Veritas Storage Foundation™ 6.0.1 Installation Guide - Solaris

April 2013

Veritas Storage Foundation™ Installation Guide

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

Product version: 6.0.1

Document version: 6.0.1 Rev 4

Legal Notice

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Contents

Section 1

Installation overview and planning

Chapter 1

Introducing Storage Foundation

This chapter includes the following topics:

About Veritas products

The following products are available for this release.

About Storage Foundation

Veritas Storage Foundation by Symantec includes Veritas File System by Symantec (VxFS) and Veritas Volume Manager by Symantec (VxVM) with various feature levels.

Veritas File System is a high-performance journaling file system that provides easy management and quick-recovery for applications. Veritas File System delivers scalable performance, continuous availability, increased I/O throughput, and structural integrity.

Veritas Volume Manager removes the physical limitations of disk storage. You can configure, share, manage, and optimize storage I/O performance online without interrupting data availability. Veritas Volume Manager also provides easy-to-use, online storage management tools to reduce downtime.

You add high availability functionality to Storage Foundation HA by installing Veritas Cluster Server software.

VxFS and VxVM are a part of all Veritas Storage Foundation products. Do not install or update VxFS or VxVM as individual components.

About Veritas Storage Foundation Basic

Storage Foundation Basic supports all Storage Foundation Standard features, however, there are deployment and technical support limitations.

About Veritas Replicator Option

Veritas Replicator Option is an optional, separately-licensable feature.

Veritas Volume Replicator replicates data to remote locations over any standard IP network to provide continuous data availability.

This option is available with Storage Foundation for Oracle RAC, Storage Foundation Cluster File System, and Storage Foundation Standard and Enterprise products.

Before installing this option, read the Release Notes for the product.

To install the option, follow the instructions in the Installation Guide for the product.

About Veritas graphical user interfaces

The following are descriptions of Veritas GUIs.

About Veritas Operations Manager

Veritas Operations Manager provides a centralized management console for Veritas Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports.

Symantec recommends using Veritas Operations Manager (VOM) to manage Storage Foundation and Cluster Server environments.

You can download Veritas Operations Manager at no charge at http://go.symantec.com/vom.

Refer to the Veritas Operations Manager documentation for installation, upgrade, and configuration instructions.

The Veritas Enterprise Administrator (VEA) console is no longer packaged with Storage Foundation products. If you want to continue using VEA, a software version is available for download from http://go.symantec.com/vcsm_download. Veritas Storage Foundation Management Server is deprecated.

Chapter 2

System requirements

This chapter includes the following topics:

- Release notes
- Hardware compatibility list (HCL)
- Supported operating systems
- Veritas File System requirements
- Disk space requirements
- Discovering product versions and various requirement information
- Database requirements

Release notes

The *Release Notes* for each Veritas product contains last minute news and important details for each product, including updates to system requirements and supported software. Review the Release Notes for the latest information before you start installing the product.

The product documentation is available on the Web at the following location:

https://sort.symantec.com/documents

Hardware compatibility list (HCL)

The hardware compatibility list contains information about supported hardware and is updated regularly. Before installing or upgrading Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

For the latest information on supported hardware, visit the following URL:

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

For information on specific High Availability setup requirements, see the *Veritas Cluster Server Installation Guide*.

Supported operating systems

For information on supported operating systems, see the *Storage Foundation Release Notes*.

Veritas File System requirements

Veritas File System requires that the values of the Solaris variables `lwp_default_stksize` and `svc_default_stksize` are at least 0x6000 (for Solaris 10) and 0x8000 (for Solaris 11). When you install the Veritas File System package, `VRTSvxfs`, the VRTSvxfs packaging scripts check the values of these variables in the kernel. If the values are less than the required values, VRTSvxfs increases the values and modifies the `/etc/system` file with the required values. If the VRTSvxfs scripts increase the values, the installation proceeds as usual except that you must reboot and restart the installation program. A message displays if a reboot is required.

To avoid an unexpected need for a reboot, verify the values of the variables before installing Veritas File System. Use the following commands to check the values of the variables:

For Solaris 10:

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

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

For Solaris 11:

```
# echo "lwp_default_stksize/X" | mdb -k
lwp_default_stksize:
lwp_default_stksize:            8000

# echo "svc_default_stksize/X" | mdb -k
svc_default_stksize:
svc_default_stksize:            8000
```

If the values shown are less than 6000 (for Solaris 10) and less than 8000 (for Solaris 11), you can expect a reboot after installation.

Note: The default value of the `svc_default_stksize` variable is 0 (zero), which indicates that the value is set to the value of the `lwp_default_stksize` variable. In this case, no reboot is required, unless the value of the `lwp_default_stksize` variable is too small.

