, and response file.

10 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Performing a full upgrade of SFHA using Install Bundles

This section describes how to perform a full upgrade of SFHA using Install Bundles.

Upgrading SFHA with Install Bundles

This section describes upgrading to the current Storage Foundation and High Availability, and you do not intend to upgrade your Solaris version. Only use this procedure if you are already running a version of Solaris that is supported with 6.1.1.

To upgrade Storage Foundation and High Availability

1. Log in as superuser.
2. Unmount any mounted VxFS file systems that are not managed by VCS.

   The installer supports the upgrade of multiple hosts, if each host is running the same version of VxVM and VxFS. Hosts must be upgraded separately if they are running different versions.

   If any VxFS file systems are mounted with the QuickLog feature, QuickLog must be disabled before upgrading. See the "Veritas QuickLog" chapter of the *Symantec™ File System Administrator's Guide* for more information.
3. If you are upgrading a high availability (HA) product, take all service groups offline.

   List all service groups:

   ```
   # /opt/VRTSvcs/bin/hagrp -list
   ```

   For each service group listed, take it offline:

   ```
   # /opt/VRTSvcs/bin/hagrp -offline service_group \
     -sys system_name
   ```
4. Enter the following commands on each node to freeze HA service group operations:

   ```
   # haconf -makerw
   # hasys -freeze -persistent nodename
   # haconf -dump -makero
   ```
5. If your system has separate `/opt` and `/var` file systems, make sure they are mounted before proceeding with installation.
6. If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date:

   ```
   # vxrlink -g diskgroup status rlink_name
   ```

   Note: Do not continue until the Primary RLINKs are up-to-date.
7. To invoke the common installer, run the `installmr` command as shown in this example:

   ```
   # cd /tmp/sfha6.1.1
   # ./installmr -base_path /tmp/sfha6.1/
   ```

8 Enter `G` to upgrade and press Return.

9 You are prompted to enter the system names (in the following example, "host1"). Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install SFHA:  host1
```

Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

10 Installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.

11 You can perform this step if you upgrading from SFHA 5.1 SP1 for Solaris.

The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's book disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer **y**.

Note: Splitting the mirrors for the root disk group backup requires a reboot upon completion of the upgrade.

---

12 The installer then prompts you to name the backup boot disk group. Enter the name for it or press **Enter** to accept the default.

Note: The split operation can take some time to complete.

---

13 You are prompted to start the split operation. Press **y** to continue.

14 Stop the product's processes.

```
Do you want to stop SFHA processes now? ? [y,n,q] (y) y
```

15 The installer lists the packages to install or upgrade, and performs the installation or upgrade.

16 If the product is licensed with a stale (old) key, the installer would prompt users to update the key.

17 The installer verifies, configures, and starts the Symantec Storage Foundation software.

18 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

19 Only perform this step if you have split the boot disk group into a backup disk group. After a successful reboot, verify the upgrade and re-join the backup disk group. If the upgrade fails, revert to the backup disk group.

20 Unfreeze the service groups.

21 Take the service groups online.

Performing a full upgrade of SFCFSHA using Install Bundles

This section describes how to perform a full upgrade of SFCFSHA using Install Bundles.

- Performing a full SFCFSHA upgrade with Install Bundles

Performing a full SFCFSHA upgrade with Install Bundles

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean
- Performing the upgrade

Ensuring the file systems are clean

Before upgrading to SFCFSHA 6.1.1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

To ensure the file systems are clean

1. Log in as superuser onto any node in the cluster.
2. Take the service group offline on each node of the cluster, which contains VxFS and CFS resources:

   ```
   # hagrp -offline group -any
   ```

   where *group* is the VCS service group that has the CVMVolDg and CFSMount resource.

   Repeat this step for each SFCFSHA service group.

   Note: This unmounts the CFS file systems.

3. Unmount all VxFS file systems not under VCS control:

   ```
   # umount /mount_point
   ```

4. Check and repair each VxFS file system:

   ```
   # fsck -F vxfs /dev/vx/rdsk/diskgroup/volume
   ```

   The `fsck` command in `/opt/VRTS/bin` accepts either the block or character device (`/dev/vx/dsk/dg/vol`) or (`/dev/vx/rdsk/dg/vol`). The operating system version of `fsck` may limit the device types it accepts.

   For more information, see the `fsck` and `fsck_vxfs` man pages.

   Repeat this step for each file system.

Performing the upgrade

To perform the upgrade

1. Log in as superuser.
2. Change to the `/tmp/sfha6.1.1` directory:

   ```
   # cd /tmp/sfha6.1.1
   ```

3 Verify there are no VxFS file systems mounted on the nodes being upgraded:

```
# mount -p | grep vxfs
```

If any VxFS file systems are mounted, offline the group on each node of the cluster:

```
# hagrp -offline group -sys sys1
# hagrp -offline group -sys sys2
# hagrp -offline group -sys sys3
# hagrp -offline group -sys sys4
```

where *group* is the VCS service group that has the CVMVolDg and CFSMount resource.

If VxFS file systems are not managed by VCS then unmount them manually:

```
# umount /mount_point
```

Repeat this step for each SFCFSHA service group.

4 Change to the `/tmp/sfha6.1.1` directory. Invoke the `installmr` script with `-base_path` option to upgrade to 6.1.1:

```
# ./installmr -base_path /tmp/sfha6.1/
```

5 From the opening Selection Menu, choose: **G** for **Upgrade a Product**. Choose **1** for **Full Upgrade**.

6 You are prompted to enter the system names (in the following example, "sys1" and "sys2") on which the software is to be upgraded. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install SFCFSHA: sys1 sys2
```

7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA). Press **y** to agree and continue.

8 The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's boot disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer **y**.

9 During the initial system check, the installer verifies that communication between systems has been set up.

If the installer hangs or asks for a login password, sertup passwordless ssh or setup rsh from the system that run `installmr` to the system that need to be upgraded to 6.1.1. Then run the installer again.

10 After you accept EULA and the system checks complete, the installer displays a list of the packages that will be upgraded. Press Enter to continue with the upgrade.

11 Output shows information that SFCFSHA must be stopped on a running system. Enter **y** to continue.

12 The installer stops, uninstalls, reinstalls, and starts specified packages.

13 Press **Enter** again for summary information about logs and reboots.

Do not remove the log files until the Symantec products are working properly on your system. Technical Support will need these log files for debugging purposes.

14 Update the configuration.

15 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

16 Only perform this step if you have split the mirrored root disk to back it up. After a successful reboot, verify the upgrade and re-join the backup disk group. If the upgrade fails, revert to the backup disk group.

Performing a full upgrade of SF Oracle RAC using Install Bundles

This section describes how to perform a full upgrade of SF Oracle RAC using Install Bundles.

- Preparing to perform a full upgrade to 6.1.1 on an SF Oracle RAC cluster
- Upgrading to SF Oracle RAC 6.1.1

Preparing to perform a full upgrade to 6.1.1 on an SF Oracle RAC cluster

Perform the preparatory steps in this section if you are performing a full upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.

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, CRSResource.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
   ```

3. Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

   If not, a warning message will be displayed after `installmr` upgrade prechecks.

   Warning: Backup `/etc/vx/cbr/bk` directory.

4. Stop all applications that use VxFS or VxVM disk groups, whether local or CFS.

   If the applications are under VCS control:

   ```
   # hagrp -offline grp_name -any
   ```

   If the applications are not under VCS control:

   Use native application commands to stop the application.

5. For Oracle RAC 9i, log in as Oracle user on each node and stop the database:
   - If the `gsd` server is configured for Oracle RAC 9i using Oracle cluster software, run the `srvctl` command to stop the Oracle database:

     ```
     $srvctl stop database -d db_name
     ```

     Run the following command to stop the `gsd` server:

     ```
     $ORACLE_HOME/bin/gsdctl stop
     ```

- If the `gsd` server is unconfigured and the cluster is using the third party software for Oracle RAC 9i, run the following command on each node from SQL prompt:

  ```
  shutdown immediate
  ```

6 Stop all Oracle RAC resources.

  For Oracle RAC 10g, Oracle RAC 11g, and Oracle RAC 12c:

  - If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

    ```
    # hagrp -offline oracle_group -any
    ```

  - If the database instances are not managed by VCS, then run the following on one node:
    - For Oracle RAC 10g and Oracle RAC 11g:

      ```
      $ srvctl stop database -d db_name
      ```

    - For Oracle RAC 12c:

      ```
      $ srvctl stop database -db db_name
      ```

7 - 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:

    ```
    # 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:
    - For Oracle RAC 10g and Oracle RAC 11g:

      ```
      $ srvctl modify database -d db_name -y MANUAL
      ```

    - For Oracle RAC 12c:

      ```
      $ srvctl modify database -db db_name -policy MANUAL
      ```

8 Stop VCS on all nodes:

```
# hastop -all
```

9 Unmount 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
```

10 If you plan to continue using the Storage Foundation for Databases (SFDB) tools, you must prepare to migrate the SFDB repository database before upgrading to 6.1.1.

See "Pre-upgrade tasks for migrating the SFDB repository database" on page 46.

11 If you plan to upgrade the operating system, stop all ports.

If you are running version 5.1 and later, stop the ports using the installer:

```
# /opt/VRTS/install/installsfrac -stop
```

If you are upgrading to Solaris 10 Update 10, apply the following Oracle patches: `144524-02` (SPARC). See the Oracle documentation for instructions.

Pre-upgrade tasks for migrating the SFDB repository database

If you plan to continue using Database Storage Checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, you must migrate the SFDB repository database to 6.1.1.

Note: The Sfua_Base repository resource group will be removed from the main.cf file. It is not required as a separate service group for SF Oracle RAC 6.1.1.

Perform the following before upgrading SF Oracle RAC.

To prepare to migrate the repository database

- Resynchronize all existing snapshots before upgrading. As Oracle user, enter:

```
$ /opt/VRTS/bin/dbed_vmsnap -S $ORACLE_SID \
-f SNAPPLAN -o resync
```

Warning: The Database Flashsnap clone database will not be able to be carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 6.1.1.

Upgrading to SF Oracle RAC 6.1.1

This section provides instructions for upgrading to SF Oracle RAC 6.1.1.

- If required, upgrade the operating system.
- Upgrade to SF Oracle RAC 6.1.1.
- Bring the SF Oracle RAC online.

Upgrading the operating system

If you want to upgrade the operating system, perform the following steps:

1. Rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

2. If you are upgrading to Solaris 10 Update 10, apply the following Oracle (Solaris) patches. For instructions, see Oracle documentation.
   - For SPARC: `144524-02`
   - For x86: `144525-02`
3. Upgrade the operating system on all nodes in the cluster.

   For instructions, see the operating system documentation.
4. After the system restarts, restore the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

Upgrading SF Oracle RAC using Install Bundles

Use the `installmr` script-based installation programs to upgrade SF Oracle RAC.

The installer performs the following tasks to upgrade SF Oracle RAC:

- Verifies the compatibility of the systems before the upgrade.
- Stops the SF Oracle RAC processes before the upgrade.
- Uninstalls SF Oracle RAC.
- Installs the SF Oracle RAC 6.1 packages on the nodes.
- Installs the SF Oracle RAC 6.1.1 patches on the nodes.
- Starts the SF Oracle RAC processes after the upgrade.
- Displays the location of the log files, summary file, and response file.

To upgrade to SF Oracle RAC 6.1.1 using the installmr program

1. Log in as superuser.
2. Change to the `/tmp/sfha6.1.1` directory.
3. Invoke the `installmr` script with `-base_path` option to upgrade to 6.1.1:

   ```
   # ./installmr -base_path /tmp/sfha6.1/
   ```

4. From the opening Selection Menu, choose: **G** for "Upgrade a Product."
5. Select 1 for **Full upgrade**.

   The installer displays the copyright message and specifies the directory where the running logs are created.

   The installer verifies the systems for compatibility.

   Note: If `had` is stopped before upgrade, the installer displays the following warning:

   VCS is not running before upgrade. Please make sure all the configurations are valid before upgrade.

   If the configuration files are valid, you may ignore the message.

   During the system verification phase, the installer checks if the boot disk is encapsulated and the upgrade path. If the upgrade is not supported, you need to un-encapsulate the boot disk.

   Review the messages displayed and make sure that you meet the requirements before proceeding with the upgrade.

6 Press **Enter** to continue with the upgrade.

Enter y to agree to the End User License Agreement (EULA).

The installer displays the list of packages that will be uninstalled. Press **Enter** to view the list of packages that will be upgraded.

The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's book disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer y.

7 Enter the name of the backup boot disk group when prompted. Press **Enter** to accept the default.

You are prompted to start the split operation.

8 Enter **y** to continue with the split operation.

The split operation can take some time to complete.

Note: Verify the boot device from which the system is set to boot. Make sure that the system is set to start from the boot device with the required version of SF Oracle RAC.

---

9 Enter **y** to stop the SF Oracle RAC processes.

```
Do you want to stop SF Oracle RAC processes now? [y,n,q,?] (y)
```

The installer stops the processes and uninstalls SF Oracle RAC. After the uninstallation, the installer installs SF Oracle RAC 6.1.1 and starts 6.1.1 on all the nodes.

If the product is licensed with stale (old) key, the installer prompts users to update the key.

10 Install the language packages and patches if you would like to run SF Oracle RAC in a language other than English.

11 Relink the SF Oracle RAC libraries with Oracle:

The installer prompts a menu after upgrade. If you want the installer to relink the Oracle Database Binary, choose the option **Relink Oracle Database Binary** from the menu.

Complete the remaining tasks to finish the upgrade.

Bringing the Oracle database online

1 Bring the Oracle database service group online.

- If the Oracle database is managed by VCS:

```
# hagrp -online oracle_group -any
```

- If the Oracle database is not managed by VCS:
  - For Oracle RAC 10g and Oracle RAC 11g:

```
# srvctl start database -d db_name
```

  - For Oracle RAC 12c:

```
# srvctl start database -db db_name
```

2 Start all applications that are not managed by VCS. Use native application commands to start the applications.

3
- If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrp -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:
  - For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

  - For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

4 Complete other post-upgrade steps.

For instructions, see the chapter *Performing post-upgrade tasks* in *Symantec™ Storage Foundation for Oracle RAC 6.1 Installation and Configuration Guide*.

5 For upgrade scenarios that involve Oracle RAC 9i, start the database:

- If the `gsd` server is configured for Oracle RAC 9i using Oracle cluster software, run the `gsd` command to start the Oracle database:

```
$ $ORACLE_HOME/bin/gsdctl start
```

Run the following command to start the `srvctl` server:

```
$ srvctl start database -d db_name
```

- If the `gsd` server is unconfigured and the cluster is using the third party software for Oracle RAC 9i, run the following command on each node from SQL prompt:

```
$ startup
```

6 Upgrade Oracle RAC, if required.

For information on Oracle RAC support, see:

http://www.symantec.com/docs/DOC5081

For instructions, see the chapter *Upgrading Oracle RAC* in 6.1 SF Oracle RAC Installation Guide.

Note: The procedure for Oracle RAC 12c is the same as that for Oracle RAC 11g Release 2.

7 If you want to upgrade all application clusters to version 6.1.1, make sure that you upgraded CP server systems that use VCS or SFHA to 6.1.1. Then, upgrade all application clusters to version 6.1.1.

For instructions to upgrade VCS or SFHA on the CP server systems, see the 6.1 VCS or SFHA installation guide.

Performing a phased upgrade using Install Bundles

This section explains how to perform a phased upgrade of SFHA Solutions on four nodes with four service groups. Note that in this scenario, SFHA Solutions and the service groups cannot stay online on the second subcluster during the upgrade of the second subcluster. Do not add, remove, or change resources or service groups on any nodes during the upgrade. These changes are likely to get lost after the upgrade.

- Performing a phased VCS upgrade using Install Bundles
- Performing a phased SFHA upgrade using Install Bundles
- Performing a phased SFCFSHA upgrade using Install Bundles

- Performing a phased upgrade of SF Oracle RAC using Install Bundles

Performing a phased VCS upgrade using Install Bundles

You can perform a phased VCS upgrade with the following steps:

1. Moving the service groups to the second subcluster.

   See *Veritas Cluster Server 6.0.1 Installation Guide*.

2. Upgrading the operating system on the first subcluster.

   See *Veritas Cluster Server 6.0.1 Installation Guide*.

3. Upgrading the first subcluster.

   See "Step 3: Upgrading the first subcluster" on page 57.

4. Preparing the second subcluster.

   See *Veritas Cluster Server 6.0.1 Installation Guide*.

5. Activating the first subcluster.

   See *Veritas Cluster Server 6.0.1 Installation Guide*.

6. Upgrading the operating system on the second subcluster.

   See *Veritas Cluster Server 6.0.1 Installation Guide*.

7. Upgrading the second subcluster.

   See "Step 7: Upgrading the second subcluster" on page 63.

8. Finishing the phased upgrade.

   See *Veritas Cluster Server 6.0.1 Installation Guide*.

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.

To move service groups to the second subcluster

1 On the first subcluster, determine where the service groups are online.

```
# hagrp -state
```

The output resembles:

```
#Group   Attribute System Value
sg1      State     sys1 |ONLINE|
sg1      State     sys2 |ONLINE|
sg1      State     sys3 |ONLINE|
sg1      State     sys4 |ONLINE|
sg2      State     sys1 |ONLINE|
sg2      State     sys2 |ONLINE|
sg2      State     sys3 |ONLINE|
sg2      State     sys4 |ONLINE|
sg3      State     sys1 |ONLINE|
sg3      State     sys2 |OFFLINE|
sg3      State     sys3 |OFFLINE|
sg3      State     sys4 |OFFLINE|
sg4      State     sys1 |OFFLINE|
sg4      State     sys2 |ONLINE|
sg4      State     sys3 |OFFLINE|
sg4      State     sys4 |OFFLINE|
```

2 Offline the parallel service groups (sg1 and sg2) from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (sys1 and sys2) to the nodes on the second subcluster (sys3 and sys4). For SFHA, vxfen sg is the parallel service group.

```
# hagrp -offline sg1 -sys sys1
# hagrp -offline sg2 -sys sys1
# hagrp -offline sg1 -sys sys2
# hagrp -offline sg2 -sys sys2
# hagrp -switch sg3 -to sys3
# hagrp -switch sg4 -to sys4
```

3 On the nodes in the first subcluster, unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -k
```

```
Filesystem          kbytes    used   avail capacity  Mounted on
/dev/dsk/c1t0d0s0   66440242 10114415 55661425  16%  /
/devices                0       0       0     0%  /devices
ctfs                    0       0       0     0%  /system/contract
proc                    0       0       0     0%  /proc
mnttab                  0       0       0     0%  /etc/mnttab
swap                 5287408    1400 5286008     1%  /etc/svc/volatile
objfs                   0       0       0     0%  /system/object
sharefs                 0       0       0     0%  /etc/dfs/sharetab
/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcap1.so.1
                   66440242 10114415 55661425    16%  /platform/sun4u-us3/lib/
libc_psr.so.1
/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1
                    66440242 10114415 55661425    16%    /platform/sun4u-us3/lib/
sparcv9/libc_psr.so.1
fd                      0       0       0     0%    /dev/fd
swap                 5286064      56 5286008     1%    /tmp
swap                 5286056      48 5286008     1%    /var/run
swap                 5286008       0 5286008     0%    /dev/vx/dmp
swap                 5286008       0 5286008     0%    /dev/vx/rdmp
                      3.0G   18M  2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
                      1.0G   18M  944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
                       10G   20M  9.4G   1% /mnt/dg2/dg2vol3
```

```
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

5 Freeze the nodes in the first subcluster.

```
# hasys -freeze -persistent sys1
# hasys -freeze -persistent sys2
```

6 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

7 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```
# hagrp -state
```

Output resembles:

```
#Group Attribute System Value
sg1  State sys1 |OFFLINE|
sg1  State sys2 |OFFLINE|
sg1  State sys3 |ONLINE|
sg1  State sys4 |ONLINE|
sg2  State sys1 |OFFLINE|
sg2  State sys2 |OFFLINE|
sg2  State sys3 |ONLINE|
sg2  State sys4 |ONLINE|
sg3  State sys1 |OFFLINE|
sg3  State sys2 |OFFLINE|
sg3  State sys3 |ONLINE|
sg3  State sys4 |OFFLINE|
sg4  State sys1 |OFFLINE|
sg4  State sys2 |OFFLINE|
sg4  State sys3 |OFFLINE|
sg4  State sys4 |ONLINE|
```

8 Backup the lltab, llthosts, gabtab, types.cf, main.cf and AT configuration files on the first subcluster.

```
# cp /etc/lltab /etc/lltab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf \
  /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf \
  /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
  /var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
  /var/VRTSat/.VRTSat/profile/certstore
  /var/VRTSat/ABAuthSource
  /etc/vx/vss/VRTSat.conf
  Quiescing ...
  Snapshot Directory :/var/VRTSatSnapShot
```

Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting LLT_START = **0**.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Step 3: Upgrading the first subcluster

After step 1 and step 2, you now navigate to the installer program and start it.

To start the installer for the phased upgrade

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Make sure that you can ssh or rsh from the node where you launched the installer to the nodes in the second subcluster without requests for a password.
3. Start the installvcs program, specify the nodes in the first subcluster (sys1 and sys2).

   ```
   # cd /tmp/sfha6.1.1

   # ./installmr -base_path /tmp/sfha6.0.1/  sys1 sys2
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs.
4. From the opening Selection Menu, choose: G for **Upgrade a Product**.
5. Enter **y** to agree to the End User License Agreement (EULA).

6 When you are prompted, reply **y** to stop appropriate processes.

```
Do you want to stop VCS processes? [y,n,q] (y)
```

7 The installer ends for the first subcluster with the following output:

```
    Configuring VCS: 100%

    Estimated time remaining: 0:00

    Performing VCS upgrade configuration ..................... Done

Veritas Cluster Server Configure completed successfully


You are performing phased upgrade (Phase 1) on the systems.
Follow  the steps in install guide to upgrade the remaining
systems.

Would you like to send the information about this installation to
Symantec to help improve installation in the future? [y,n,q,?] (y)
```

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the Preparing the second subcluster procedure.

Preparing the second subcluster

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.

To prepare to upgrade the second subcluster

1 Get the summary of the status of your resources.

```
# hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen

A  sys1             EXITED               1
A  sys2             EXITED               1
A  sys3             RUNNING              0
A  sys4             RUNNING              0

-- GROUP STATE
-- Group           System  Probed     AutoDisabled    State

B  sg1             sys1    Y          N               OFFLINE
B  sg1             sys2    Y          N               OFFLINE
B  sg1             sys3    Y          N               ONLINE
B  sg1             sys4    Y          N               ONLINE
B  sg2             sys1    Y          N               OFFLINE
B  sg2             sys2    Y          N               OFFLINE
B  sg2             sys3    Y          N               ONLINE
B  sg2             sys4    Y          N               ONLINE
B  sg3             sys1    Y          N               OFFLINE
B  sg3             sys2    Y          N               OFFLINE
B  sg3             sys3    Y          N               ONLINE
B  sg3             sys4    Y          N               OFFLINE
B  sg4             sys1    Y          N               OFFLINE
B  sg4             sys2    Y          N               OFFLINE
B  sg4             sys3    Y          N               OFFLINE
B  sg4             sys4    Y          N               ONLINE
```

2 Unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -k
```

```
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c1t0d0s0    66440242 10114415 55661425    16%    /
/devices                   0       0       0     0%    /devices
ctfs                       0       0       0     0%    /system/contract
proc                       0       0       0     0%    /proc
mnttab                     0       0       0     0%    /etc/mnttab
swap                 5287408    1400 5286008     1%    /etc/svc/volatile
objfs                      0       0       0     0%    /system/object
sharefs                    0       0       0     0%    /etc/dfs/sharetab
/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcap1.so.1
                     66440242 10114415 55661425    16%    /platform/sun4u-us3/
lib/libc_psr.so.1
/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1
                     66440242 10114415 55661425    16%    /platform/sun4u-us3/
lib/sparcv9/libc_psr.so.1
fd                         0       0       0     0%    /dev/fd
swap                 5286064      56 5286008     1%    /tmp
swap                 5286056      48 5286008     1%    /var/run
swap                 5286008       0 5286008     0%    /dev/vx/dmp
swap                 5286008       0 5286008     0%    /dev/vx/rdmp
                      3.0G   18M  2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
                      1.0G   18M  944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
                       10G   20M  9.4G   1% /mnt/dg2/dg2vol3
```

```
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

3 Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

4 Unfreeze the service groups.

```
# hagrp -unfreeze sg1 -persistent
# hagrp -unfreeze sg2 -persistent
# hagrp -unfreeze sg3 -persistent
# hagrp -unfreeze sg4 -persistent
```

5 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

6 Take the service groups offline on sys3 and sys4.

```
# hagrp -offline sg1 -sys sys3
# hagrp -offline sg1 -sys sys4
# hagrp -offline sg2 -sys sys3
# hagrp -offline sg2 -sys sys4
# hagrp -offline sg3 -sys sys3
# hagrp -offline sg4 -sys sys4
```

7 Verify the state of the service groups.

```
# hagrp -state
#Group       Attribute    System     Value
sg1            State      sys1    |OFFLINE|
sg1            State      sys2    |OFFLINE|
sg1            State      sys3    |OFFLINE|
sg1            State      sys4    |OFFLINE|
sg2            State      sys1    |OFFLINE|
sg2            State      sys2    |OFFLINE|
sg2            State      sys3    |OFFLINE|
sg2            State      sys4    |OFFLINE|
sg3            State      sys1    |OFFLINE|
sg3            State      sys2    |OFFLINE|
sg3            State      sys3    |OFFLINE|
sg3            State      sys4    |OFFLINE|
```

8 Stop VCS, I/O Fencing, GAB, and LLT on sys3 and sys4.

- Solaris 10 and 11:

```
# svcadm disable -t /system/vcs
# svcadm disable -t /system/vxfen
# svcadm disable -t /system/gab
# svcadm disable -t /system/llt
```

9 Make sure that the VXFEN, GAB, and LLT modules on sys3 and sys4 are not configured.

- Solaris 10 and 11:

```
# /lib/svc/method/vxfen status
VXFEN: loaded

# /lib/svc/method/gab status
GAB: module not configured

# /lib/svc/method/llt status
LLT: is loaded but not configured
```

Activating the first subcluster

Get the first subcluster ready for the service groups.

Note: These steps fulfill part of the installer's output instructions, see Step 3: Upgrading the first subcluster step Preparing the second subcluster.

To activate the first subcluster

1 Start LLT and GAB.

```
# svcadm enable system/llt

# svcadm enable system/gab
```

2 Seed sys1 and sys2 in the first subcluster.

```
# gabconfig -x
```

3 On the first half of the cluster, start VCS:

```
# cd /opt/VRTS/install

# ./installvcs<version> -start  sys1 sys2
```

Where <*version*> is the specific release version.

4 Start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

5 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

6 Unfreeze the nodes in the first subcluster.

```
# hasys -unfreeze -persistent sys1
# hasys -unfreeze -persistent sys2
```

7 Unfreeze service groups in the first subcluster.

```
# hagrp -unfreeze sg1 -persistent

# hagrp -unfreeze sg2 -persistent
```

8 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

9 Bring the service groups online on sys1 and sys2.

```
# hagrp -online sg1 -sys sys1
# hagrp -online sg1 -sys sys2
# hagrp -online sg2 -sys sys1
# hagrp -online sg2 -sys sys2
# hagrp -online sg3 -sys sys1
# hagrp -online sg4 -sys sys2
```

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting LLT_START = **0**.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Step 7: Upgrading the second subcluster

After step 4 to step 6, perform the following procedure to upgrade the second subcluster (sys3 and sys4).

To start the installer to upgrade the second subcluster

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Navigate to the folder that contains the SFHA Solutions 6.1.1 binary.

   ```
   # cd /tmp/sfha6.1.1
   ```

3. Confirm that VCS is stopped on sys3 and sys4. Specify the nodes in the second subcluster (sys3 and sys4).

   ```
   # ./installmr -base_path /tmp/sfha6.0.1/ sys3 sys4
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs.
4. From the opening Selection Menu, choose: G for **Upgrade a Product**.
5. Enter **y** to agree to the End User License Agreement (EULA).
6. Monitor the installer program answering questions as appropriate until the upgrade completes.

Finishing the phased upgrade

Complete the following procedure to complete the upgrade.

To finish the upgrade

1. Verify that the cluster UUID is the same on the nodes in the second subcluster and the first subcluster. Run the following command to display the cluster UUID:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl
   -clus -display sys1 [sys2 ...]
   ```

   If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus
   -copy -from_sys sys1 -to_sys sys3 sys4
   ```

2. On the second half of the cluster, start VCS:

   ```
   # cd /opt/VRTS/install

   # ./installvcs<version> -start sys3 sys4
   ```

   Where <*version*> is the specific release version.

3 For nodes that use Solaris 10, start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

4 Check to see if VCS and its components are up.

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   nxxxnn membership 0123
Port b gen   nxxxnn membership 0123
Port h gen   nxxxnn membership 0123
```

5 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```
# hastatus -sum

-- SYSTEM STATE
-- System          State           Frozen

A  sys1          RUNNING         0
A  sys2          RUNNING         0
A  sys3          RUNNING         0
A  sys4          RUNNING         0

-- GROUP STATE
-- Group    System    Probed   AutoDisabled   State
B  sg1      sys1    Y        N              ONLINE
B  sg1      sys2    Y        N              ONLINE
B  sg1      sys3    Y        N              ONLINE
B  sg1      sys4    Y        N              ONLINE
B  sg2      sys1    Y        N              ONLINE
B  sg2      sys2    Y        N              ONLINE
B  sg2      sys3    Y        N              ONLINE
B  sg2      sys4    Y        N              ONLINE
B  sg3      sys1    Y        N              ONLINE
B  sg3      sys2    Y        N              OFFLINE
B  sg3      sys3    Y        N              OFFLINE
B  sg3      sys4    Y        N              OFFLINE
B  sg4      sys1    Y        N              OFFLINE
B  sg4      sys2    Y        N              ONLINE
B  sg4      sys3    Y        N              OFFLINE
B  sg4      sys4    Y        N              OFFLINE
```

In this example, you have performed a phased upgrade of VCS. The service groups were down when you took them offline on sys3 and sys4, to the time VCS brought them online on sys1 and sys2.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

Performing a phased SFHA upgrade using Install Bundles

You can perform a phased upgrade from SFHA 5.0 MP3 or other supported previous versions to SFHA 6.1.1.

Performing a phased upgrade involves the following tasks:

1. Moving the service groups to the second subcluster.

   See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

2. Upgrading the operating system on the first subcluster.

   See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

3. Upgrading the first subcluster.

   See "Upgrading the first subcluster" on page 72.

4. Preparing the second subcluster.

   See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

5. Activating the first subcluster.

   See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

6. Upgrading the operating system on the second subcluster.

   See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

7 Upgrading the second subcluster.

See “Upgrading the second subcluster” on page 78.

8 Finishing the phased upgrade.

See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.

To move service groups to the second subcluster

1 On the first subcluster, determine where the service groups are online.

```
# hagrp -state
```

The output resembles:

```
#Group   Attribute System Value
sg1      State     sys1 |ONLINE|
sg1      State     sys2 |ONLINE|
sg1      State     sys3 |ONLINE|
sg1      State     sys4 |ONLINE|
sg2      State     sys1 |ONLINE|
sg2      State     sys2 |ONLINE|
sg2      State     sys3 |ONLINE|
sg2      State     sys4 |ONLINE|
sg3      State     sys1 |ONLINE|
sg3      State     sys2 |OFFLINE|
sg3      State     sys3 |OFFLINE|
sg3      State     sys4 |OFFLINE|
sg4      State     sys1 |OFFLINE|
sg4      State     sys2 |ONLINE|
sg4      State     sys3 |OFFLINE|
sg4      State     sys4 |OFFLINE|
```

2 Offline the parallel service groups (sg1 and sg2) from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (sys1 and sys2) to the nodes on the second subcluster (sys3 and sys4). For SFHA, vxfen sg is the parallel service group.

```
# hagrp -offline sg1 -sys sys1
# hagrp -offline sg2 -sys sys1
# hagrp -offline sg1 -sys sys2
# hagrp -offline sg2 -sys sys2
# hagrp -switch sg3 -to sys3
# hagrp -switch sg4 -to sys4
```

3 On the nodes in the first subcluster, unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -k
```

```
Filesystem          kbytes    used   avail capacity  Mounted on
/dev/dsk/c1t0d0s0   66440242 10114415 55661425  16%  /
/devices                0       0       0     0%  /devices
ctfs                    0       0       0     0%  /system/contract
proc                    0       0       0     0%  /proc
mnttab                  0       0       0     0%  /etc/mnttab
swap                 5287408    1400 5286008     1%  /etc/svc/volatile
objfs                   0       0       0     0%  /system/object
sharefs                 0       0       0     0%  /etc/dfs/sharetab
/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcap1.so.1
                   66440242 10114415 55661425    16%  /platform/sun4u-us3/lib/
libc_psr.so.1
/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1
                    66440242 10114415 55661425    16%    /platform/sun4u-us3/lib/
sparcv9/libc_psr.so.1
fd                      0       0       0     0%    /dev/fd
swap                 5286064      56 5286008     1%    /tmp
swap                 5286056      48 5286008     1%    /var/run
swap                 5286008       0 5286008     0%    /dev/vx/dmp
swap                 5286008       0 5286008     0%    /dev/vx/rdmp
                      3.0G   18M  2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
                      1.0G   18M  944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
                       10G   20M  9.4G   1% /mnt/dg2/dg2vol3
```

```
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

4 On the nodes in the first subcluster, stop all VxVM volumes (for each disk group) that VCS does not manage.

5 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

6 Freeze the nodes in the first subcluster.

```
# hasys -freeze -persistent sys1
# hasys -freeze -persistent sys2
```

7 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

8 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```
# hagrp -state
```

Output resembles:

```
#Group Attribute System Value
sg1  State sys1 |OFFLINE|
sg1  State sys2 |OFFLINE|
sg1  State sys3 |ONLINE|
sg1  State sys4 |ONLINE|
sg2  State sys1 |OFFLINE|
sg2  State sys2 |OFFLINE|
sg2  State sys3 |ONLINE|
sg2  State sys4 |ONLINE|
sg3  State sys1 |OFFLINE|
sg3  State sys2 |OFFLINE|
sg3  State sys3 |ONLINE|
sg3  State sys4 |OFFLINE|
sg4  State sys1 |OFFLINE|
sg4  State sys2 |OFFLINE|
sg4  State sys3 |OFFLINE|
sg4  State sys4 |ONLINE|
```

9 Back up the llttab, llthosts, gabtab, types.cf, main.cf and AT configuration files on the first subcluster.

```
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf \
    /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf \
    /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
B|/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B|/var/VRTSat/.VRTSat/profile/certstore
B|/var/VRTSat/ABAuthSource
B|/etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
```

Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting LLT_START = **0**.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the first subcluster

After step 1 and step 2, you now navigate to the installer program and start it.

To start the installer for the phased upgrade

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Navigate to the folder that contains the SFHA Solutions 6.1.1 binary.

   ```
   # cd /tmp/sfha6.1.1.
   ```

3. Make sure that you can ssh or rsh from the node where you launched the installer to the nodes in the second subcluster without requests for a password.
4. Start the installmr program, specify the nodes in the first subcluster (sys1 and sys2).

   ```
   # ./installmr -base_path /tmp/sfha6.0.1/ sys1 sys2
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs. It performs a system verification and outputs upgrade information.
5. From the opening Selection Menu, select G for **Upgrade a Product** and from the sub menu, select **Full Upgrade**.
6. Enter **y** to agree to the End User License Agreement (EULA).

7 The installer displays the list of packages that get removed, installed, and upgraded on the selected systems.

8 When you are prompted, reply **y** to stop appropriate processes.

```
Do you want to stop SFHA processes now? [y,n,q] (y)
```

The installer stops processes, uninstalls packages, and installs packages.

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the Upgrading the second subcluster procedure.

Preparing the second subcluster

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.

To prepare to upgrade the second subcluster

1 Get the summary of the status of your resources.

```
# hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen

A  sys1              EXITED               1
A  sys2              EXITED               1
A  sys3              RUNNING              0
A  sys4              RUNNING              0

-- GROUP STATE
-- Group           System  Probed     AutoDisabled    State

B  sg1             sys1   Y          N               OFFLINE
B  sg1             sys2   Y          N               OFFLINE
B  sg1             sys3   Y          N               ONLINE
B  sg1             sys4   Y          N               ONLINE
B  sg2             sys1   Y          N               OFFLINE
B  sg2             sys2   Y          N               OFFLINE
B  sg2             sys3   Y          N               ONLINE
B  sg2             sys4   Y          N               ONLINE
B  sg3             sys1   Y          N               OFFLINE
B  sg3             sys2   Y          N               OFFLINE
B  sg3             sys3   Y          N               ONLINE
B  sg3             sys4   Y          N               OFFLINE
B  sg4             sys1   Y          N               OFFLINE
B  sg4             sys2   Y          N               OFFLINE
B  sg4             sys3   Y          N               OFFLINE
B  sg4             sys4   Y          N               ONLINE
```

2 Unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -k
```

```
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c1t0d0s0    66440242 10114415 55661425    16%    /
/devices                 0       0       0     0%    /devices
ctfs                     0       0       0     0%    /system/contract
proc                     0       0       0     0%    /proc
mnttab                   0       0       0     0%    /etc/mnttab
swap                5287408    1400 5286008     1%    /etc/svc/volatile
objfs                    0       0       0     0%    /system/object
sharefs                  0       0       0     0%    /etc/dfs/sharetab
/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcap1.so.1
                    66440242 10114415 55661425    16%    /platform/sun4u-us3/
lib/libc_psr.so.1
/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1
                    66440242 10114415 55661425    16%    /platform/sun4u-us3/
lib/sparcv9/libc_psr.so.1
fd                       0       0       0     0%    /dev/fd
swap                5286064      56 5286008     1%    /tmp
swap                5286056      48 5286008     1%    /var/run
swap                5286008       0 5286008     0%    /dev/vx/dmp
swap                5286008       0 5286008     0%    /dev/vx/rdmp
                     3.0G   18M  2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
                     1.0G   18M  944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
                      10G   20M  9.4G   1% /mnt/dg2/dg2vol3
```

```
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

3 Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

4 Unfreeze the service groups.

```
# hagrp -unfreeze sg1 -persistent
# hagrp -unfreeze sg2 -persistent
# hagrp -unfreeze sg3 -persistent
# hagrp -unfreeze sg4 -persistent
```

5 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

6 Take the service groups offline on sys3 and sys4.

```
# hagrp -offline sg1 -sys sys3
# hagrp -offline sg1 -sys sys4
# hagrp -offline sg2 -sys sys3
# hagrp -offline sg2 -sys sys4
# hagrp -offline sg3 -sys sys3
# hagrp -offline sg4 -sys sys4
```

7 Verify the state of the service groups.

```
# hagrp -state
#Group       Attribute    System     Value
sg1            State      sys1    |OFFLINE|
sg1            State      sys2    |OFFLINE|
sg1            State      sys3    |OFFLINE|
sg1            State      sys4    |OFFLINE|
sg2            State      sys1    |OFFLINE|
sg2            State      sys2    |OFFLINE|
sg2            State      sys3    |OFFLINE|
sg2            State      sys4    |OFFLINE|
sg3            State      sys1    |OFFLINE|
sg3            State      sys2    |OFFLINE|
sg3            State      sys3    |OFFLINE|
sg3            State      sys4    |OFFLINE|
```

8 Stop all VxVM volumes (for each disk group) that VCS does not manage.

9 Stop VCS, I/O Fencing, GAB, and LLT on sys3 and sys4.

- Solaris 10 and 11:

```
# svcadm disable -t /system/vcs
# svcadm disable -t /system/vxfen
# svcadm disable -t /system/gab
# svcadm disable -t /system/llt
```

10 Make sure that the VXFEN, GAB, and LLT modules on sys3 and sys4 are not configured.

- Solaris 10 and 11:

```
# /lib/svc/method/vxfen status
VXFEN: loaded

# /lib/svc/method/gab status
GAB: module not configured

# /lib/svc/method/llt status
LLT: is loaded but not configured
```

Activating the first subcluster

Get the first subcluster ready for the service groups.

To activate the first subcluster

1 Start LLT and GAB.

```
# svcadm enable system/llt

# svcadm enable system/gab
```

2 Seed sys1 and sys2 in the first subcluster.

```
# gabconfig -x
```

3 If the product doesn't start automatically, on the first half of the cluster, start SFHA:

```
# cd /opt/VRTS/install

# ./installsfha<version> -start sys1 sys2
```

Where <*version*> is the specific release version.

4 Start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

5 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

6 Unfreeze the nodes in the first subcluster.

```
# hasys -unfreeze -persistent sys1
# hasys -unfreeze -persistent sys2
```

7 Unfreeze service groups in the first subcluster:

```
# hagrp -unfreeze sg1 -persistent

# hagrp -unfreeze sg2 -persistent
```

8 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

9 Bring the service groups online on sys1 and sys2.