To avoid a reboot after installation, you can modify the `/etc/system` file with the appropriate values. Reboot the system prior to installing the packages. Add the following lines to the `/etc/system` file:

For Solaris 10:

```
set lwp_default_stksize=0x6000
set rpcmod:svc_default_stksize=0x6000
```

For Solaris 11:

```
set lwp_default_stksize=0x8000
set rpcmod:svc_default_stksize=0x8000
```

Disk space requirements

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

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

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

```
# ./installer -precheck
```

See "About the Veritas installer" on page 25.

Discovering product versions and various requirement information

Symantec provides several methods to check the Veritas product you have installed, plus various requirement information.

You can check the existing product versions using the `installer` command with the `-version` option before or after you install. After you have installed the current version of the product, you can use the `showversion` script in the /opt/VRTS/install directory to find version information.

The information that the `version` option or the `showversion` script discovers on systems includes the following:

- The installed version of all released Storage Foundation and High Availability Suite of products
- The required packages or patches (if applicable) that are missing
- The available updates (including patches or hotfixes) from Symantec Operations Readiness Tools (SORT) for the installed products

To run the version checker

1. Mount the media.
2. Start the installer with the `-version` option.

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

Database requirements

The following TechNote identifies the most current information on supported database and operating system combinations:

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

Note: SF supports running Oracle, DB2, and Sybase on VxFS and VxVM.

SF does not support running SFDB tools with DB2 and Oracle.

Chapter 3

Planning to install SF

This chapter includes the following topics:

About planning for SF installation

Before you continue, make sure that you are using the current version of this guide. The latest documentation is available on the Symantec Symantec Operations Readiness Tools (SORT) website.

https://sort.symantec.com/documents

Document version: 6.0.1 Rev 4.

This installation guide is designed for system administrators who already have a knowledge of basic UNIX system and network administration. Basic knowledge includes commands such as `tar`, `mkdir`, and simple shell scripting. Also required is basic familiarity with the specific platform and operating system where SF will be installed.

Follow the preinstallation instructions if you are installing Storage Foundation.

The following Veritas Storage Foundation products by Symantec are installed with these instructions:

- Veritas Storage Foundation Basic
- Veritas Storage Foundation (Standard and Enterprise Editions)

Several component products are bundled with each of these SF products.

About installation and configuration methods for SF

You can install and configure SF using Veritas installation programs or using native operating system methods.

Use one of the following methods to install and configure SF:

- The Veritas product installer
  The installer displays a menu that simplifies the selection of installation options.
- The product-specific installation scripts
  The installation scripts provide a command-line interface to install a specific product. The product-specific scripts enable you to specify some additional command-line options. Installing with the installation script is also the same as specifying SF from the installer menu.
- The Web-based Veritas installer
  The installer provides an interface to manage the installation from a remote site using a standard Web browser.
  See "About the Web-based installer" on page 47.
- Silent installation with response files
  You can use any of the above options to generate a response file. You can then customize the response file for another system. Run the product installation script with the response file to install silently on one or more systems.
  See "About response files" on page 24.
- JumpStart
  You can use the Veritas product installer or the product-specific installation script to generate a Jumpstart script file. Use the generated script to install Veritas packages from your JumpStart server.

About response files

The installer or product installation script generates a response file during any installation, configuration, upgrade (except rolling upgrade), or uninstall procedure. The response file contains the configuration information that you entered during the procedure. When the procedure completes, the installation script displays the location of the response files.

You can use the response file for future installation procedures by invoking an installation script with the `-responsefile` option. The response file passes arguments to the script to automate the installation of that product. You can edit the file to automate installation and configuration of additional systems.

You can generate a response file using the `-makeresponsefile` option.

See “Installation script options” on page 207.

Syntax in the response file

The syntax of the Perl statements that are included in the response file variables varies. It can depend on whether the variables require scalar or list values.

For example, in the case of a string value:

```
$CFG{Scalar_variable}="value";
```

or, in the case of an integer value:

```
$CFG{Scalar_variable}=123;
```

or, in the case of a list:

```
$CFG{List_variable}=["value", "value", "value"];
```

About the Veritas installer

To install your Veritas product, use one of the following methods:

- The general product installer. The general product installer enables you to install and configure the product, verify preinstallation requirements, and view the product’s description. You perform the installation from a disc, and you are prompted to choose a product to install.
  See “Installing Storage Foundation using the installer” on page 43.
- Product-specific installation scripts. If you obtained a standalone Veritas product from an electronic download site, the single product download files do not contain the general product installer. Use the product installation script to install the individual products. You can find these scripts at the root of the product media in the scripts directory. These scripts are also installed with the product.