```
# hagrp -online sg1 -sys sys1
# hagrp -online sg1 -sys sys2
# hagrp -online sg2 -sys sys1
# hagrp -online sg2 -sys sys2
# hagrp -online sg3 -sys sys1
# hagrp -online sg4 -sys sys2
```

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting LLT_START = **0**.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the second subcluster

After step 4 to step 6, perform the following procedure to upgrade the second subcluster (sys3 and sys4).

To start the installer to upgrade the second subcluster

1 Confirm that you are logged on as the superuser and you mounted the product disc.

2 Navigate to the folder that contains the SFHA Solutions 6.1.1 binary.

```
# cd /tmp/sfha6.1.1.
```

3 Confirm that SFHA is stopped on sys3 and sys4. Start the installmr program, specify the nodes in the second subcluster (sys3 and sys4).

```
# ./installmr -base_path /tmp/sfha6.0.1/ sys3
  sys4
```

The program starts with a copyright message and specifies the directory where it creates the logs.

4 From the opening Selection Menu, select G for **Upgrade a Product** and from the sub menu, select **Full Upgrade**.

5 The installer displays the list of packages that get removed, installed, and upgraded on the selected systems.

6 When you are prompted, reply **y** to stop appropriate processes.

```
Do you want to stop SFHA processes now? [y,n,q] (y)
```

The installer stops processes, uninstalls packages, and installs packages.

7 Enter **y** to agree to the End User License Agreement (EULA).

8 Monitor the installer program answering questions as appropriate until the upgrade completes.

After this step, for finishing the phased upgrade, see *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.*

Finishing the phased upgrade

Complete the following procedure to complete the upgrade.

To finish the upgrade

1 Verify that the cluster UUID is the same on the nodes in the second subcluster and the first subcluster. Run the following command to display the cluster UUID:

```
# /opt/VRTSvcs/bin/uuidconfig.pl
-clus -display sys1 [sys2 ...]
```

If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus
-copy -from_sys sys1 -to_sys sys3 sys4
```

2 On the second half of the cluster, start SFHA:

```
# cd /opt/VRTS/install

# ./installsfha<version> -start sys3 sys4
```

Where <*version*> is the specific release version.

3 For nodes that use Solaris 10, start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

4 Check to see if SFHA and its components are up.

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   nxxxnn membership 0123
Port b gen   nxxxnn membership 0123
Port h gen   nxxxnn membership 0123
```

5 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```
# hastatus -sum

-- SYSTEM STATE
-- System          State           Frozen

A  sys1          RUNNING         0
A  sys2          RUNNING         0
A  sys3          RUNNING         0
A  sys4          RUNNING         0

-- GROUP STATE
-- Group    System    Probed   AutoDisabled   State
B  sg1      sys1    Y        N              ONLINE
B  sg1      sys2    Y        N              ONLINE
B  sg1      sys3    Y        N              ONLINE
B  sg1      sys4    Y        N              ONLINE
B  sg2      sys1    Y        N              ONLINE
B  sg2      sys2    Y        N              ONLINE
B  sg2      sys3    Y        N              ONLINE
B  sg2      sys4    Y        N              ONLINE
B  sg3      sys1    Y        N              ONLINE
B  sg3      sys2    Y        N              OFFLINE
B  sg3      sys3    Y        N              OFFLINE
B  sg3      sys4    Y        N              OFFLINE
B  sg4      sys1    Y        N              OFFLINE
B  sg4      sys2    Y        N              ONLINE
B  sg4      sys3    Y        N              OFFLINE
B  sg4      sys4    Y        N              OFFLINE
```

6 After the upgrade is complete, start the VxVM volumes (for each disk group) and mount the VxFS file systems.

In this example, you have performed a phased upgrade of SFHA. The service groups were down when you took them offline on sys3 and sys4, to the time SFHA brought them online on sys1 or sys2.

Note: If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

Performing a phased SFCFSHA upgrade using Install Bundles

Performing a phased upgrade involves the following tasks:

1. Moving the service groups to the second subcluster.

   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

2. Upgrading the SFCFSHA stack on the first subcluster.

   See "Upgrading the SFCFSHA stack on the first subcluster" on page 84.

3. Preparing the second subcluster.

   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

4. Activating the first subcluster.

   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

5. Upgrading the operating system on the second subcluster.

   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

6. Upgrading the second subcluster.

   See "Upgrading the second subcluster" on page 89.

7. Completing the phased upgrade.

Before you start the upgrade on the first half of the cluster, back up the VCS configuration files `main.cf` and `types.cf` which are in the directory `/etc/VRTSvcs/conf/config/`.

Moving the service groups to the second subcluster

To move the service groups to the second subcluster

1. Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, `sys1` is a node in the first half of the cluster and `sys4` is a node in the second half of the cluster. Enter the following:

   ```
   # hagrp -switch failover_group -to sys4
   ```

2. On the first half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the applications.
3. On the first half of the cluster, unmount the VxFS or CFS file systems that are not managed by VCS.

   ```
   # mount -p | grep vxfs
   ```

   Verify that no processes use the VxFS or CFS mount point. Enter the following:

   ```
   # fuser -c /mount_point
   ```

   Stop any processes using a VxFS or CFS mount point with the mechanism provided by the application.

   Unmount the VxFS or CFS file system. Enter the following:

   ```
   # umount /mount_point
   ```

4. On the first half of the cluster, bring all the VCS service groups offline including CVM group. Enter the following:

   ```
   # hagrp -offline group_name -sys sys1
   ```

   When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.
5. Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

   ```
   # hagrp -state group_name
   ```

6. Freeze the nodes in the first half of the cluster. Enter the following:

   ```
   # haconf -makerw
   # hasys -freeze -persistent sys1
   # haconf -dump -makero
   ```

7 Verify that only GAB ports a, b, d and h are open. Enter the following:

```
# gabconfig -a
GAB Port Memberships
=======================================================
Port a gen 6b5901 membership 01
Port b gen 6b5904 membership 01
Port d gen 6b5907 membership 01
Port h gen ada40f membership 01
```

Do not stop VCS. Port h should be up and running.

8 In the first half of the cluster, stop all VxVM and CVM volumes. Enter the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open. Enter the following:

```
# vxprint -Aht -e v_open
```

9 On first half of the cluster, upgrade the operating system on all the nodes, if applicable. For instructions, see the upgrade paths for the operating system.

When the node starts, prevent LLT from starting automatically with one of the following methods. For example, . Or, change the /etc/default/llt file by setting LLT_START = 0. After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

- Enter:

  ```
  # mv /etc/llttab /etc/llttab.save
  ```

  OR:

- Set LLT_START = 0 in the `/etc/default/llt` file

Note: After upgrading the OS, change the LLT configuration to its original configuration.

Upgrading the SFCFSHA stack on the first subcluster

After step 1, you now navigate to the installer program and start it.

To upgrade the SFCFSHA stack on the first subcluster

1 **Note:** This procedure is based on an "in-place" upgrade path; that is, if the operating system is upgraded, the release will be the same, but only the path level will change. If you are moving from major operating system release to another, you must uninstall the SFCFSHA stack before you upgrade the operating system. After the operating system is upgraded, you must reinstall SFCFSHA.

On the first half of the cluster, upgrade SFCFSHA by using the installmr script. For example use the installmr script with Install Bundles as shown below:

```
# ./installmr -base_path /tmp/sfha6.0.1/ sys1
```

where <*sys1*> is the node on the first subcluster.

Note: Do not reboot the nodes in the first subcluster until you complete the Preparing the second subcluster procedure.

After the upgrade for first half of the cluster is complete, no GAB ports will be shown in `gabconfig -a` output.

2 From the opening Selection Menu, choose: G for **Upgrade a Product**.

Preparing the second subcluster

To prepare the second subcluster

1. On the second half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the application. [Downtime starts now.]
2. On the second half of the cluster, unmount the VxFS and CFS file systems that are not managed by VCS. Enter the following:

   ```
   # mount -p | grep vxfs
   ```

   Verify that no processes use the VxFS and CFS mount point. Enter the following:

   ```
   # fuser -c /mount_point
   ```

   Stop any processes using a VxFS and CFS mount point with the mechanism provided by the application.

   Unmount the VxFS and CFS file system. Enter the following:

   ```
   # umount /mount_point
   ```

3. On the second half of the cluster, unfreeze all the VCS service groups on all the nodes using the following commands:

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

4. On the second half of the cluster, bring all the VCS service groups offline, including CVM group. Enter the following:

   ```
   # hagrp -offline group_name -sys sys4
   ```

5. On the second half of the cluster, verify that the VCS service groups are offline. Enter the following:

   ```
   # hagrp -state group_name
   ```

6 Stop VCS on the second half of the cluster. Enter the following:

```
# hastop -local
```

7 On the second half of the cluster, stop the following SFCFSHA modules: GLM, ODM, GMS, VxFEN, GAB, and LLT. Enter the following:

For 5.1:

For Solaris 9:

```
# modunload -i [modid of vxglm]
# /etc/init.d/vxodm stop
# modunload -i [modid of vxgms]
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

For Solaris 10 and 11:

```
# modunload -i [modid of vxglm]
# /usr/sbin/svcadm -st disable vxodm
# modunload -i [modid of vxgms]
# /usr/sbin/svcadm -st disable vxfen
# /usr/sbin/svcadm -st disable gab
# /usr/sbin/svcadm –st disable llt
```

Or

You can enter the following to stop all these processes:

```
# ./installer/installsfcfs/installsfcfsha - stop
```

Note: You can use this command to stop the processes only if you have upgraded to product version 5.1 or later. You should use the manual steps if you have upgraded from 5.0 MP3.

For 5.0MP3:

```
# /etc/init.d/odm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

Activating the first subcluster

To activate the first subcluster

1. Start LLT and GAB:

```
# svcadm enable system/llt

# svcadm enable system/gab
```

2. Force GAB to form a cluster in the first half of the cluster.

```
# /sbin/gabconfig -x
```

   GAB port a appear in `gabconfig -a` command output.

3. If the product doesn't start automatically, on the first half of the cluster, start SFCFSHA:

```
# cd /opt/VRTS/install

# ./installsfcfsha<version> -start sys1 sys2
```

   Where <*version*> is the specific release version.

4. Unfreeze the nodes in the first half of the cluster. Enter the following:

```
# haconf -makerw
# hasys -unfreeze -persistent node_name
# haconf -dump -makero
```

5. For nodes that use Solaris 10, start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

6. On the first half of the cluster, bring the VCS service groups online. Enter the following:

```
# hagrp -online group_name -sys node_name
```

   After you bring the CVM service group ONLINE, all the GAB ports u, v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically. Only failover service groups need to be brought ONLINE manually.

7. Manually mount the VxFS and CFS file systems that are not managed by VCS. [Downtime ends now.]

Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting LLT_START = **0**.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system's documentation for more information.

Upgrading the second subcluster

After step 3 to step 5, upgrade the second subcluster.

To upgrade the second subcluster

1 Enter the following:

```
# ./installmr -base_path /tmp/sfha6.0.1/ node_name
```

2 From the opening Selection Menu, choose: G for **Upgrade a Product**.

Finishing the phased upgrade

To finish the phased upgrade

1 Verify that the cluster UUID on the nodes in the second subcluster is the same as the cluster UUID on the nodes in the first subcluster. Run the following command to display the cluster UUID:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -display nodename
```

If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

```
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -copy -from_sys \
sys1 -to_sys sys3 sys4
```

2 Start LLT and GAB.

```
# svcadm enable system/llt

# svcadm enable system/gab
```

3 Run the installer to start SFCFSHA on the second subcluster:

```
# ./opt/VRTS/install/installsfcfsha61 sys3 sys4
```

4 For nodes that use Solaris 10, start VCS in first half of the cluster:

```
# svcadm enable system/vcs
```

5 Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.

6 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

7 On the CVM master node, upgrade the CVM protocol. Enter the following:

```
# vxdctl upgrade
```

Performing a phased upgrade of SF Oracle RAC using Install Bundles

The phased upgrade methodology involves upgrading half of the nodes in the cluster at a time. The procedure involves the following tasks:

1 Performing pre-upgrade tasks on the first half of the cluster.

See "Step 1: Performing pre-upgrade tasks on the first half of the cluster" on page 91.

2 Upgrading the first half of the cluster.

Step 2: Upgrading the first half of the cluster

3 Performing pre-upgrade tasks on the second half of the cluster.

See "Step 3: Performing pre-upgrade tasks on the second half of the cluster" on page 96.

4 Performing post-upgrade tasks on the first half of the cluster.

Step 4: Performing post-upgrade tasks on the first half of the cluster

5 Upgrading the second half of the cluster.

Step 5: Upgrading the second half of the cluster

6 Performing post-upgrade tasks on the second half of the cluster.

Step 6: Performing post-upgrade tasks on the second half of the cluster

Step 1: Performing pre-upgrade tasks on the first half of the cluster

Perform the following pre-upgrade steps on the first half of the cluster.

To perform the pre-upgrade tasks on the first half of the cluster

1 Back up the following configuration files: `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/vxfenmodemain.cf, types.cf, CVMTypes.cf, CFSTypes.cf, SybaseTypes.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 \
/etc/VRTSvcs/conf/config/PrivNIC.cf.save
# cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
/etc/VRTSvcs/conf/config/MultiPrivNIC.cf.save
```

```
# 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/SybaseTypes.cf \
 /etc/VRTSvcs/conf/config/SybaseTypes.cf.save
```

The installer verifies that recent backups of configuration files in the VxVM private region are saved in `/etc/vx/cbr/bk`.

If not, the following warning message is displayed: `Warning: Backup /etc/vx/cbr/bk directory.`

2 Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

3 If you plan to continue using Storage Checkpoint or storage tiering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, complete the following preparatory step before migrating the SFDB repository database to 6.1.1.

4 Stop the applications configured under VCS. Stop the Oracle database:

- If the Oracle RAC instance is managed by VCS:

```
# hagrp -offline oracle_group -sys sys1
# hagrp -offline oracle_group -sys sys2
```

- If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the first half of the cluster and shut down the instances:
  For Oracle RAC 12c:

```
$ srvctl stop instance -db db_name \
-node node_name
```

  For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

  For Oracle RAC 11.2.0.1 and earlier versions:

```
$ 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:

```
# 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:
  For Oracle 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

  For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

6 Unmount the CFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the CFS mount point:

```
# mount | grep vxfs | grep cluster

# fuser -cu /mount_point
```

- Unmount the CFS file system:

```
# umount /mount_point
```

7 Stop the parallel service groups and switch over failover service groups on each of the nodes in the first half of the cluster:

```
# hastop -local -evacuate

# hastop -local
```

8 Unmount the VxFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS mount point:

```
# mount | grep vxfs

# fuser -cu /mount_point
```

- Unmount the VxFS file system:

```
# umount /mount_point
```

9 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

10 Verify that only ports a, b, d, and o are open:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   79c302 membership 0123
Port b gen   79c307 membership 0123
Port d gen   79c306 membership 0123
Port o gen   79c304 membership 0123
```

11 If you plan to upgrade the operating system, stop all ports.

For 5.1x and 6.0 versions:

```
# /opt/VRTS/install/installsfrac -stop sys1 sys2
```

If you are running version 5.0 MP3 and earlier, stop the ports manually as follows:

For Solaris 9 and Solaris 10:

```
# /etc/init.d/odm stop
# /etc/init.d/lmx stop
# /etc/init.d/vcsmm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# modinfo |grep lmx
# modunload -i module_no
# /etc/init.d/llt stop
```

Step 2: Upgrading the first half of the cluster

Perform the following steps to upgrade the first half of the cluster.

To upgrade the first half of the cluster

1 If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

```
# mv /etc/llttab /etc/llttab.save
```

If you are upgrading to Solaris 10 Update 10, apply the following Oracle patches: `144524-02` (SPARC); `144525-02` (x64). See the Oracle documentation for instructions.

2 Upgrade the operating system, if required.

For instructions, see the operating system documentation.

3 If you upgraded the operating system, restart the nodes:

```
# shutdown -g0 -y -i6
```

You may see some errors in the system log file when the nodes restart. This is because LLT is disabled. Ignore these messages.

```
svc.startd[7]: [ID 652011 daemon.warning] svc:/system/llt:default:
Method "/lib/svc/method/llt start" failed with exit status 2.
gab: [ID 438192 kern.notice] GAB WARNING V-15-1-20115
Port d registration failed, GAB not configured
```

4 Rename the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

6 On the first half of the cluster, upgrade SF Oracle RAC by using the `installmr` script. When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```
# cd /tmp/sfha6.0.5

# ./installmr -base_path /tmp/sfha6.0.1 sys1 sys2
```

Note: After you complete the upgrade of the first half of the cluster, no GAB ports will be shown in the output when you run the `gabconfig -a` command.

If you are upgrading from 5.0 releases that use regular license keys (not vxkeyless), then the installer shows the following warning. Select 'n' when prompted for additional liceses.

```
CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not
updated to 6.0 on sys1. It's recommended to upgrade to a 6.0 key.
CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not updated
to 6.0 on sys2. It's recommended to upgrade to a 6.0 key.

SFRAC is licensed on the systems
Do you wish to enter additional licenses? [y,n,q,b] (n) n
```

7 On all nodes of the subcluster, change the `/etc/default/llt` file to prevent LLT from starting automatically after reboot by setting the LLT_START attribute to 0:

```
LLT_START=0
```

8 Restart the nodes on the first subcluster:

```
# shutdown -g0 -y -i6
```

You may see some errors in the system log file when the nodes restart. This is because LLT is disabled. Ignore these messages.

```
svc.startd[7]: [ID 652011 daemon.warning] svc:/system/llt:default:
Method "/lib/svc/method/llt start" failed with exit status 2.
gab: [ID 438192 kern.notice] GAB WARNING V-15-1-20115
Port d registration failed, GAB not configured
```

Step 3: Performing pre-upgrade tasks on the second half of the cluster

Perform the following pre-upgrade steps on the second half of the cluster.

To perform the pre-upgrade tasks on the second half of the cluster

1 Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

Note: The downtime starts now.

2 If you plan to continue using Storage Checkpoint or storage tiering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, complete the following preparatory step before migrating the SFDB repository database to 6.1.1.

3 Stop all applications that are configured under VCS. Stop the Oracle database:

- If the Oracle RAC instance is managed by VCS:

```
# hagrp -offline oracle_group -sys sys3
# hagrp -offline oracle_group -sys sys4
```

- If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the second half of the cluster and shut down the instances:
  For Oracle RAC 12c:

  ```
  $ srvctl stop instance -db db_name \
  -node node_name
  ```

  For Oracle RAC 11.2.0.2 and later versions:

  ```
  $ srvctl stop instance -d db_name \
  -n node_name
  ```

  For Oracle RAC 11.2.0.1 and earlier versions:

  ```
  $ srvctl stop instance -d db_name \
  -i instance_name
  ```

4 Unmount the CFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

  ```
  # mount | grep vxfs | grep cluster

  # fuser -cu /mount_point
  ```

- Unmount the non-system VxFS file system:

  ```
  # umount /mount_point
  ```

5 Stop VCS on each of the nodes in the second half of the cluster:

```
# hastop -local
```

6 Unmount the VxFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

  ```
  # mount | grep vxfs

  # fuser -cu /mount_point
  ```

- Unmount the non-system VxFS file system:

```
# umount /mount_point
```

7 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

8 Stop all ports.

For 5.1x and 6.0 versions:

```
# /opt/VRTS/install/installsfrac -stop sys1 sys2
```

If you are running version 5.0 MP3 and earlier, stop the ports manually as follows:

For Solaris 9 and Solaris 10:

```
# /etc/init.d/odm stop
# /etc/init.d/lmx stop
# /etc/init.d/vcsmm stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# modinfo |grep lmx
# modunload -i module_no
# /etc/init.d/llt stop
```

Step 4: Performing post-upgrade tasks on the first half of the cluster

Perform the following post-upgrade steps on the first half of the cluster.

To perform the post-upgrade tasks on the first half of the cluster

1 Change `/etc/default/llt` to start LLT on the nodes by setting the LLT_START attribute to 1:

Run the following command to bring LLT online, if it is in maintenance mode:

```
# svcadm clear llt

LLT_START=1
```

2 On any one node on the first half of the cluster, force GAB to form a cluster.

```
# gabconfig -x
```

3 On the first half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install

# ./installsfrac<version> -start node1 node2
```

Where <*version*> is the specific release version.

4 On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.

5 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

6 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```
# hagrp -online oracle_group -sys node_name
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later verions:

```
$ srvctl start instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
-i instance_name
```

Note: The downtime ends here.

---

7 On the first half of the cluster, start all applications that are not managed by VCS. Use native application commands to start the applications.

Step 5: Upgrading the second half of the cluster

Perform the following steps to upgrade the second half of the cluster.

To upgrade the second half of the cluster

1. If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

   ```
   # mv /etc/llttab /etc/llttab.save
   ```

   If you are upgrading to Solaris 10 Update 10, apply the following Oracle patches: `144524-02` (SPARC); `144525-02` (x64). See the Oracle documentation for instructions.

2. Upgrade the operating system, if required.

   For instructions, see the operating system documentation.

3. If you upgraded the operating system, restart the nodes:

   ```
   # shutdown -g0 -y -i6
   ```

4. Rename the `/etc/llttab` file to its original name:

   ```
   # mv /etc/llttab.save /etc/llttab
   ```

5. Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

6 On the second half of the cluster, upgrade SF Oracle RAC with the *installmr* script.

When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```
# cd /tmp/sfha6.0.5

# ./installmr -base_path /tmp/sfha6.0.1 sys3 sys4
```

If you are upgrading from 5.0 releases that use regular license keys (not vxkeyless), then the installer shows the following warning. Select 'n' when prompted for additional liceses.

```
CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not
updated to 6.0 on sys1. It's recommended to upgrade to a 6.0 key.
CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not updated
to 6.0 on sys2. It's recommended to upgrade to a 6.0 key.

SFRAC is licensed on the systems
Do you wish to enter additional licenses? [y,n,q,b] (n) n
```

7 Restart the nodes:

```
# shutdown -g0 -y -i6
```

Step 6: Performing post-upgrade tasks on the second half of the cluster

Perform the following post-upgrade steps on the second half of the cluster.

To perform the post-upgrade tasks on the second half of the cluster

1 Manually mount the VxFS and CFS file systems that are not managed by VCS.

2 On the second half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install

# ./installsfrac<version> -start node3 node4
```

Where <*version*> is the specific release version.

3 Relink the SF Oracle RAC libraries with Oracle:

If you want the installer to relink the Oracle Database Binary, you can choose the option **Relink Oracle Database Binary** from the menu.

Complete the remaining tasks to finish the upgrade.

4 Upgrade VxVM disk group version.

For instructions, see the chapter "Post-upgrade tasks" in the *Veritas Storage Foundation for Oracle RAC 6.0.1 Installation and Configuration Guide*.

5 Upgrade disk layout version.

For instructions, see the chapter "Post-upgrade tasks" in the *Veritas Storage Foundation for Oracle RAC 6.0.1 Installation and Configuration Guide*.

6 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```
# hagrp -online oracle_group -sys node3
# hagrp -online oracle_group -sys node4
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
-node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
-i instance_name
```

7 - If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrp -modify oracle_group AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:
  For Oracle RAC 12c:

  ```
  $ srvctl modify database -db db_name -policy AUTOMATIC
  ```

  For Oracle RAC 10g and Oracle RAC 11g:

  ```
  $ srvctl modify database -d db_name -y AUTOMATIC
  ```

8 Start all applications that are not managed by VCS. Use native application commands to start the applications.

9 Set or change the product license level, if required.

10 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

11 Upgrade Oracle RAC, if required.

Note: Oracle RAC 11g Release 1 Clusterware is not supported. Make sure that you install Oracle RAC 11g Release 2 Grid Infrastructure or later in order to use the Oracle RAC 11g Release 1 database. All database versions starting from Oracle 10g Release 2 and later are supported.

For instructions, see the chapter *Upgrading Oracle RAC* 6.0.1 SF Oracle RAC Installation Guide.

Note: The procedure for Oracle RAC 12c is the same as that for Oracle RAC 11g Release 2.

Performing an automated upgrade using response files with Install Bundles

Depending on the installed product, use one of the following procedures:

Performing an automated upgrade of VCS, SFHA, or SFCFSHA using response files with Install Bundles

Typically, you can use the response file that the installer generates after you perform VCS, SFHA, or SFCFSHA upgrade with Install Bundles on one system to upgrade VCS, SFHA, or SFCFSHA on other systems. You can also create a response file using the `makeresponsefile` option of the installer.

To perform automated VCS, SFHA, or SFCFSHA upgrade

1. Make sure the systems where you want to upgrade VCS, SFHA, or SFCFSHA meet the upgrade requirements.
2. Make sure the pre-upgrade tasks are completed.
3. Copy the response file to one of the systems where you want to upgrade SFHA.
4. Edit the values of the response file variables as necessary.
5. Mount the product disc and navigate to the folder that contains the installation program.
6. Start the upgrade from the system to the `/tmp/sfha6.1.1` directory. For example:

   ```
   # ./installmr -responsefile /tmp/response_file
   ```

   Where /tmp/*response_file* is the response file's full path name.

Upgrading SF Oracle RAC using a response file

You can upgrade from SF Oracle RAC version 5.0 and later using a response file.

Perform the steps in the following procedure to upgrade to 6.1.1 using a response file.

To upgrade SF Oracle RAC using a response file

1. Upgrade the operating system, if required.

   For instructions, see the operating system documentation.

2. Create a response file using one of the available options.

   Note: Make sure that you replace the host names in the response file with the names of the systems that you plan to upgrade.

   For more information, refer to *Veritas Storage Foundation for Oracle RAC 6.0.1 Installation and Configuration Guide*.

3. Navigate to the product directory on the installation media that contains the SF Oracle RAC installation program.

4. Start the installation:

   ```
   # ./installmr -responsefile /tmp/response_file
   ```

   Where `/tmp/response_file` is the full path name of the response file.

5. Complete the post-upgrade steps.

   See the chapter "Performing post-upgrade tasks" in SF Oracle RAC 6.0.1 Installation Guide.

Performing rolling upgrade of SFHA Solutions using response files

Typically, you can use the response file that the installer generates after you perform SFHA Solutions upgrade on one system to upgrade SFHA Solutions on other systems.

You can also create a response file using the `makeresponsefile` option of the installer.

To perform automated SFHA Solutions rolling upgrade

1. Make sure the systems where you want to upgrade SFHA Solutions meet the upgrade requirements.

2. Make sure the pre-upgrade tasks are completed.

3. Copy the response file to the systems where you want to launch the installer.

   See the sample response file in the 6.1 Installation Guides.

4. Edit the values of the response file variables as necessary.

   See the response file variables in the 6.1 Installation Guides.

5 Mount the product disc and navigate to the folder that contains the installation program.

6 Start the upgrade from the system to which you copied the response file. For example:

```
# ./installmr -responsefile /tmp/response_file
```

Performing a rolling upgrade using Install Bundles

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

- Supported rolling upgrade paths
- Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles
- Performing a rolling upgrade of SF Oracle RAC with Install Bundles

Supported rolling upgrade paths

You can perform a rolling upgrade using the `installmr` script with Install Bundles.

Table 4-5 shows the versions for which you can perform a rolling upgrade to 6.1.1.

Table 4-5 Supported rolling upgrade paths for Install Bundles

Platform	version
Solaris 10 SPARC	5.1, 5.1RPs 5.1SP1, 5.1SP1RPs, 5.1SP1PR3 6.0, 6.0RP1 6.0.1, 6.0.3, 6.0.5
Solaris 11 SPARC	6.0PR1 6.0.1, 6.0.3, 6.0.5

Note: Before performing a rolling upgrade from version 5.1SP1RP3 to version 6.1.1, install patch VRTSvxfen-5.1SP1RP3P2. For downloading the patch, search VRTSvxfen-5.1SP1RP3P2 in Patch Lookup on the SORT website.

OS upgrade support during rolling upgrades on Solaris

If the upgrade scenario involves operating system upgrades, SFHA Solutions supports rolling upgrade for both major OS upgrades and minor OS upgrades.

For the following scenarios, use phased upgrades instead of rolling upgrades:

- Upgrades from versions prior to 6.0.3 on Sol11 SRU1 to 6.1.1 on Sol11 U1.

Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles

Before you start the rolling upgrade, make sure that Symantec Cluster Server (VCS) is running.

To perform a rolling upgrade

1. Complete the preparatory steps on the first sub-cluster.
2. Log in as superuser.
3. Change to the `/tmp/sfha6.1.1` directory.
4. Start the installer.

   ```
   # ./installmr -base_path /tmp/sfha6.1
   ```

5. From the menu, select `Upgrade` and from the sub menu, select `Rolling Upgrade`.
6. Enter one system of the cluster on which you would like to perform rolling upgrade.
7. The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type **y** to continue.
8. 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.
9. 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.
10. Review the end-user license agreement, and type **y** if you agree to its terms.
11. 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.

12 The installer prompts you to stop the applicable processes. Type **y** to continue.

The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.

13 The installer stops relevant processes, uninstalls old kernel packages, and installs the new packages.

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.

14 Complete the preparatory steps on the nodes that you have not yet upgraded.

15 The installer begins phase 1 of the upgrade on the remaining node or nodes. Type **y** to continue the rolling upgrade.

If the installer prompts to reboot nodes, reboot the nodes. Then, restart the installer.

The installer repeats step 8 through step 13.

For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

16 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.

17 The installer determines the remaining packages to upgrade. Press **Enter** to continue.

18 The installer stops Symantec 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.

19 A prompt message appears to ask if you would like to send the information about this installation to Symantec to help improve installation in the future?

Type **y** or **n** to help Symantec improve the installation.

20 If you have network connection to the Internet, the installer checks for updates.

If updates are discovered, you can apply them now.

21 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.

22 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Performing a rolling upgrade of SF Oracle RAC with Install Bundles

Use a rolling upgrade to upgrade Symantec Storage Foundation for Oracle RAC to the latest release with minimal application downtime.

Using the installmr script with Install Bundles, you can upgrade to 6.1.1 from releases earlier than 6.1.

- Preparing to perform a rolling upgrade to SF Oracle RAC 6.1.1
- Using Install Bundles to perform a rolling upgrade of SF Oracle RAC

Preparing to perform a rolling upgrade to SF Oracle RAC 6.1.1

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: Rolling upgrades of SF Oracle RAC 5.1 SP1 RP2 are affected by memory corruption issues. Customers are advised to upgrade to SF Oracle RAC 5.1 SP1 RP2 P1 patch to resolve the issue before performing a rolling upgrade. For more information, see the following Technote:

http://www.symantec.com/docs/TECH185862

To prepare to upgrade SF Oracle RAC

Perform the steps on the first subcluster.

1. Log in as superuser to one of the nodes in the subcluster.
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, CRSResource.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
   ```

3. Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

   If not, a warning message will be displayed after `installmr` upgrade prechecks..

   Warning: Backup `/etc/vx/cbr/bk` directory.

4. For Oracle RAC 10g, Oracle RAC 11g, and Oracle RAC 12c:

   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 oracle_group -sys node_name
     ```

   - If the database instances are not managed by VCS, then run the following on one node:
     For Oracle RAC 12c:

     ```
     # srvctl stop instance -db db_name -node node_name
     ```

     For Oracle RAC 11.2.0.2 and later versions:

     ```
     $ srvctl stop instance -d db_name \
     -n node_name
     ```

     For Oracle RAC 11.2.0.1 and earlier versions:

     ```
     $ 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:
For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

6 Unmount all the CFS file system which is not under VCS control.

```
# mount -v |grep vxfs | grep cluster

# 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
```

7 Take all the parallel VCS service groups offline on each of the nodes in the current subcluster:

```
# hagrp -offline grp_name -sys sys_name
```

8 Unmount all the VxFS file system which is not under VCS control.

```
# mount -v |grep vxfs

# fuser -c /mount_point

# umount /mount_point
```

9 If you plan to continue using the Storage Foundation for Databases (SFDB) tools, you must prepare to migrate the SFDB repository database before upgrading to SF Oracle RAC 6.1.1.

See "Pre-upgrade tasks for migrating the SFDB repository database" on page 46.

Using Install Bundles to perform a rolling upgrade of SF Oracle RAC

Before you start the rolling upgrade, make sure that Symantec Cluster Server (VCS) is running.

Note: SF Oracle RAC does not support rolling upgrades between major versions of the operating system, for example, from Solaris 9 to Solaris 10.

To perform a rolling upgrade

1 Complete the preparatory steps on the first sub-cluster.

See "Preparing to perform a rolling upgrade to SF Oracle RAC 6.1.1" on page 109.

2 If you are upgrading to Solaris 10 Update 10, apply the Oracle (Solaris) patches of `144524-02`. For instructions, see Oracle documentation.

Complete updates to the operating system, if required.

Note: Make sure that the operating system update you apply is supported by the existing version of SF Oracle RAC. If the existing version of SF Oracle RAC does not support the operating system update, first upgrade SF Oracle RAC to a version that supports the operating system update. For example, if you plan to apply Solaris 10 Update 9 to SF Oracle RAC version 5.1 running on Solaris 10 Update 6, you need to perform the following steps before proceeding with the steps in this procedure:

First, upgrade SF Oracle RAC to version 5.1 SP1RP1. For instructions, see the product documentation of that release.

Next, update the operating system.

For instructions, see the operating system documentation.

The nodes are restarted after the operating system update.

Restart the nodes again manually. Failing to perform this additional reboot prevents the upgrade from proceeding further.

```
# shutdown -g0 -y -i6
```

3 Log in as superuser.

4 Change to the `sfha6.1.1` directory.

5 Start the installmr script.

```
# ./installmr -base_path /tmp/sfha6.1/
```

6 From the menu, select `Upgrade` and from the sub menu, select `Rolling Upgrade`.

7 The installer suggests system names for the upgrade. Enter `Yes` to upgrade the suggested systems, or enter `No`, and then enter the name of any one system in the cluster on which you want to perform a rolling upgrade.

8 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type **y** to continue.

9 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.

See "Pre-upgrade tasks for migrating the SFDB repository database" on page 46.

10 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.

11 Review the end-user license agreement, and type **y** if you agree to its terms.

12 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.

13 The installer prompts you to stop the applicable processes. Type **y** to continue.

The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.

14 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.

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.

---

15 Perform the following steps if the subcluster has non-global zones.

- Take the zone service groups in the subcluster offline:

```
# hagrp -offline zone_group -sys sys_name
```

- From the global zone, run the following command for each non-global zone in the subcluster:

  ```
  # zoneadm -z zone_name attach -u
  ```

- Uninstall and install version 6.1 of the `VRTSodm` package on each global zone of the subcluster:

  ```
  # pkgrm VRTSodm
  # pkgadd -d vrtsodmpkg_path
  ```

- Boot each non-global zone:

  ```
  # zoneadm -z zone_name boot
  ```

- Log in to each non-global zone of the subcluster and run the following command:

  ```
  # svcadm enable -r vxodm
  ```

- Halt each non-global zone:

  ```
  # zoneadm -z zone_name halt
  ```

- Bring the zone service group on the subcluster online:

  ```
  # hagrp -online zone_group -sys sys_name
  ```

16 Manually mount the VxFS and CFS file systems that are not managed by VCS.

17 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

Note: If the subcluster has non-global zones, you need to relink only the ODM library.

---

18 If the boot disk is encapsulated, the installer strongly recommends a reboot of the nodes. Reboot the nodes as prompted by the installer.

Note: Before you reboot the nodes, ensure that the boot device is set to the disk containing the upgraded version of the product.

```
# eeprom
```

---

19 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:
  For Oracle RAC 10g and Oracle RAC 11g:

  ```
  $ srvctl start database -d db_name
  ```

  For Oracle RAC 12c:

  ```
  $ srvctl start database -db db_name
  ```

20 Start all applications that are not managed by VCS. Use native application commands to start the applications.

21 Complete the preparatory steps on the nodes that you have not yet upgraded.

22 Complete updates to the operating system, if required, on the nodes that you have not yet upgraded. For instructions, see the operating system documentation.

The nodes are restarted after the operating system update.

Restart the nodes again manually. Failing to perform this additional reboot prevents the upgrade from proceeding further.

```
# shutdown -g0 -y -i6
```

23 If the nodes are rebooted, restart the installer and continue phase-1 for second sub-cluster.Type **y** to continue the rolling upgrade.

The installer repeats step 15 through step 20.

For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

This completes phase 1 of the upgrade.

24 ■ 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:
For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

25 Phase 2 of the rolling upgrade begins here. This phase includes downtime for the VCS engine (HAD), which does not include application downtime.

26 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

27 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.

28 Phase 2 of the upgrade begins here. This phase includes downtime for the VCS engine (HAD), which does not include application downtime. Type **y** to continue.

29 The installer determines the remaining packages to upgrade. Press **Enter** to continue.

30 The installer stops Symantec 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.

31 When the following message appears, type **y** or **n** to help Symantec improve the installation:

```
Would you like to send the information about this installation to
Symantec to help improve installation in the future?
```

32 If you have network connection to the Internet, the installer checks for updates.

If updates are discovered, you can apply them now.

33 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.

34 Upgrade Oracle RAC to the supported version.

For information on Oracle RAC support, see:

http://www.symantec.com/docs/DOC5081

For instructions, see the chapter *Upgrading Oracle RAC* in *SF Oracle RAC 6.1 Installation Guide*.

Note: The procedure for Oracle RAC 12c is the same with that for Oracle RAC 11g Release 2.

---

35 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Upgrading using Live Upgrade with Install Bundles on Solaris 10 systems

You can use Live Upgrade on Solaris 10 systems for upgrading VCS, SFHA, SFCFSHA, and SF Oracle RAC.

Usages of the vxlustart option

Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot environment for the upgrade. The `vxlustart` script is in the `/tmp/sfha6.1.1/scripts` directory.

Table 4-6 Usages of the vxlustart option

vxlustart option	Usage
-V	Lists the commands to be executed during the upgrade process without executing them.
-v	Indicates verbose, print commands before executing them.
-f	Forces the vtoc creation on the disk.
-Y	Indicates a default yes with no questions asked.
-m	Uses the already existing vtoc on the disk.
-D	Prints with debug option on, and is for debugging.
-U	Specifies that only the Storage Foundation products are upgraded.
-g	Specifies the DG to which the rootdisk belongs. Optional.
-d	Indicates the name of the alternate boot disk **c#t#d#s2** on which you intend to upgrade. The default disk is **mirrordisk**.

Table 4-6 Usages of the vxlustart option *(continued)*

vxlustart option	Usage
-u	Specifies the operating system version for the upgrade on the alternate boot disk. For example, use `5.10` for Solaris 10. If you want to upgrade only SF products, specify the current OS version.
-F	Specifies the rootdisk's file system, where the default is `ufs`.
-s	Specifies the path to the Solaris image. It can be a network/directory path. If the installation uses the CD, this option must not be specified. See *Solaris Live Upgrade installation guide* for more information about the path.
-r	If the machine crash/reboot before vxlufinish, you can remount the alternate disk using this option.
-k	Specifies the location of file containing auto-registration information. This file is required by luupgrade(1M) for OS upgrade to Solaris 10 9/10 or a later release.
-x	Excludes file from newly created BE. (`lucreate -x` option)
-X	Excludes file list from newly created BE. (`lucreate -f` option)
-i	Includes file from newly created BE. (`lucreate -y` option)
-I	Includes file list from newly created BE. (`lucreate -Y` option)
-z	Filters file list from newly created BE. (`lucreate -z` option)
-w	Specifies additional mount points. (`lucreate -m` option)
-W	Specifies additional mount points in a file (`lucreate -M` option)

Upgrading VCS using Live Upgrade on Solaris 10

Before you upgrade VCS using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1. Make sure that the VCS installation media and the operating system installation images are available and on hand.
2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.

   If the primary boot disk is mirrored, you need to break off the mirror for the alternate boot disk.
3. Before you perform the Live Upgrade, take offline any services that involve non-root file systems. This prevents file systems from being copied to the alternate boot environment that could potentially cause a root file system to run out of space.
4. If the nodes to be upgraded are on Solaris 9, on the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
5. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.

     Note: While you can perform Live Upgrade in the presence of branded zones, they must be halted, and the branded zones themselves are not upgraded.

6 Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot disk for the upgrade.

Note: The upgrade procedure assumes that the SFHA stack is already installed when the `vxlustart` and `vxlufinish` scripts are run.

To preview the commands, specify the `vxlustart` script with the `-v` option.

Symantec recommends that you preview the commands to ensure there are no problems before beginning the Live Upgrade process.

The `vxlustart` script is located in the `/tmp/sfha6.1.1/scripts` directory.

```
# cd /tmp/sfha6.1.1/scripts
```

```
# ./vxlustart -V -u targetos_version -s osimage_path \
-d diskname -k auto_regfile_path
```

For usages of the vxlustart option, see Usages of the vxlustart option.

For example, to preview the commands to upgrade the Symantec products only:

```
# ./vxlustart -V -u 5.10 -d disk_name
```

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6
```

7 If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

Upgrading VCS and Solaris using Live Upgrade with Install Bundles

You can use the Veritas product installer to upgrade VCS as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade VCS on all the nodes in the cluster. The program uninstalls the existing version of VCS on the alternate boot disk during the process.

At the end of the process the following occurs:

- VCS 6.1.1 is installed on the alternate boot disk.

To perform Live Upgrade of VCS using the installer

1. Insert the product disc with VCS 6.1.1 or access your copy of the software on the network.
2. `# ./installmr -base_path /tmp/sfha6.1/ -rootpath /altroot.5.10`
3. Enter the names of the nodes that you want to upgrade to VCS 6.1.1.

   The installer displays the list of packages to be installed or upgraded on the nodes.
4. Press **Return** to continue with the installation.

   During Live Upgrade, if the OS of the alternate boot disk is upgraded, the installer will not update the VCS configurations for Oracle, Netlsnr, and Sybase resources. If cluster configurations include these resources, you will be prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate boot disks.
5. Verify that the version of the Symantec packages on the alternate boot disk is 6.1.1.

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

   For example:

   `# pkginfo -R /altroot.5.10 -l VRTSvcs`
6. Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

To complete the Live Upgrade

1 Complete the Live upgrade process. Enter the following command on all nodes in the cluster.

```
# ./vxlufinish -u target_os_version
Live Upgrade finish on the Solaris release <5.10>
```

2 If the system crashes or reboots before Live Upgrade completes successfully, you can remount the alternate disk using the following command:

```
# ./vxlustart -r -u target_os_version
```

Then, rerun the `vcslufinish` command from step 1

```
# ./vxlufinish -u target_os_version
```

Note: The `vxlustart` script and the `vxlufinish` script are located in the `/tmp/sfha6.1.1/scripts` directory.

---

3 ---

Note: Do not use the `reboot`, `halt`, or `uadmin` commands to reboot the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate boot environment.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

```
# shutdown -g0 -y -i6
```

4 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Upgrading SFHA using Live Upgrade on Solaris 10

Before you upgrade SFHA using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1. Make sure that the SFHA installation media and the operating system installation images are available and on hand.
2. If the nodes to be upgraded are on Solaris 9, on the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
3. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.

   Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at */cdrom/solaris_release*/Tools/Installers/liveupgrade20. If scripting, you can use:

   ```
   # /cdrom/solaris_release/Tools/Installers/liveupgrade20 \
   -nodisplay -noconsole
   ```

4. If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

Upgrading SFHA and Solaris using Live Upgrade

Perform the Live Upgrade manually or use the installer. For SFHA, the nodes do not form a cluster until all of the nodes are upgraded to SFHA 6.1.1. At the end of

the Live Upgrade of the last node, all the nodes must boot from the alternate boot environment and join the cluster.

Upgrading SFHA using Live Upgrade involves the following steps:

- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 126.
- Upgrade SFHA using the installer.
  See "Upgrading SFHA using the installer for a Live Upgrade" on page 129.
- Switch the alternate boot environment to be the new primary.
  See "Completing the Live Upgrade " on page 130.
- Verify Live Upgrade of SFHA.
  See "Verifying Live Upgrade of SFHA" on page 132.

Creating a new boot environment on the alternate boot disk

Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot environment for the upgrade.

```
# cd /cdrom/scripts
```

For usages of the vxlustart option, see Usages of the vxlustart option.

If the `-U` option is specified, you can omit the `-s` option. The operating system is cloned from the primary boot disk.

Symantec recommends that you preview the commands with `-V` option to ensure there are no problems before beginning the Live Upgrade process. The `vxlustart` script is located on the distribution media, in the scripts directory.

For example, to preview the commands to upgrade only the Symantec product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s2
```

In the procedure examples, the primary or current boot environment resides on*Disk0 (c0t0d0s2)* and the alternate or inactive boot environment resides on *Disk1 (c0t1d0s2)*.

Note: This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

To create a new boot environment on the alternate boot disk

Perform the steps in this procedure on each node in the cluster.

1 View the list of VxVM disks on which you want to create the new boot environment.

```
# vxdisk list
```

2 Before you upgrade, make sure that you exclude the file system mount points on a shared storage that applications use from getting copied to the new boot environment. To prevent these shared mount points from being copied to the new boot environment, create a temporary file containing the file system mountpoints that need to be excluded.

```
# cat /var/tmp/file_list
- /ora_mnt
- /sap_mnt
```

where `/var/tmp/file_list` is a temporary file that contains the list of mount points to be excluded from the new boot environment. The items in the file list are preceded either by a '+' or '-' symbol.

The '+' symbol indicates that the mount point is included in the new boot environment.

The '-' symbol indicates that the mount point is excluded from the new boot.

Apart from file system mount points, you may choose to include or exclude other files.

If you have non-global zone in running state in the current boot environment and zone root path is on a VxVM, create another volume of same or more size for each zone root in alternate boot environment path using vxvm commands.

3 Run one of the following commands to create the alternate boot environment:

For example:

To upgrade the operating system:

```
# ./vxlustart -v -u 5.10 -s /mnt/sol10u9 -d
c0t1d0s2 -z /var/tmp/file_list
```

where `/mnt/sol10u9` is the path to the operating system image that contains the `.cdtoc` file.

To clone the operating system of current boot environment:

```
# ./vxlustart -v -u 5.10 -U -d c0t1d0s2 -z /var/tmp/file_list
```

If you have non-global zone with zone root path on VxVM, then to upgrade the OS:

```
# ./vxlustart -v -u 5.10 -U -d c0t1d0s2 -z
/var/tmp/file_list -w /zone1-rootpath:/dev/vx/dsk/rootpathdg_alt/
rootpathvol_alt:vxfs
```

Where `zone1-rootpath` is root path of zone in present boot environment.

4 Update the permissions, user name, and group name of the mount points (created on the ABE) to match that of the existing directories on the primary boot environment.

5 If zone root path is on VxVM, update the`/altroot.5.10/etc/VRTSvcs/conf/config/main.cf` file with new block device created in step 2 for all zones to reflect the ABE zone root paths.

6 Review the output of `df` commands and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

If you need to remount, run the command:

```
# vxlustart -r -u targetos_version -d disk_name
```

7 After the alternate boot disk is created and mounted on */altroot.5.10*, install any operating system patches or packages on the alternate boot disk that are required for the Symantec product installation:

```
# pkgadd -R /altroot.5.10 -d pkg_dir
```

8 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Upgrading SFHA using the installer for a Live Upgrade

You can use the Veritas product installer to upgrade SFHA as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade SFHA on all the nodes in the cluster. The program uninstalls the existing version of SFHA on the alternate boot disk during the process.

At the end of the process the following occurs:

- SFHA 6.1.1 is installed on the alternate boot disk.

To perform Live Upgrade of SFHA using the installer

1 Insert the product disc with SFHA 6.1.1 or access your copy of the software on the network.

2 Run the installer script specifying the root path as the alternate boot disk:

```
# ./installmr -rootpath /altroot.5.10 -base_path /tmp/sfha6.1
```

3 Enter the names of the nodes that you want to upgrade to SFHA 6.1.1.

The installer displays the list of packages to be installed or upgraded on the nodes.

4 Press **Return** to continue with the installation.

During Live Upgrade, if the OS of the alternate boot disk is upgraded, the installer will not update the VCS configurations for Oracle, Netlsnr, and Sybase

resources. If cluster configurations include these resources, you will be prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate boot disks.

5 Verify that the version of the Symantec packages on the alternate boot disk is 6.1.1.

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

Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

Completing the Live Upgrade

At the end of the process:

- If the original primary boot disk was encapsulated, the alternate boot disk is encapsulated.
- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.

To complete the Live Upgrade

1 Complete the Live upgrade process using one of the following commands. You must enter the command on all nodes in the cluster.

If the primary root disk is not encapsulated, run the following command:

```
# ./vxlufinish -u target_os_version
Live Upgrade finish on the Solaris release <5.10>
```

If the primary root disk is encapsulated by VxVM, run the following command:

```
# ./vxlufinish -u target_os_version -g diskgroup
Live Upgrade finish on the Solaris release <5.10>
```

The Live Upgrade process encapsulates the alternate root disk if the primary root disk was encapsulated.

Note: The `vxlustart` script and the `vxlufinish` script are located in the `/tmp/sfha6.1.1/scripts` directory.

---

2 If the system crashes or reboots before Live Upgrade completes successfully, you can remount the alternate disk using the following command:

```
# ./vxlustart -r -u target_os_version
```

Then, rerun the vxlufinish command from step 1

```
# ./vxlufinish -u target_os_version
```

3 **Note:** Do not use the `reboot`, `halt`, or `uadmin` commands to reboot the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate boot environment.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

```
# shutdown -g0 -y -i6
```

4 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Verifying Live Upgrade of SFHA

To ensure that Live Upgrade has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

To verify that Live Upgrade completed successfully

1 Verify that the alternate boot environment is active.

```
# lustatus
```

If the alternate boot environment is not active, you can revert to the primary boot environment.

2 In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

3 Perform other verification as required to ensure that the new boot environment is configured correctly. The non-global zones must be brought to configured state and then attached with `-U` option so that packages are upgraded inside the non-global zone also.

Upgrading SFCFSHA using Live Upgrade on Solaris 10

Before you upgrade SFCFSHA using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1. Make sure that the SFCFSHA installation media and the operating system installation images are available and on hand.
2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.

   If the primary boot disk is mirrored, you need to break off the mirror for the alternate boot disk.
3. Before you perform the Live Upgrade, take offline any services that involve non-root file systems. This prevents file systems from being copied to the alternate boot environment that could potentially cause a root file system to run out of space.
4. If the nodes to be upgraded are on Solaris 9, on the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
5. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.
     Solaris 10 zones or Branded zones also requires: SUNWluzone package.

     Note: While you can perform Live Upgrade in the presence of branded zones, they must be halted, and the branded zones themselves are not upgraded.

Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at */cdrom/solaris_release*/Tools/Installers/liveupgrade20. If scripting, you can use:

```
# /cdrom/solaris_release/Tools/Installers/liveupgrade20 \
-nodisplay -noconsole
```

6 Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot disk for the upgrade.

To preview the commands, specify the `vxlustart` script with the `-V` option.

Symantec recommends that you preview the commands to ensure there are no problems before beginning the Live Upgrade process.

Note: The `vxlustart` script and the `vxlufinish` script are located in the `/tmp/sfha6.1.1/scripts` directory.

```
# cd /tmp/sfha6.1.1/scripts
```

```
# ./vxlustart -V -u targetos_version -s osimage_path -d diskname
```

For usages of the vxlustart option, see Usages of the vxlustart option.

For example, to preview the commands to upgrade only the Symantec product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s0
```

Note: This command prompts you to compare the patches that are installed on the image with the patches installed on the primary boot disk. If any patches are missing from the new operating system's image, note the patch numbers. To ensure the alternate boot disk is the same as the primary boot disk, you will need to install these patches on the alternate boot disk.

---

7 If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

Upgrading SFCFSHA and Solaris using Live Upgrade

Upgrading SFCFSHA using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 135.
- Upgrade to SFCFSHA 6.1.1 on the alternate boot environment using the installer.

  To upgrade SFCFSHA using the installer, refer to the following procedure:
  - See "Upgrading SFCFSHA using the installer for a Live Upgrade" on page 137.
- Switch the alternate boot environment to be the new primary.
  See "Completing the Live Upgrade " on page 138.
- Verify Live Upgrade of SFCFSHA.
  See "Verifying Live Upgrade of SFCFSHA" on page 140.

Creating a new boot environment on the alternate boot disk

Run the `vxlustart` command on each node in the cluster to create a new boot environment on the alternate boot disk.

For usages of the vxlustart option, see Usages of the vxlustart option.

If the `-U` option is specified, you can omit the `-s` option. The operating system is cloned from the primary boot disk.

Symantec recommends that you preview the commands with `-V` option to ensure there are no problems before beginning the Live Upgrade process. The `vxlustart` script is located on the distribution media, in the scripts directory.

For example, to preview the commands to upgrade only the Symantec product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s2
```

In the procedure examples, the primary or current boot environment resides on*Disk0 (c0t0d0s2)* and the alternate or inactive boot environment resides on *Disk1 (c0t1d0s2)*.

Note: This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

To create a new boot environment on the alternate boot disk

Perform the steps in this procedure on each node in the cluster.

1 Navigate to the install media for the Symantec products:

```
# cd /tmp/sfha6.1.1/scripts
```

2 View the list of VxVM disks on which you want to create the new boot environment.

```
# vxdisk list
```

3 Run one of the following commands to perform the upgrade:

To upgrade the operating system, by itself or together with upgrading the Symantec products:

```
# ./vxlustart -v -u targetos_version \
-s osimage_path -d disk_name
```

where *targetos_version* is the version of the operating system

osimage_path is the full path to the operating system image

disk_name is the name of the disk as displayed in the output of step 2.

To upgrade the Symantec product only:

```
# ./vxlustart -v -u 5.10 -U -d disk_name
```

The options to the `vxlustart` command are listed in the preupgrade section.

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

4 Review the output of `df` commands and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

If you need to remount, run the command:

```
# vxlustart -r -u targetos_version -d disk_name
```

5 After the alternate boot disk is created and mounted on */altroot.5.10*, install any operating system patches or packages on the alternate boot disk that are required for the Symantec product installation:

```
# pkgadd -R /altroot.5.10 -d pkg_dir
```

Upgrading SFCFSHA using the installer for a Live Upgrade

You can use the Veritas product installer to upgrade SFCFSHA as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade SFCFSHA on all the nodes in the cluster. The program uninstalls the existing version of SFCFSHA on the alternate boot disk during the process.

At the end of the process the following occurs:

- SFCFSHA 6.1.1 is installed on the alternate boot disk.

To perform Live Upgrade of SFCFSHA using the installer

1 Insert the product disc with SFCFSHA 6.1.1 or access your copy of the software on the network.

2 Run the installer script specifying the root path as the alternate boot disk, enter the following:

```
# ./installmr -upgrade -rootpath /altroot.5.10 -base_path /tmp/sfha6.1
```

3 Enter the names of the nodes that you want to upgrade to SFCFSHA 6.1.1.

Note: Make sure that the installed version of VxFS uses the disk layout version 6 or later. If you are on a previous disk layout version, upgrade the version before you proceed with the SFCFSHA installation.

The installer displays the list of packages to be installed or upgraded on the nodes.

4 Press **Return** to continue with the installation.

During Live Upgrade, if the OS of the alternate boot disk is upgraded, the installer will not update the VCS configurations for Oracle, Netlsnr, and Sybase resources. If cluster configurations include these resources, you will be prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate boot disks.

5 Verify that the version of the Symantec packages on the alternate boot disk is 6.1.1.

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

For example:

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

Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

Completing the Live Upgrade

At the end of the process:

- If the original primary boot disk was encapsulated, the alternate boot disk is encapsulated.
- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.

To complete the Live Upgrade

1 Complete the Live upgrade process using one of the following commands. You must enter the command on all nodes in the cluster.

If the primary root disk is not encapsulated, run the following command:

```
# ./vxlufinish -u target_os_version
Live Upgrade finish on the Solaris release <5.10>
```

If the primary root disk is encapsulated by VxVM, run the following command:

```
# ./vxlufinish -u target_os_version -g diskgroup
Live Upgrade finish on the Solaris release <5.10>
```

The Live Upgrade process encapsulates the alternate root disk if the primary root disk was encapsulated.

2 If the system crashes or reboots before Live Upgrade completes successfully, you can remount the alternate disk using the following command:

```
# ./vxlustart -r -u target_os_version
```

Then, rerun the vxlufinish command from step 1

```
# ./vxlufinish -u target_os_version
```

3 If you are upgrading VVR, run the `vvr_upgrade_lu_start` command.

Note: Only run the `vvr_upgrade_lu_start` command when you are ready to reboot the nodes and switch over to the alternate boot environment.

4

Note: Do not use the `reboot`, `halt`, or `uadmin` commands to reboot the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate boot environment.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

```
# shutdown -g0 -y -i6
```

5 After the alternate boot environment is activated, you can switch boot environments. If the root disk is encapsulated, refer to the procedure to switch the boot environments manually.

6 After the upgrade, perform any required post-upgrade tasks such as upgrading the disk group.

7 After the objects are recovered, and the disk group version is upgraded (if desired), run the `vvr_upgrade_lu_finish` script.

8 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

   For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Verifying Live Upgrade of SFCFSHA

To ensure that Live Upgrade has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

To verify that Live Upgrade completed successfully

1 Verify that the alternate boot environment is active.

```
# lustatus
```

   If the alternate boot environment is not active, you can revert to the primary boot environment.

2 In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

3 Perform other verification as required to ensure that the new boot environment is configured correctly. The non-global zones must be brought to configured state and then attached with `-U` option so that packages are upgraded inside the non-global zone also.

4 In a zone environment, verify the zone configuration.

Upgrading SF Oracle RAC using Live Upgrade on Solaris 10

- Upgrading Solaris only using Live Upgrade

Before you upgrade SF Oracle RAC using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1. Make sure that the SF Oracle RAC installation media and the operating system installation images are available and on hand.
2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.

   If the primary boot disk is mirrored, you need to break off the mirror for the alternate boot disk.
3. If the nodes to be upgraded are on Solaris 9, on the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
4. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:

   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
     All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.

   Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at */cdrom/solaris_release*/Tools/Installers/liveupgrade20. If scripting, you can use:

   ```
   # /cdrom/solaris_release/Tools/Installers/liveupgrade20 \
   -nodisplay -noconsole
   ```

   After you install the packages, install the latest Live Upgrade patch. For more information on required packages and patches, see the Oracle Metalink document: 1004881.1 or visit the following site:

   https://support.oracle.com/

5 Symantec provides the `vxlustart` script that runs a series of commands to create the alternate boot disk for the upgrade.

To preview the commands, specify the `vxlustart` script with the `-V` option.

Symantec recommends that you preview the commands to ensure there are no problems before beginning the Live Upgrade process.

Note: The `vxlustart` script and the `vxlufinish` script are located in the `/tmp/sfha6.1.1/scripts` directory.

```
# cd /tmp/sfha6.1.1/scripts
```

```
# ./vxlustart -V -u targetos_version -s osimage_path -d diskname
```

For usages of the vxlustart option, see Usages of the vxlustart option.

For example, to preview the commands to upgrade only the Symantec product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s0
```

Note: This command prompts you to compare the patches that are installed on the image with the patches installed on the primary boot disk. If any patches are missing from the new operating system's image, note the patch numbers. To ensure the alternate boot disk is the same as the primary boot disk, you will need to install these patches on the alternate boot disk.

---

6 If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

Upgrading the operating system and SF Oracle RAC using Live Upgrade

Perform the following steps to upgrade both the operating system and SF Oracle RAC using Live Upgrade.

To upgrade the operating system and SF Oracle RAC using Live Upgrade

1 Prepare to upgrade using Solaris Live Upgrade.

See "Before you upgrade SF Oracle RAC using Solaris Live Upgrade" on page 141.

2 Create a new boot environment on the alternate boot disk.

See "Creating a new boot environment on the alternate boot disk" on page 143.

3 Upgrade SF Oracle RAC using the installer or manually.

See "Upgrading SF Oracle RAC using the installer for a Live Upgrade" on page 150.

4 Complete the Live Upgrade.

See "Completing the Live Upgrade" on page 151.

5 Verify Live Upgrade of SF Oracle RAC.

See "Verifying Live Upgrade of SF Oracle RAC 6.1.1" on page 154.

Upgrading SF Oracle RAC only using Live Upgrade

Perform the following steps to upgrade only SF Oracle RAC using Live Upgrade.

To upgrade only SF Oracle RAC using Live Upgrade

1 Prepare to upgrade using Solaris Live Upgrade.

See "Before you upgrade SF Oracle RAC using Solaris Live Upgrade" on page 141.

2 Create a new boot environment on the alternate boot disk.

See "Creating a new boot environment on the alternate boot disk" on page 143.

3 Upgrade SF Oracle RAC using the installer or manually.

See "Upgrading SF Oracle RAC using the installer for a Live Upgrade" on page 150.

4 Complete the Live Upgrade.

See "Completing the Live Upgrade" on page 151.

5 Verify Live Upgrade of SF Oracle RAC.

See "Verifying Live Upgrade of SF Oracle RAC 6.1.1" on page 154.

Creating a new boot environment on the alternate boot disk

Run the `vxlustart` command on each node in the cluster to create a new boot environment on the alternate boot disk.

For usages of the vxlustart option, see Usages of the vxlustart option.

If the `-U` option is specified, you can omit the `-s` option. The operating system is cloned from the primary boot disk.

Symantec recommends that you preview the commands with `-V` option to ensure there are no problems before beginning the Live Upgrade process. The `vxlustart` script is located on the distribution media, in the scripts directory.

For example, to preview the commands to upgrade only the Symantec product:

```
# ./vxlustart -V -u 5.10 -U -d disk_name
```

For example, to preview the commands for an upgrade to Solaris 10 update 6:

```
# ./vxlustart -V -u 5.10 -s /mnt/Solaris_10u6 -d c0t1d0s2
```

In the procedure examples, the primary or current boot environment resides on*Disk0 (c0t0d0s2)* and the alternate or inactive boot environment resides on *Disk1 (c0t1d0s2)*.

Note: This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

To create a new boot environment on the alternate boot disk

Perform the steps in this procedure on each node in the cluster.

1 Navigate to the install media for the Symantec products:

```
# cd /tmp/sfha6.1.1/scripts
```

2 View the list of VxVM disks on which you want to create the new boot environment.

```
# vxdisk list
```

3 Before you upgrade, make sure that you exclude the file system mount points on a shared storage that applications use from getting copied to the new boot environment. To prevent these shared mount points from being copied to the new boot environment, create a temporary file containing the file system mountpoints that need to be excluded.

```
# cat /var/tmp/file_list
- /ora_mnt
- /sap_mnt
```

where `/var/tmp/file_list` is a temporary file that contains the list of mount points to be excluded from the new boot environment. The items in the file list are preceded either by a '+' or '-' symbol.

The '+' symbol indicates that the mount point is included in the new boot environment.

The '-' symbol indicates that the mount point is excluded from the new boot.

Apart from file system mount points, you may choose to include or exclude other files.

If you have non-global zone in running state in the current boot environment and zone root path is on a VxVM, create another volume of same or more size for each zone root in alternate boot environment path using vxvm commands.

4 Run one of the following commands to create the alternate boot environment:

For example:

To upgrade the operating system:

```
# ./vxlustart -v -u 5.10 -s /mnt/sol10u9 -d
c0t1d0s2 -z /var/tmp/file_list
```

where `/mnt/sol10u9` is the path to the operating system image that contains the `.cdtoc` file.

To clone the operating system of current boot environment:

```
# ./vxlustart -v -u 5.10 -U -d c0t1d0s2 -z /var/tmp/file_list
```

If you have non-global zone with zone root path on VxVM, then to upgrade the OS:

```
# ./vxlustart -v -u 5.10 -U -d c0t1d0s2 -z
/var/tmp/file_list -w /zone1-rootpath:/dev/vx/dsk/rootpathdg_alt/
rootpathvol_alt:vxfs
```

Where `zone1-rootpath` is root path of zone in present boot environment.

5 Update the permissions, user name, and group name of the mount points (created on the ABE) to match that of the existing directories on the primary boot environment.

6 If zone root path is on VxVM, update the`/altroot.5.10/etc/VRTSvcs/conf/config/main.cf` file with new block device created in step 2 for all zones to reflect the ABE zone root paths.

7 Run one of the following commands to perform the upgrade:

To upgrade the operating system, by itself or together with upgrading the Symantec products:

```
# ./vxlustart -v -u targetos_version \
-s osimage_path -d disk_name
```

where *targetos_version* is the version of the operating system

osimage_path is the full path to the operating system image

disk_name is the name of the disk as displayed in the output of step 2.

To upgrade the Symantec product only:

```
# ./vxlustart -v -u 5.10 -U -d disk_name
```

The options to the `vxlustart` command are listed in the preupgrade section.

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

8 Before you upgrade, make sure that you exclude the CFS mount points that are used by the database or applications from being copied to the new boot environment. During Live Upgrade, the `vxlustart` utility fails to recognize the CFS mount points that are configured under VCS. As a result, the data in the Oracle database and Oracle Clusterware mount points that are configured as CFS mount points under VCS get copied into the local file system of the alternate boot environment. To prevent these shared mount points from being copied to the new boot environment, you need to identify and exclude these mount points as follows:

```
# for i in `hatype -resources CFSMount`; \
do hares -display $i -attribute MountPoint | awk ' \
NR != 1 { print "-", $4}'; done > /var/tmp/file_list
# cat /var/tmp/file_list
- /ocrvote
- /oradata
- /oradata1
```

where */var/tmp/file_list* is a temporary file that contains the list of CFS mount points to be excluded from the new boot environment and */ocrvote, /oradata, and /oradata1* are CFS mount points that are used by the database or applications. The items in the file list are preceded either by a + or - symbol. The + symbol indicates that the mount point is included in the new boot environment and the - symbol indicates that the mount point is excluded from the new boot environment. Apart from CFS mount points, you may choose to include or exclude other files.

9 Run one of the following commands to create the alternate boot environment:

For example:

To upgrade both the operating system and the Symantec product:

```
# ./vxlustart -v -u 5.10 -s /mnt/sol10u9 -d c0t1d0s2 \
-z /var/tmp/file_list
```

where */mnt/sol10u9* is the path to the operating system image that contains the `.cdtoc` file.

To only upgrade the Symantec product:

```
# ./vxlustart -v -u 5.10 -U -d c0t1d0s2 -z /var/tmp/file_list
```

10 On each node, run one of the following commands:

To upgrade the operating system, by itself or together with upgrading the Symantec products:

```
# ./vxlustart -v -u targetos_version \
-s osimage_path -d disk_name
```

To upgrade the Symantec products only:

```
# ./vxlustart -v -u 5.10 -d disk_name
```

Refer to the step on command options.

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

For example, to upgrade the Symantec products only:

```
# ./vxlustart -v -u 5.10
```

11 Create the mount points manually on the alternate boot environment as follows:

```
# for i in `cat /var/tmp/file_list` ; \
do mkdir -p /altroot.5.10/$i; done
```

12 Update the permissions, user name, and group name of the mount points (created on the ABE) to match that of the existing directories on the primary boot environment.

13 Review the output of `df` commands and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

If you need to remount, run the command:

```
# vxlustart -r -u targetos_version -d disk_name
```

```
# vxlustart -r -u targetos_version -d disk_name
```

14 After the alternate boot disk is created and mounted on */altroot.5.10*, install any operating system patches or packages on the alternate boot disk that are required for the Symantec product installation:

```
# pkgadd -R /altroot.5.10 -d pkg_dir
```

Upgrading SF Oracle RAC using the installer for a Live Upgrade

You can use the Veritas product installer to upgrade SF Oracle RAC as part of the Live Upgrade.

On a node in the cluster, run the installer on the alternate boot disk to upgrade SF Oracle RAC on all the nodes in the cluster. The program uninstalls the existing version of SF Oracle RAC on the alternate boot disk during the process.

At the end of the process the following occurs:

- SF Oracle RAC 6.1.1 is installed on the alternate boot disk.

To perform Live Upgrade of SF Oracle RAC 6.1.1 using the installer

1. Insert the product disc with SF Oracle RAC 6.1.1 or access your copy of the software on the network.
2. Run the installer script specifying the root path as the alternate boot disk:

   ```
   # ./installmr -upgrade -rootpath /altroot.5.10 -base_path /tmp/sfha6.1
   ```

3. Enter the names of the nodes that you want to upgrade to SF Oracle RAC 6.1.1.

   Note: Make sure that the installed version of VxFS uses the disk layout version 6 or later. If you are on a previous disk layout version, upgrade the version before you proceed with the SF Oracle RAC 6.1.1 installation.

   The installer displays the list of packages to be installed or upgraded on the nodes.
4. Press **Return** to continue with the installation.

   During Live Upgrade, if the OS of the alternate boot disk is upgraded, the installer will not update the VCS configurations for Oracle, Netlsnr, and Sybase resources. If cluster configurations include these resources, you will be prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate boot disks.
5. Verify that the version of the Symantec packages on the alternate boot disk is 6.1.1.

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

   For example:

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

   Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

Completing the Live Upgrade

At the end of the process:

- If the original primary boot disk was encapsulated, the alternate boot disk is encapsulated.
- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.

When completing the Live Upgrade process, take the following limitations into consideration for Solaris 10 Update 10:

- In a shared disk group environment, extra CFS mount entries are ignored when the `vxlustart` command is run, as they are included in `/etc/vfstab`. The entries must be manually removed before booting from the alternate boot environment.
- On Sparc, Live Upgrade from Solaris 9 to Solaris 10 Update 10 may fail using the `lucreate` command.

See the *Symantec™ Storage Foundation for Oracle RAC 6.1 Release notes* for more details.

To complete the Live Upgrade

1 Complete the Live Upgrade process using one of the following commands:

If the primary root disk is not encapsulated, run the following command:

```
# ./vxlufinish -u target_os_version
Live Upgrade finish on the Solaris release <5.10>
```

If the primary root disk is encapsulated by VxVM, run the following command:

```
# ./vxlufinish -u target_os_version -g diskgroup
Live Upgrade finish on the Solaris release <5.10>
```

The Live Upgrade process encapsulates the alternate root disk if the primary root disk was encapsulated.

2 If the system crashes or reboots before Live Upgrade completes successfully, you may remount the alternate disk using the following command:

```
# ./vxlustart -r -u target_os_version
```

Then, rerun the `vxlufinish` command:

```
# ./vxlufinish -u target_os_version
```

3 If the Oracle database is managed by VCS, modify the VCS configuration file on the alternate root disk (`/altroot.5.10/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 0. This prevents the database service group from starting automatically when VCS starts:

```
group oradb_grp (
        SystemList = { sys1 = 0, sys2 = 1 }
        AutoStart = 0
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { sys1, sys2 }
        )
.
.
```

If the database is not managed by VCS, change the management policy for the database to manual on the primary boot disk:

```
$ srvctl modify database -d db-name -y manual
```

4 Perform the following steps on the primary boot environment:

- Stop Oracle Clusterware on each node in the cluster:

  ```
  # clus_home/bin/crsctl crs stop
  ```

  where *clus_home* is the path of the Oracle Clusterware/Grid Infrastructure home directory

- Stop the applications using native application commands.
- Make sure that no processes are running which make use of mounted shared file system or shared volumes.

  ```
  # fuser -cu mount-point
  ```

- Take offline all VCS groups that contain CFSMount and CVMVolDg:

  ```
  # hagrp -offline group -sys sys1
  # hagrp -offline group -sys sys2
  ```

- Unmount the VxFS file systems:

  ```
  # mount -v |grep vxfs
  # fuser -c /mount_point
  # umount /mount_point
  ```

- Deport CVM disk groups:

```
# vxdg deport diskgroup_name
```

- Make sure that no disk groups are imported:

```
# vxdg list
NAME STATE ID
```

5 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

Note: DO NOT use the reboot, halt, or uadmin commands to reboot the system. Use either the init or the shutdown commands to enable the system to boot using the alternate boot environment.

```
# shutdown -g0 -y -i6
```

6 Relink the SF Oracle RAC libraries with the Oracle RAC libraries:

See *Symantec™ Storage Foundation for Oracle RAC 6.1 Installation and Configuration Guide*.

7 Start the database group on all nodes:

```
# hagrp -online oradb_grpname -any
```

8 If the Oracle database is managed by VCS, modify the VCS configuration file (`/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 1.

```
group oradb_grp (
        SystemList = { sys1 = 0, sys2 = 1 }
        AutoStart = 1
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { sys1, sys2 }
        )
.
.
```

If the database is not managed by VCS, change the management policy for the database to automatic on the primary boot disk:

```
$ srvctl modify database -d db-name -y AUTOMATIC
```

9 Complete the post-upgrade tasks.

See *Symantec™ Storage Foundation for Oracle RAC 6.1 Installation and Configuration Guide*.

10 If you are on an unsupported version of Oracle RAC, upgrade Oracle RAC.

For instructions, see the chapter *Upgrading Oracle RAC* in this document.

11 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Verifying Live Upgrade of SF Oracle RAC 6.1.1

To ensure that Live Upgrade has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

To verify that Live Upgrade completed successfully

1 Verify that the alternate boot environment is active.

```
# lustatus
```

If the alternate boot environment is not active, you can revert to the primary boot environment.

See *Symantec™ Storage Foundation for Oracle RAC 6.1 Installation and Configuration Guide*.

2 In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

```
# gabconfig -a
Port a gen   d77c08 membership 0123
Port b gen   d77c0a membership 0123
Port d gen   d77c0c membership 0123
Port f gen   d77c2d membership 0123
Port h gen   d77c3d membership 0123
Port o gen   d77c0b membership 0123
Port u gen   d77c2f membership 0123
Port v gen   d77c28 membership 0123
Port w gen   d77c2a membership 0123
Port y gen   d77c26 membership 0123
```

3 Perform other verification as required to ensure that the new boot environment is configured correctly. The non-global zones must be brought to configured state and then attached with `-U` option so that packages are upgraded inside the non-global zone also.

For example, verify the version in the `/etc/release` file and verify the `VRTSdbac` version.

Upgrading Solaris only using Live Upgrade

Perform the following steps to upgrade only Solaris using Live Upgrade.

To upgrade only Solaris using Live Upgrade

1 Prepare to upgrade using Solaris Live Upgrade.

See "Before you upgrade SF Oracle RAC using Solaris Live Upgrade" on page 141.

2 Create a new boot environment on the alternate boot disk.

See "Creating a new boot environment on the alternate boot disk" on page 143.

3 Complete the Live Upgrade.

See "Completing the Live Upgrade" on page 151.

4 Verify Live Upgrade of SF Oracle RAC.

See "Verifying Live Upgrade of SF Oracle RAC 6.1.1" on page 154.

Performing Boot Environment upgrade with Install Bundles on Solaris 11 systems

Perform the BE upgrade manually or use the installer. For VCS, SFHA, SFCFSHA, and SF Oracle RAC, the nodes do not form a cluster until all of the nodes are upgraded. At the end of the BE upgrade of the last node, all the nodes must boot from the alternate BE and join the cluster.

Table 4-7 Upgrading VCS, SFHA, SFCFSHA, and SF Oracle RAC using BE upgrade

Step	Description
Step 1	Create a new BE on the primary boot disk. See "Creating a new Solaris 11 BE on the primary boot disk" on page 157.
Step 2	Upgrade VCS, SFHA, SFCFSHA, and SF Oracle RAC using the installer. See "Upgrading VCS, SFHA, SFCFSHA, and SF Oracle RAC using the installer for upgrading BE on Solaris 11" on page 157.
	To upgrade only Solaris See the Oracle documentation on Oracle Solaris 11 operating system.
Step 3	Switch the alternate BE to be the new primary. See "Completing the upgrade for VCS on BE on Solaris 11" on page 159. See "Completing the upgrade for SFHA, SFCFSHA, and SF Oracle RAC on BE on Solaris 11" on page 160.
Step 4	Verify BE upgrade of VCS, SFHA, SFCFSHA, and SF Oracle RAC. See "Verifying Solaris 11 BE upgrade" on page 161.

Creating a new Solaris 11 BE on the primary boot disk

Run the `beadm create` command on each node in the cluster to create a new BE on the primary boot disk.

At the end of the process, a new BE is created on the primary boot disk by cloning the primary BE.

To create a new BE on the primary boot disk

Perform the steps in this procedure on each node in the cluster.

1. View the list of BE in the primary disk.

```
# beadm list
```

2. If you have solaris brand zones in running state for which zone root is on shared storage, set `AutoStart` to 0 for the service group containing zone resource.

```
# hagrp -modify <group> AutoStart 0

# haconf -dump
```

3. Create a new BE in the primary boot disk.

```
# beadm create beName

# beadm mount beName mountpoint
```

4. Reset `AutoStart` to 1 for the service group containing zone resource in step 2

```
# hagrp -modify <group> AutoStart 1

# haconf -dump
```

If VVR is configured, it is recommended that <*beName*> should have the value *altroot.5.11* and <*mountpoint*> should have the value `/altroot.5.11`.

Upgrading VCS, SFHA, SFCFSHA, and SF Oracle RAC using the installer for upgrading BE on Solaris 11

You can use the Veritas product installer to upgrade VCS, SFHA, SFCFSHA, and SF Oracle RAC on a BE.

On a node in the cluster, run the installer on the primary boot disk to upgrade VCS, SFHA, SFCFSHA, and SF Oracle RAC on all the nodes in the cluster.

At the end of the process, the VCS, SFHA, SFCFSHA, or SF Oracle RAC is installed on the alternate BE.

To perform BE upgrade of VCS, SFHA, SFCFSHA, and SF Oracle RAC using the installer

1. Access your copy of the software on the network.
2. If you had solaris brand zones in running state in the present BE when you created alternate BE, set the publisher for package repository for BEs of each of the zones.

   ```
   # /usr/bin/pkg -R /altrootpath/zone-root/root
   set-publisher -g  /<path>/VRTSpatches.p5p Symantec
   ```

   For example:

   ```
   # /usr/bin/pkg -R /altroot.5.11/export/home/zone1/root
   set-publisher -g /mnt/VRTSpatches.p5p Symantec
   ```

3. Run the installer script specifying the root path as the alternate BE:

   ```
   # ./installmr -rootpath /altroot.5.11
   ```

4. Enter the names of the nodes that you want to upgrade to 6.1.1.

   Note: If you are upgrading SFHA, SFCFSHA, or SF Oracle RAC, make sure that the installed version of VxFS uses the disk layout version 6 or later. If you are on a previous disk layout version, upgrade the version before you proceed with the product installation.

   The installer displays the list of packages to be installed or upgraded on the nodes.

5. Press **Return** to continue with the installation.

   During BE upgrade, if the OS of the alternate BE is upgraded, the installer does not update the VCS configurations for Oracle, Netlsnr, and Sybase resources. If cluster configurations include these resources, you are prompted to run a list of commands to manually update the configurations after the cluster restarts from the alternate BE.

6. Verify that the version of the Symantec packages on the alternate BE is 6.1.1.

   ```
   # pkg -R /altroot.5.11 list VRTS\*
   ```

   For example:

   - For SFCFSHA:

```
# pkg -R /altroot.5.1list VRTSvxvm
```

- For VCS:

```
# pkg -R /altroot.5.11 list VRTSvcs
```

- For SF Oracle RAC:

```
# pkg -R /altroot.5.11 list VRTSdbac
```

Review the installation logs at `/altroot.5.11/opt/VRTS/install/logs`.

7 Unset the publisher set in step 2.

```
# /usr/bin/pkg -R /altrootpath/zone-root/root
unset-publisher Symantec
```

Completing the upgrade for VCS on BE on Solaris 11

At the end of the process:

- The alternate BE is activated.
- The system is booted from the alternate BE.

To complete the BE upgrade

1 Activate the alternate BE.

```
# beadm activate altroot.5.11
```

2 Stop application and VCS on all nodes.

```
# hastop -all
```

If you have enabled VVR,

3 Restart all the nodes in the cluster. The BE on the alternate disk is activated when you restart the nodes.

Note: Do not use the `reboot`, `halt`, or `uadmin` commands to restart the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate BE.

```
# shutdown -g0 -y -i6
```

4 After the alternate BE is activated, you can switch BEs. If the root disk is encapsulated, refer to the procedure to switch the BEs manually.

5 If you want to upgrade the CP server systems that use VCS or SFHA to this version, make sure that you upgrade all application clusters to this version. 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*.

Completing the upgrade for SFHA, SFCFSHA, and SF Oracle RAC on BE on Solaris 11

At the end of the process:

- The alternate BE is activated.
- The system is booted from the alternate BE.

To complete the BE upgrade

1 Activate the alternate BE.

```
# beadm activate altroot.5.11
```

2 Stop application and VCS on all nodes.

```
# hastop -all
```

If you have enabled VVR,

3 Restart all the nodes in the cluster. The BE on the alternate disk is activated when you restart the nodes.

Note: Do not use the `reboot`, `halt`, or `uadmin` commands to restart the system. Use either the `init` or the `shutdown` commands to enable the system to boot using the alternate BE.

```
# shutdown -g0 -y -i6
```

4 After the alternate BE is activated, you can switch BEs. If the root disk is encapsulated, refer to the procedure to switch the BEs manually.

5 After the upgrade, perform any required post-upgrade tasks such as upgrading the disk group.

6 After the objects are recovered, and the disk group version is upgraded (if desired), run the `vvr_upgrade_lu_finish` script.

7 If you want to upgrade the CP server systems that use VCS or SFHA to this version, make sure that you upgrade all application clusters to this version. 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*.

Verifying Solaris 11 BE upgrade

To ensure that BE upgrade has completed successfully, verify that all the nodes have booted from the alternate BE and joined the cluster.

To verify that BE upgrade completed successfully

1 Verify that the alternate BE is active.

```
# beadm list
```

If the alternate BE fails to be active, you can revert to the primary BE.

2 In a cluster environment, make sure that all the GAB ports are up. Note that different ports appear for different products. For example:

- For SFHA:

```
# gabconfig -a
Port a gen   c03c01 membership 0
Port h gen   c03c03 membership 0
```

- For SF Oracle RAC:

```
# gabconfig -a
Port a gen   d77c08 membership 0123
Port b gen   d77c0a membership 0123
Port d gen   d77c0c membership 0123
Port f gen   d77c2d membership 0123
Port h gen   d77c3d membership 0123
Port o gen   d77c0b membership 0123
Port u gen   d77c2f membership 0123
Port v gen   d77c28 membership 0123
Port w gen   d77c2a membership 0123
Port y gen   d77c26 membership 0123
```

- For VCS:

```
# gabconfig -a
Port a gen   39d901 membership 01
Port h gen   39d909 membership 01
```

3 Make sure that GAB ports a and h are up.

4 Perform other verification as required to ensure that the new BE is configured correctly.

For example, if you are upgrading SF Oracle RAC, verify the version in the `/etc/release` file and verify the `VRTSdbac` version.

5 In a zone environment, verify the zone configuration.

If you have set `AutoStart` to 0 for the service group containing zone resource earlier, perform the following steps:

- Verify whether the zpool on which the root file system of the zone is residing is imported

  ```
  # zpool list
  ```

  If not imported, `online` the zpool resource.

- Attach the zone.

  ```
  # zoneadm -z <zone> attach
  ```

- Reset `AutoStart` to 1 for the service group containing zone resource.

  ```
  # hagrp -modify <group> AutoStart 1
  ```

If you have solaris10 brand zone on your system, you must manually upgrade the packages inside the solaris10 brand zone with packages from Solaris 10 install media.

If you have installed `VRTSvxfs` or `VRTSodm` packages inside the zones, you need to manually upgrade these packages inside the zone.

Reverting to the primary BE on a Solaris 11 system

Boot the system to `ok` prompt.

View the available BEs.

To view the BEs, enter the following:

```
ok> boot -L
```

Select the option of the original BE to which you need to boot.

To boot to the BE

```
# boot -Z <path to boot env>
```

For example:

```
{0} ok boot -L
Boot device: /virtual-devices@100/channel-devices@200/disk@0:a
File and args: -L
1 Oracle Solaris 11 11/11 SPARC
2 solaris-backup-1
Select environment to boot: [ 1 - 2 ]: 1
```

To boot the selected entry, enter the following:

```
boot [<root-device>] -Z rpool/ROOT/solaris

Program terminated
{0} ok boot -Z rpool/ROOT/solaris
```

Chapter 5

Upgrading to 6.1.1 from 6.1

This chapter includes the following topics:

About using the installer to upgrade from 6.1 when the root disk is encapsulated

Upgrading a system with an encapsulated root disk to 6.1.1 requires a reboot after upgrade.

Table 5-1 Upgrading using the installer from 6.1 when the root disk is encapsulated

Starting version	Ending version	Action required
6.1	6.1.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.

Prerequisites for upgrading to 6.1.1

If you are upgrading from 6.1, see the following list for prerequisites for upgrading to the 6.1.1 release:

- For any product in the Symantec Storage Foundation stack, you must have the 6.1.1 release binaries.
- Each system must have sufficient free space to accommodate patches.
- 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 6.1.1 " on page 165.

For information on supported upgrade types, See "Supported upgrade types" on page 31.

Downloading required software to upgrade to 6.1.1

This section describes how to download the latest patches for the installer.

To download required software to upgrade to 6.1.1

1. Download SFHA 6.1.1 from https://sort.symantec.com/patches.
2. Extract it to a directory, say /tmp/sfha611.
3. On Solaris 11, Symantec recommends you creating a backup boot environment.

   See "Creating a new boot environment on Solaris 11" on page 13.

Performing a full upgrade to 6.1.1 on a cluster

Performing a full upgrade on a cluster requires stopping cluster failover functionality during the entire procedure.

Depending on your cluster's configuration, select one of the following procedures to upgrade to 6.1.1:

- Performing a full upgrade to 6.1.1 on a Symantec Cluster Server
- Performing a full upgrade to 6.1.1 on an SFHA cluster
- Performing a full upgrade to 6.1.1 on an SFCFSHA cluster
- Performing a full upgrade to 6.1.1 on an SF Oracle RAC cluster

Performing a full upgrade to 6.1.1 on a Symantec Cluster Server

The following procedure describes performing a full upgrade on a Symantec 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 6.1.1 " on page 165.

2. Log in as superuser.

   Note: Upgrade the Operating System and reboot the systems if required.

3. 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 VCS stack in the global zone.
4. Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the installmr script. Start the pre-upgrade check:

   ```
   # ./installmr -precheck sys1 sys2 ... nodeN
   ```

5. Resolve any issues that the precheck finds.
6. Start the upgrade:

   ```
   # ./installmr sys1 sys2 ... nodeN
   ```

7. After the upgrade, review the log files for any issues.

Performing a full upgrade to 6.1.1 on an SFHA cluster

The following procedure describes performing a full upgrade on an SFHA and VCS cluster.

To perform a full upgrade to 6.1.1 on an SFHA cluster

1. Make sure you have downloaded the latest software required for the upgrade.
2. Log in as superuser.
3. Verify that `/opt/VRTS/bin` and `/opt/VRTSvcs/bin` are in your `PATH` so that you can execute all product commands.

4 If you install SFHA 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 each 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 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 Oracle's documentation for the procedures.

15 On each node, stop the VCS command server:

```
# ps -ef | grep CmdServer
# kill -9 pid_of_CmdServer
```

pid_of_CmdServer is the process ID of CmdServer.

16 Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the `installmr` script. Start the pre-upgrade check:

```
# ./installmr -precheck sys1 sys2 ... nodeN
```

where *sys1* and *sys2* are nodes which are to be upgraded.

Resolve any issue that the precheck finds.

17 Start the upgrade.

```
# ./installmr [-rsh]  sys1 sys2 ... nodeN
```

Review the output and follow the instructions to finish the upgrade.

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 6.1.1 on an SFCFSHA cluster

The following procedure describes performing a full upgrade on an SFCFSHA cluster.

To perform a full upgrade to 6.1.1 on an SFCFSHA cluster

1. Make sure you have downloaded the latest software required for the upgrade.
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 SFCFSHA on Solaris 10 systems that run non-global zones, make sure that all the installed non-global zones are bootable.

   Run the following command to get the state of non-global zones:

   ```
   # zoneadm list -cv
   ```

5. From any node in the cluster, make the VCS configuration writable:

   ```
   # haconf -makerw
   ```

6. Enter the following command to freeze HA service group operations on any node:

   ```
   # hagrp -freeze groupname -persistent
   ```

7. Make the configuration read-only:

   ```
   # haconf -dump -makero
   ```

8. Stop VCS. To stop applications, unmount VxFS/CFS file systems and stop VxVM or CVM volumes managed under VCS.

   ```
   # hastop -all
   ```

9. Stop all applications which are using CFS file systems and VxVM volumes not managed by VCS. Use application native commands to stop applications.

10 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
```

11 On each node, enter the following command to check if any VxFS file systems are mounted:

```
# 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:

  ```
  # umount /filesystem
  ```

  Or

  ```
  # cfsumount /filesystem
  ```

12 If you have created any 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.

13 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.

14 On each node, 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
```

15 Deport all the disk groups which are not managed under VCS:

```
# vxdg deport diskgroup
```

16 On each node, stop the VCS command server:

```
# ps -ef | grep CmdServer
# kill -9 pid_of_CmdServer
```

where *pid_of_CmdServer* is the process ID of CmdServer.

17 If required, apply the OS kernel patches.

See Oracle's documentation for the procedures.

18 From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the installmr script. Start the upgrade.

```
# ./installmr [-rsh] sys1 sys2 ... nodeN
```

Review the output and follow the instructions to finish the upgrade..

19 If necessary, reinstate any missing mount points in the `/etc/vfstab` file on each node.

20 Make the VCS configuration writable again from any node:

```
# haconf -makerw
```

21 Enter the following command on any node to unfreeze HA service group operations:

```
# hagrp -unfreeze groupname -persistent
```

22 Make the configuration read-only:

```
# haconf -dump -makero
```

23 Bring the CVM service group online on each node:

```
# hagrp -online cvm -sys nodename
```

24 Import all the VxVM or CVM diskgroups that are not managed by VCS:

```
# vxdg import diskgroup
```

or

```
$vxdg import -s disgroup
```

25 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

26 If you stopped any RVGs in step 12, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

27 Remount all VxFS/CFS file systems on all nodes:

```
# mount -F fstype blockdevice mountpoint
```

Or

```
# cfsmount /mountpoint
```

28 Remount all Storage Checkpoints on all nodes:

```
# cfsmount /checkpoint_name
```

Or

```
# mount vxfs -o ckpt=name blockdevicemountpoint
```

29 Start all applications which are using VxFS/CFS file systems that are not managed by VCS. Use the application native commands to start the applications.

Performing a full upgrade to 6.1.1 on an SF Oracle RAC cluster

The following procedure describes performing a full upgrade on an SF for Oracle RAC cluster.

To upgrade to 6.1.1 on an SF Oracle RAC cluster

1. Make sure you have downloaded the latest software required for the upgrade.
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. For Oracle RAC 10g, Oracle RAC 11g, and Oracle RAC 12c:

   Stop all Oracle RAC resources.

   - If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

     ```
     # hagrp -offline group_name -any
     ```

   - If the database instances are not managed by VCS, then run the following on one node:
     For Oracle RAC 12c:

     ```
     $ srvctl stop database -db db_name
     ```

     For Oracle RAC 10g and Oracle RAC 11g:

     ```
     $ srvctl stop database -d db_name
     ```

8. - 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:

     ```
     # 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:
  For Oracle RAC 12c:

  ```
  $ srvctl modify database -db db_name -policy MANUAL
  ```

  For Oracle RAC 10g and Oracle RAC 11g:

  ```
  $ srvctl modify database -d db_name -y MANUAL
  ```

9 If Oracle Clusterware is not controlled by VCS, enter the following command on each node of the cluster to stop Oracle Clusterware:

```
# GRID_HOME/bin/crsctl stop crs
```

10 Stop all applications that use VxFS or VxVM disk groups, whether local or CFS.

If the applications are under VCS control:

```
# hagrp -offline grp_name -any
```

If the applications are not under VCS control:

Use native application commands to stop the application.

11 Unmount 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
```

12 Stop VCS.

```
# hastop -all
```

13 If required, apply the OS kernel patches.

See *Oracle's* documentation for the procedures.

14 From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the installmr script. Enter:

```
# ./installmr  sys1 sys2
```

where `sys1` and `sys2` are nodes which are to be upgraded.

15 After the entire cluster is upgraded, follow the installer instructions to proceed further.

16 If necessary, reinstate any missing mount points in the `/etc/vfstab` file on each node.

17 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

18 From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```

19 Enter the following command on each node to unfreeze HA service group operations:

```
# hasys -unfreeze -persistent nodename
```

20 Make the configuration read-only:

```
# haconf -dump -makero
```

21 Enter the following command on each node to take service groups online:

```
# hagrp -online service_group -sys nodename
```

22 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

23 Remount all VxFS file systems on all nodes:

```
# mount /filesystem
```

24 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
```

25 Bring the Oracle database service group online.

- If the Oracle database is managed by VCS:

```
#  hagrp -online Oracle_group -any
```

- If the Oracle database is not managed by VCS:
  For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl start database -d db_name
```

  For Oracle RAC 12c:

```
$ srvctl start database -db db_name
```

26 - If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```
# haconf -makerw
# hagrp -modify oracle_groupname AutoStart 1
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:
  For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

  For Oracle RAC 12c:

```
$ srvctl  modify database -db db_name -policy AUTOMATIC
```

27 Upgrade Oracle RAC.

For information on Oracle RAC support, see:

http://www.symantec.com/docs/DOC5081

For instructions, see the chapter *Upgrading Oracle RAC* in *Symantec™ Storage Foundation for Oracle® RAC Installation and Configuration Guide*.

Note: The procedure for Oracle RAC 12c is the same with that for Oracle RAC 11g Release 2.

Upgrading to 6.1.1 on a standalone system

You can use this procedure to upgrade on a standalone system that runs SF.

To upgrade to 6.1.1 on a standalone system

1. Make sure you have downloaded the latest software required for the upgrade.
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 kernel patches as mentioned in the System requirements.

   For more inforamtion, see System requirements in *Symantec™ Storage Foundation and High Availability Solutions 6.1.1 Release Notes*.

   See IBM'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:

   ```
   # umount /checkpoint_name
   # umount /filesystem
   ```
7. If you have created any 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 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
```

11 If necessary, reinstate any missing mount points in the `/etc/vfstab` file.

12 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

13 If you stopped any RVGs in step 7, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

14 Remount all VxFS file systems and Storage Checkpoints:

```
# mount /filesystem
# mount /checkpoint_name
```

Upgrading Symantec products using Live Upgrade

This section describes how to upgrade 6.1 to 6.1.1 using Live Upgrade.

Supported live upgrade paths:

- Upgrading Symantec Products without Solaris OS upgrade:
  - Upgrading Solaris 10 Update x 6.1 to Solaris 10 Update x 6.1.1
- Upgrading Symantec Products with Solaris OS upgrade
  - Upgrading Solaris 10 Update x 6.1 to Solaris 10 Update y 6.1.1

Prerequisites to upgrade to 6.1.1 using Live Upgrade:

- The node should have an alternate boot disk that is identical to the primary boot disk.
- Installation disc for 6.1 and 6.1.1 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 Symantec products using Live Upgrade from 6.1 to 6.1.1 without OS upgrade

This section describes how to upgrade SF, SFHA, SFCFS, SFCFSHA, Sybase ASE CE, or SF for Oracle RAC from 6.1 to 6.1.1 using Live Upgrade where OS upgrade is not involved.

To upgrade your Symantec product using Live Upgrade

1. Ensure that 6.1 is installed and configured on PBE.

   See your Symantec product 6.1 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 Symantec product:

```
# cd /tmp/sfha6.1.1/scripts

# ./vxlustart -v -u target_os_version -U -d disk_name
```

4 Run the `installmr` command to upgrade your Symantec product:

```
# cd /tmp/sfha6.1.1

# ./installmr -rootpath /altroot_path
```

5 Run the `vxlufinish` command to complete the Live Upgrade:

- If the primary root disk is not encapsulated, run the following command:

```
# cd /tmp/sfha6.1.1/scripts

# ./vxlufinish -u target_os_version
```

- If the primary root disk is encapsulated by VxVM, run the following command:

```
# cd /tmp/sfha6.1.1/scripts

# ./vxlufinish -u target_os_version -g diskgroup
```

6 If the Oracle database is managed by VCS, modify the VCS configuration file on the alternate root disk (`/altroot.5.10/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 0. This prevents the database service group from starting automatically when VCS starts:

For SFRAC:

```
group oradb_grp (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoStart = 0
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )
.
.
```

If the database is not managed by VCS, change the management policy for the database to manual on the primary boot disk:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 10g and 11g:

```
$ srvctl modify database -d db_name -y manual
```

7 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

Note: DO NOT use the reboot, halt, or uadmin commands to reboot the system. Use either the init or the shutdown commands to enable the system to boot using the alternate boot environment.

```
# shutdown -g0 -y -i6
```

8 In case of SFRAC, refer to the “Performing post-upgrade Tasks” section to relink Oracle RAC libraries with SF Oracle RAC from 6.1 Installation and Configuration guide.

9 For SFRAC, relink the SFHA libraries with the Oracle RAC libraries:

10 Start the database group on all nodes:

For SFRAC:

```
# hagrp -online oradb_grpname -any
```

11 If the Oracle database is managed by VCS, modify the VCS configuration file (/etc/VRTSvcs/conf/config/main.cf) to set the AutoStart value to 1.

For SFRAC:

```
group oradb_grp (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoStart = 1
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )
.
.
```

If the database is not managed by VCS, change the management policy for the database to automatic on the primary boot disk:

For Oracle RAC 12c:

```
$ srvctl modify database -db  db_name -policy AUTOMATIC
```

For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

12 If you are on an unsupported version of Oracle RAC, upgrade Oracle RAC.

For instructions, see the chapter *Upgrading Oracle RAC* in this document.

13 Verify that the alternate boot environment is active.

```
# lustatus
```

14 In a cluster environment, make sure that all the GAB ports are up. Note different ports appear for different products.

```
# gabconfig -a
```

Upgrading Symantec products using Live Upgrade from 6.1 to 6.1.1 with OS upgrade

This section describes how to upgrade SF, SFHA, SFCFS, SFCFSHA, Sybase ASE CE, or SF for Oracle RAC from 6.1 to 6.1.1 using Live Upgrade where OS upgrade is involved..

To upgrade your Symantec product using Live Upgrade

1. Ensure that 6.1 is installed and configured on PBE.

   See your Symantec product 6.1 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 Symantec product:

   ```
   # cd /tmp/sfha6.1.1/scripts

   # ./vxlustart -v -u target_os_version -s osimage_path -d disk_name
   ```

4. Run the `installmr` command to upgrade your Symantec product:

   ```
   # cd /tmp/sfha6.1.1

   # ./installmr -rootpath  /altroot_path
   ```

5. Run the `vxlufinish` command to complete the Live Upgrade:

   - If the primary root disk is not encapsulated, run the following command:

     ```
     # cd /tmp/sfha6.1.1/scripts

     # ./vxlufinish -u target_os_version
     ```

- If the primary root disk is encapsulated by VxVM, run the following command:

```
# cd /tmp/sfha6.1.1/scripts

# ./vxlufinish -u target_os_version -g diskgroup
```

6 If the Oracle database is managed by VCS, modify the VCS configuration file on the alternate root disk (`/altroot.5.10/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 0. This prevents the database service group from starting automatically when VCS starts:

For SFRAC:

```
group oradb_grp (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoStart = 0
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )
.
.
```

If the database is not managed by VCS, change the management policy for the database to manual on the primary boot disk:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy manual
```

For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y manual
```

7 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

Note: DO NOT use the reboot, halt, or uadmin commands to reboot the system. Use either the init or the shutdown commands to enable the system to boot using the alternate boot environment.

```
# shutdown -g0 -y -i6
```

8 In case of SFRAC, refer to the “Performing post-upgrade Tasks” section to relink Oracle RAC libraries with SF Oracle RAC from 6.1 Installation and Configuration guide.

9 For SFRAC, relink the SFHA libraries with the Oracle RAC libraries:

10 Start the database group on all nodes:

For SFRAC:

```
# hagrp -online oradb_grpname -any
```

11 If the Oracle database is managed by VCS, modify the VCS configuration file (`/etc/VRTSvcs/conf/config/main.cf`) to set the AutoStart value to 1.

For SFRAC:

```
group oradb_grp (
        SystemList = { galaxy = 0, nebula = 1 }
        AutoStart = 1
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { galaxy, nebula }
        )
.
.
```

If the database is not managed by VCS, change the management policy for the database to automatic on the primary boot disk:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

12 If you are on an unsupported version of Oracle RAC, upgrade Oracle RAC.

For instructions, see the chapter *Upgrading Oracle RAC* in this document.

13 Verify that the alternate boot environment is active.

```
# lustatus
```

14 In a cluster environment, make sure that all the GAB ports are up. Note that different ports appear for different products.

```
# gabconfig -a
```

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.

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:

- Symantec Cluster Server
- Storage Foundation and High Availability
- Storage Foundation Cluster File System High Availability
- Storage Foundation for Oracle RAC
- Symantec VirtualStore

- Storage Foundation for Sybase CE

Prerequisites for a rolling upgrade

Meet the following prerequisites before performing a rolling upgrade:

- Make sure that the product you want to upgrade supports rolling upgrades.
- Make a plan on splitting up your clusters 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.
- VCS must be running before performing the rolling upgrade.
- Make sure you have downloaded the latest software required for the upgrade.

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 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 as subcluster1and nodeB as subcluster2.

To perform the rolling upgrade on kernel packages: phase 1

1 On the first sub-cluster, start the installer for the rolling upgrade with the `-rollingupgrade_phase1` option.

```
# ./installmr -rollingupgrade_phase1 nodeA
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, start the web-based installer with the `./webinstaller start` command, select **Rolling Upgrade** from the task list, make sure the **Phase-1: Upgrade Kernel packages** radio button is checked, and then click **Next**.

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, package versions, product versions, and completes prechecks. It then upgrades applicable kernel patches.

If you are using the web-based installer, input one node of the cluster. The web-based installer detects the whole cluster, and then recommend some nodes (NodeA) as the subcluster to run the rolling upgrade phase 1. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel packages.

4 The installer loads new kernel modules and starts all the relevant processes and brings all the service groups online.

5 If the boot disk is encapsulated, reboot the first sub-cluster's system. Otherwise go to step 6.

6 After rolling upgrade phase 1 is completed on nodeA, the following message displays:

```
It is recommended to perform rolling upgrade phase 1 on the
systems nodeB in the next step.

Would you like to perform rolling upgrade phase 1 on the systems?
[y,n,q] (y)
```

If you choose `y`, it continues to run rolling upgrade phase 1 by itself on nodeB.

If you choose `n` or `q`, you need to complete step 1 to step 4 on nodeB.

7 After rolling upgrade phase 1 of the cluster, the following message displays:

```
Would you like to perform rolling upgrade phase 2 on the cluster?
[y,n,q] (y)
```

- If you choose `y`, it continues to run rolling upgrade phase 2 of the cluster by itself. You don't need to run phase 2:
  After phase 2 upgrade, verify the cluster's status:
  ```
  # hastatus -sum
  ```
- If you choose `n` or `q`, you need to use the following steps to finish rolling upgrade phase 2 of the cluster:

Performing a rolling upgrade on non-kernel packages for VCS, SFHA and SFCFSHA : phase 2

In this phase installer installs all non-kernel filesets on all the nodes in cluster and restarts VCS cluster.

To perform the rolling upgrade on non-kernel packages: phase 2

1. Start the installer for the rolling upgrade with the `-rollingupgrade_phase2` option. Specify all the nodes in the cluster:

   ```
   # ./installmr -rollingupgrade_phase2 nodeA nodeB nodeC nodeD
   ```

   You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, select **Rolling Upgrade** from the task list, make sure the **Phase-2: Upgrade non Kernel packages** radio button is checked, and then click **Next**.

2. The installer checks system communications, patch versions, product versions, and completes prechecks. It upgrades non-kernel patches. It also verifies completion of phase 1.

   If you are using the web-based installer, input one node of the cluster, the web-based installer detects the whole cluster to run the rolling upgrade phase 2. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.

3. Installer will start HA daemon (had) on all nodes, HA will be available once HA daemon is up.

4. Verify the cluster's status:

   ```
   # hastatus -sum
   ```

5. If you want to upgrade CP server systems that use VCS or SFHA to 6.1, make sure that you upgraded all application clusters to version 6.1. 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.

Performing a rolling upgrade on kernel packages for SF Oracle RAC: phase 1

Note that in the following instructions that a subcluster can represent one or more nodes in a full cluster, but is represented by nodeA, nodeB as subcluster1 and nodeC, nodeD as subcluster2.

To perform the rolling upgrade on kernel: phase 1

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/lltab`, `/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/tmp/PrivNIC.cf.save
# cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
  /var/tmp/MultiPrivNIC.cf.save
```

3
- 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:
  For Oracle RAC 10g and Oracle RAC 11g:

  ```
  $ srvctl modify database -d db_name -y MANUAL
  ```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

4 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.

5 For Oracle RAC 10g, Oracle RAC 11g, and Oracle RAC 12c:

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 oracle_group -sys nodeA
# hagrp -offline oracle_group -sys nodeB
```

- If the database instances are not managed by VCS, then run the following on one node:
  For Oracle RAC 12 c:

```
$ srvctl stop instance -db db_name -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
-n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
-i instance_name
```

6 Switch over all failover service groups to the other nodes in the cluster:

```
# hagrp -switch grp_name -to node_name
```

7 Take all the VCS service groups offline:

```
# hagrp -offline grp_name -sys node_name
```

8 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
```

Note: Installer will automatically stop all the applications, database instances, filesystems and volumes which are under VCS control on nodes, while using the `rollingupgrade_phase1` option.

---

9 On the sub-cluster, start the installer for the rolling upgrade with the `-rollingupgrade_phase1` option.

```
# ./installmr -rollingupgrade_phase1 nodeA nodeB
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, start the web-based installer with the `./webinstaller start` command, select **Rolling Upgrade** from the task list, make sure the **Phase-1: Upgrade Kernel packages** radio button is checked, and then click **Next**.

10 Note that if the boot-disk is encapsulated, you do not need to perform an unencapsulation for upgrades.

11 The installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel patches.

If you are using the web-based installer, input one node of the cluster. The web-based installer detects the whole cluster, and then recommend some nodes (NodeA) as the subcluster to run the rolling upgrade phase 1. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel.

12 Relink the SF Oracle RAC libraries with Oracle:

Choose the option **Relink Oracle Database Binary** from the program menu.

13 When prompted, choose the option " Continue Rolling Upgrade " from the menu:

```
1)  Relink Oracle Database Binary
     2)  Continue Rolling Upgrade

Choose option: [1-2,q] (1) 2
```

14 If the boot disk is encapsulated, the installer strongly recommends a reboot of the nodes. Reboot the nodes as prompted by the installer.

Note: Before you reboot the nodes, ensure that the boot device is set to the disk containing the upgraded version of the product.

```
# eeprom
```

---

15 Manually mount the VxFS and CFS file systems that are not managed by VCS.

16 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:
  For Oracle RAC 12c:

  ```
  $ srvctl start instance -db db_name \
  -node node_name
  ```

  For Oracle RAC 11.2.0.2 and later versions:

  ```
  $ srvctl start instance -d db_name \
  -n node_name
  ```

  For Oracle RAC 11.2.0.1 and earlier versions:

  ```
  $ srvctl start instance -d db_name \
  -i instance_name
  ```

17 Start all applications that are not managed by VCS. Use native application commands to start the applications.

18 After rolling upgrade phase 1 is completed on nodeA and nodeB, the following message displays:

```
It is recommended to perform rolling upgrade phase 1 on the
systems nodeC and nodeD in the next step.

Would you like to perform rolling upgrade phase 1 on the systems?
[y,n,q] (y)
```

- If you choose `y`, first complete step 4 to step 8 on the remaining subcluster. Then it continues to run rolling upgrade phase 1 on nodeC and nodeD by itself.
- If you choose `n` or `q`, go to step 15.

19 After rolling upgrade phase 1 of the cluster, the following message displays:

```
Would you like to perform rolling upgrade phase 2 on the cluster?
[y,n,q] (y)
```

- If you choose `y`, it continues to run rolling upgrade phase 2 of the cluster by itself. You don't need to run phase 2: See "Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2" on page 196. After rolling upgrade phase 2, complete step 18 to step 21 (except step 20)verify the cluster's status:

  ```
  # hastatus -sum
  ```

- If you choose `n` or `q`, you need to complete step 18 to step 21 and run rolling upgrade phase 2: See "Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2" on page 196.

20 Before you proceed to phase 2, complete step 4 to 17 on the remaining subcluster.

21 Perform one of the following steps:

- If VCS manages the Oracle database, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

  ```
  # haconf -makerw
  # hagrp -modify oracle_group AutoStart 1
  # haconf -dump -makero
  ```

- If the VCS does not manage the Oracle database, change the management policy for the database to automatic:
  For Oracle RAC 12c:

  ```
  $ srvctl modify database -db db_name -policy AUTOMATIC
  ```

  For Oracle RAC 10g and Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2

In this phase, the 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. Start the installer for the rolling upgrade with the `-rollingupgrade_phase2` option. Specify all the nodes in the cluster:

   ```
   ./installmr -rollingupgrade_phase2 nodeA nodeB nodeC nodeD
   ```

   You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, select **Rolling Upgrade** from the task list, make sure the **Phase-2: Upgrade non Kernel packages** radio button is checked, and then click **Next**.

2. The installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.

   If you are using the web-based installer, input one node of the cluster, the web-based installer detects the whole cluster to run the rolling upgrade phase 2. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.

3. Installer will start HA daemon (had) on all nodes, HA will be available once HA daemon is up.

4. Verify the cluster's status:

   ```
   # hastatus -sum
   ```

Manually installing packages on Solaris brand non-global zones

With Oracle Solaris 11, you must manually install Symantec product 6.1.1 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. On the global zone, ensure that the SMF service `svc:/application/pkg/system-repository:default` is online:

   ```
   global># svcs svc:/application/pkg/system-repository
   ```

2. Log on to the non-global zone as a superuser.
3. Copy the VRTSpkgs.p5p package from the `pkgs` directory from the 6.1 installation media to the non-global zone (for example at `/tmp/install` directory).
4. Copy the VRTSpatches.p5p package from the `patches` directory from the Symantec product 6.1.1 installation media to the non-global zone (for example at `/tmp/install` directory).
5. Disable the publishers that are not reachable, as the package install may fail if any of the recently added repositories are unreachable. For system publishers added from the global zone that are not reachable inside the non-global zone, disable them from global zone and reboot the zone.

   ```
   local># pkg set-publisher --disable <publisher_name>
   ```

   where *publisher_name* is the name of the publisher.
6. Add a file-based repository in the non-global zone.

   ```
   local># pkg set-publisher -g /tmp/install/VRTSpkgs.p5p Symantec
   local># pkg set-publisher -g /tmp/install/VRTSpatches.p5p Symantec
   ```

7. Install the required packages as per the product you have installed on the global zone.

   ```
   local># pkg install --accept VRTSperl VRTSvlic VRTSvxfs VRTSvcs \
   VRTSvcsag VRTSvcsea VRTSodm
   ```

8. Verify that required packages are installed.

   ```
   local># pkg list | grep VRTS
   ```

9. Remove the publisher on the non-global zone.

   ```
   local># pkg unset-publisher Symantec
   ```

10 Enable the publishers that were disabled earlier in step 5.

```
local># pkg set-publisher --enable <publisher_name>
```

11 Repeat steps 2 through 10 on each non-global zone.

Verifying software versions

To verify the version of the software, enter the following command:

```
# installmr -version
```

The output version for 6.1.1 is `6.1.1.000`, and the VRTSperl version is `5.14.2.20`.

Chapter 6

Rolling back Symantec Storage Foundation and High Availability Solutions

This chapter includes the following topics:

About rolling back Symantec Storage Foundation and High Availability Solutions 6.1.1

This section describes how to roll back either by using the `uninstallmr` script, web-based installer, or manually.

The `uninstallmr` script uninstalls all the patches associated with packages installed, and starts the processes.

The uninstallmr script uninstalls all the 6.1.1 patches. A scenario wherein the product is upgraded from 6.1 to 6.1.1, after you run the uninstallmr script, all the 6.1.1 patches are uninstalled while the 6.1 packages are retained.

Note: The uninstallmr script is available only on Solaris 10 and not on Solaris 11.

Note: On Solaris 10, if you upgraded the products to 6.1.1 from 6.1 or versions earlier than 6.1, the products roll back to 6.1.

Rolling back using the uninstallmr script on Solaris 10

Use the following procedure to roll back from any Symantec 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

- For SFRAC:

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:

For Oracle RAC 12c:

```
$ srvctl stop database -db db_name
```

For Oracle RAC 10g and Oracle RAC 11g:

```
$ 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 11gR2 and later verions:

```
# GRID_HOME/bin/crsctl stop crs
```

- For 10gR2:

```
# CRS_HOME/bin/crsctl stop crs
```

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 For Solaris 10, on nodes that run non-global zones managed by VCS, make sure the non-global zones are in the running state. If there are non-global zones managed by VCS, but not in the running state, boot those non-global zones.

9 Run the `uninstallmr` command, type:

```
# ./uninstallmr node A node B node C...
```

10 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 to previous boot environment on Solaris 11

On Solaris 11, SFHA Solutions 6.1.1 contains only packages, so rolling back to versions early than 6.1.1 is not supported. You can only uninstall the entire SFHA stack with the `uninstallmr` script. Instead, if you have already created a boot environment for installing 6.1.1, you can roll back to the previous boot environment available before installing 6.1.1.

To roll back to previous boot environment

1 Activate the boot environment available before installing 6.1.1:

```
# 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 6.1.1 is installed:

```
# beadm destroy bename
```

For example,

```
# beadm destroy pre_sfha_6.1.1
```

Rolling back manually

Use one of the following procedures to roll back to 6.1 manually.

- Rolling back Storage Foundation or Storage Foundation and High Availability manually
- Rolling back Storage Foundation Cluster File System High Availability manually
- Rolling back SF for Oracle RAC manually
- Rolling back Symantec Cluster Server manually
- Rolling back Symantec VirtualStore manually
- Rolling back Dynamic Multi-Pathing manually

Note: You must reboot systems when 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 6.1 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 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 Remove the SF 6.1.1 patches.

- Get the list of 6.1.1 patches, type:

```
# ./installmr -listpatches
```

- Remove each patch from the patch list. For example, on Solaris 10:

```
# patchrm 143287-07
```

Rolling back Storage Foundation Cluster File System High Availability manually

Use the following procedure to roll back to 6.1 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 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 Remove the SFCFSHA 6.1.1 patches.

- Get the list of 6.1.1 patches, type:

```
# ./installmr -listpatches
```

- Remove each patch from the patch list. For example, on Solaris 10:

```
# patchrm 143287-07
```

Rolling back SF for Oracle RAC manually

Use the following procedure to roll back to 6.1 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:

For Oracle RAC 12c:

```
$ srvctl stop database -db db_name
```

For Oracle RAC 11g and Oracle RAC 10g:

```
$ 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:

```
# CRS_HOME/bin/crsctl stop crs
```

- For 11gR2 and later versions:

```
# GRID_HOME/bin/crsctl stop crs
```

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:

```
# ./installsfrac61 -stop <sys1> <sys2> ... <nodeN>
```

9 Remove the SF for Oracle RAC 6.1.1 patches.

- Get the list of 6.1.1 patches, type:

```
# ./installmr -listpatches
```

- Remove each patch from the patch list. For example, on Solaris 10:

```
# patchrm 143287-07
```

10 Verify that the patches have been remove on all the nodes.

11 Reboot the nodes.

```
# /usr/sbin/shutdown -g0 -y -i6
```

Rolling back Symantec Cluster Server manually

Use the following procedure to roll back VCS 6.1.1 to VCS 6.1 on your cluster manually. To uninstall VCS, see the *Symantec Cluster Server 6.1 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 High Availability 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
210 7ba44000 39488 258 1 vxfen (VRTS Fence 6.1.1)
```

- 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
149 50cc6000 2b451 112 1 gab (GAB device 6.1.1)
```

- 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
147 50ca4000 d6bc 110 1 llt (LLT 6.1.1)
```

- Unload LLT using the module number:

```
# modunload -i 147
```

17 Remove the VCS 6.1.1 patches. On each node, perform the following steps:

- Get the list of 6.1.1 patches, type:

```
# ./installmr -listpatches
```

- Remove each patch from the patch list. For example:

```
# patchrm 148492-02
```

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 6.1 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 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 Remove the SVS 6.1.1 patches.

- Get the list of 6.1.1 patches, type:

```
# ./installmr -listpatches
```

- Remove each patch from the patch list. For example, on Solaris 10:

```
# patchrm 143287-07
```

16 Bring up SVS.

Rolling back Dynamic Multi-Pathing manually

Use the following procedure to roll back to 6.1 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 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 Remove the DMP 6.1.1 patches.

- Get the list of 6.1.1 patches, type:

```
# ./installmr -listpatches
```

- Remove each patch from the patch list. For example, on Solaris 10:

```
# patchrm 143287-07
```

16 Bring up DMP.

Rolling back 6.1.1 with the Web-based installer on Solaris 10

This section describes how to roll back this release with the Web-based installer.

To roll back 6.1.1

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 In an HA configuration, stop VCS processes on either the local system or all systems.

To stop VCS processes on all systems:

```
# hastop -all
```

3 Start the Web-based installer.

4 On the **Select a task and a product** page, select **Rollback 6.1.1** from the **Task** drop-down list and click **Next**.

5 Indicate the systems on which to roll back. Enter one or more system names, separated by spaces. Click **Next**.

6 After the validation completes successfully, click **Next** to roll back the patches on the selected system.

7 If there are any processes running on the target system, the installer stops the processes. Click **Next**.

8 After the installer stops the processes, the installer removes the patches from the specified system. Click **Next**.

9 After removing the patches from the system, the installer displays the following message:

```
Do you want to restore and reuse the previous SF Oracle RAC
configuration on all systems?
```

If you select **yes**, the installer restores the previous configuration. In this case, you don't need to configure again.

10 After the rolling back completes, the installer displays the location of the summary, response, and log files.

   If required, view the files to confirm the status of the removal

11 Click **Finish**.

   The Web-based installer prompts you for another task.

Appendix A

About the installation and the uninstallation scripts

This appendix includes the following topics:

About the installation and the uninstallation scripts

Symantec™ Storage Foundation and High Availability Solutions 6.1.1 provides an installation and upgrade script. To install or upgrade the patches that are included in this release, you can use the `installmr` script. The `installmr` script lets you install or upgrade all the patches that are associated with the packages installed.

For more information regarding installation,

Symantec has introduced a new Install Bundles feature to help you install or upgrade directly to maintenance level with one execution. You can use the `-base_path` option to install or upgrade base and maintenance bundles. There are a few prerequisites for using Install Bundles feature for installation and upgrade of 6.1.1 mentioned below:

The installmr script options

The following table lists the command line options for the installmr and upgrade script:

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

Command Line Option	Function
system1 system2...	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
-base_path	The *-base_path* option is used to define the path of a base level release to be integrated with a maintenance level release in order for the two releases to be simultaneously installed.
–precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.
–postcheck	Checks any issues after installation or upgrading on the system.
–responsefile *response_file*	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
–logpath *log_path*	Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved.
–tmppath *tmp_path*	Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where packages are copied on remote systems before installation.

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

Command Line Option	Function
–timeout *timeout_value*	The `-timeout` option is used 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*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
–hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.
–patchpath *patch_path*	Designates the path of a directory that contains all patches to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–jumpstart *dir_path*	Produces a sample finish file for Solaris JumpStart installation. The *dir_path* indicates the path to the directory in which to create the finish file. **Note:** This option is supported only on Solaris 10. **Note:** The –jumpstart option is not supported with `-base_path` option.
–rootpath *root_path*	Specifies an alternative root directory on which to install packages. **Note:** This option is supported only on Solaris 10.

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

Command Line Option	Function
-flash_archive<*flash_archive_path*>	The `-flash_archive` option is used 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. **Note:** This option is supported only on Solaris 10. **Note:** The `-flash_archive` option is not supported with `-base_path` option.
-require	The `-require` option is used to specify a installer hot fix file.
–serial	Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.
–rsh	Specifies this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.
–redirect	Displays progress details without showing the progress bar.
–pkgset	Discovers and displays the package group (minimum, recommended, all) and packages that are installed on the specified systems.
–pkgtable	Displays product's packages in correct installation order by group.
–listpatches	The `-listpatches` option displays product patches in correct installation order.
–makeresponsefile	Use the `-makeresponsefile` option only to generate response files. No actual software installation occurs when you use this option.

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

Command Line Option	Function
–comcleanup	The `-comcleanup` option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated.
–version	Checks and reports the installed products and their versions. Identifies the installed and missed packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missed packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.
–nolic	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
-ignorepatchreqs	The *-ignorepatchreqs* option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
-rolling_upgrade	Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly.
–rollingupgrade_phase1	The `-rollingupgrade_phase1` option is used to perform rolling upgrade Phase-I. In the phase, the product kernel packages get upgraded to the latest version
–rollingupgrade_phase2	The `-rollingupgrade_phase2` option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent packages upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version."

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

Command Line Option	Function
-disable_dmp_native_support	Disables Dynamic multi-pathing support for native the LVM volume groups/ZFS pools during an upgrade. Retaining Dynamic multi-pathing support for the native LVM volume groups/ZFS pools during an upgrade increases package upgrade time depending on the number of LUNs and native LVM volume groups/ZFS pools configured on the system. The `-disable_dmp_native_support` option is supported in upgrade scenario only.
-noipc	Disables the installer from making outbound networking calls to Symantec Operations Readiness Tool (SORT) in order to automatically obtain hot fixes and release information updates.

The uninstallmr script options

The following table lists the command line options for uninstallmr script:

Table A-2 The command line options for the product uninstallmr script

Command Line Option	Function
system1 system2...	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
–responsefile *response_file*	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.
–logpath *log_path*	Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved.

Table A-2 The command line options for the product uninstallmr script *(continued)*

Command Line Option	Function
–tmppath *tmp_path*	Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where packages are copied on remote systems before installation.
–timeout *timeout_value*	The `-timeout` option is used 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*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
–hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.
–rootpath *root_path*	Specifies an alternative root directory on which to install packages.
–serial	Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.
–rsh	Specifies this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.
–redirect	Displays progress details without showing the progress bar.
–listpatches	The `-listpatches` option displays product patches in correct installation order.
–makeresponsefile	Use the `-makeresponsefile` option only to generate response files. No actual software uninstallation occurs when you use this option.

Table A-2 The command line options for the product uninstallmr script *(continued)*

Command Line Option	Function
–comcleanup	The `-comcleanup` option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated.
–version	Checks and reports the installed products and their versions. Identifies the installed and missed packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missed packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.
-ignorepatchreqs	The -ignorepatchreqs option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
-require	The `-require` option is used to specify a installer hot fix file.
-noipc	Disables the installer from making outbound networking calls to Symantec Operations Readiness Tool (SORT) in order to automatically obtain hot fixes and release information updates.
-comsetup	Sets up the ssh or rsh communication between systems without requests for passwords or passphrases.