Table 3-1 lists all the SFHA Solutions product installation scripts. The list of product installation scripts that you find on your system depends on the product that you install on your system.

Note: The name of the script is different depending on whether you run the script from the install media or from a system on which the product software is installed.

Table 3-1 Product installation scripts

Veritas product name	Product installation script (When running the script from the install media)	Product installation script (When running the script from a system on which the SFHA Solutions product is installed)
Veritas Cluster Server (VCS)	`installvcs`	`installvcs`*`<version>`*
Veritas Storage Foundation (SF)	`installsf`	`installsf`*`<version>`*
Veritas Storage Foundation and High Availability (SFHA)	`installsfha`	`installsfha`*`<version>`*
Veritas Storage Foundation Cluster File System High Availability (SFCFSHA)	`installsfcfsha`	`installsfcfsha`*`<version>`*
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`	`installsfrac`*`<version>`*
Veritas Storage Foundation for Sybase ASE CE (SF Sybase CE)	`installsfsybasece`	`installsfsybasece`*`<version>`*
Veritas Dynamic Multi-Pathing	`installdmp`	`installdmp`*`<version>`*
Symantec VirtualStore	`installsvs`	`installsvs`*`<version>`*

The scripts that are installed on the system include the product version in the script name. For example, to install the SF script from the install media, run the `installsf` command. However, to run the script from the installed binaries, run the `installsf`*`<version>`* command.

For example, for the 6.0.1 version:

```
# /opt/VRTS/install/installsf601 -configure
```

Note: Do not include the release version if you use the general product installer to install the product.

At most points during the installation you can type the following characters for different actions:

- Use `b` (back) to return to a previous section of the installation procedure. The back feature of the installation scripts is context-sensitive, so it returns to the beginning of a grouped section of questions.
- Use `Control+c` to stop and exit the program if an installation procedure hangs. After a short delay, the script exits.
- Use `q` to quit the installer.
- Use `?` to display help information.
- Use the Enter button to accept a default response.

See “Installation script options” on page 207.

Downloading the Storage Foundation software

One method of obtaining the Storage Foundation software is to download it to your local system from the Symantec Web site.

For a Trialware download, perform the following. Contact your Veritas representative for more information.

To download the trialware version of the software

1. Open the following link in your browser:

   http://www.symantec.com/index.jsp

2. In Products and Solutions section, click the **Trialware & Downloads** link.
3. On the next page near the bottom of the page, click **Business Continuity**.
4. Under Cluster Server, click **Download Now**.
5. In the new window, click **Download Now**.
6. Review the terms and conditions, and click **I agree**.
7. You can use existing credentials to log in or create new credentials.
8. Find the product that you want to download and select it. Continue with the installation.

If you download a standalone Veritas product, the single product download files do not contain the product installer. Use the installation script for the specific product to install the product.

Note: Trialware is the full product version. The enabled licensing places the product in a demo or a trial state.

See “About the Veritas installer” on page 25.

To download the software

1 Verify that you have enough space on your filesystem to store the downloaded software.

The estimated space for download, gunzip, and tar extract is 2 GB for SPARC and 1.5 GB for Opteron.

If you plan to install the software on the same system, make sure that you also have enough space for the installed software.

See “Disk space requirements” on page 21.

2 To see the space available, you can use the `df` command with the name of the local file system where you intend to download the software.

```
# /usr/bin/df -l filesystem
```

Caution: When you select a location to download files, do not select a directory that contains Veritas products from a previous release or maintenance pack. Make sure that different versions exist in different directories.

3 Download the software, specifying the file system with sufficient space for the file.

Licensing SF

This chapter includes the following topics:

About Veritas product licensing

You have the option to install Veritas products without a license key. Installation without a license does not eliminate the need to obtain a license. A software license is a legal instrument governing the usage or redistribution of copyright protected software. The administrator and company representatives must ensure that a server or cluster is entitled to the license level for the products installed. Symantec reserves the right to ensure entitlement and compliance through auditing.

If you encounter problems while licensing this product, visit the Symantec licensing support website.

www.symantec.com/techsupp/

The Veritas product installer prompts you to select one of the following licensing methods:

- Install a license key for the product and features that you want to install.
  When you purchase a Symantec product, you receive a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased.
- Continue to install without a license key.
  The installer prompts for the product modes and options that you want to install, and then sets the required product level.

Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled. If you do not comply with the above terms, continuing to use the Symantec product is a violation of your end user license agreement, and results in warning messages.
For more information about keyless licensing, see the following URL:
http://go.symantec.com/sfhakeyless

If you upgrade to this release from a prior release of the Veritas software, the installer asks whether you want to upgrade the key to the new version. The existing license keys may not activate new features in this release.

If you upgrade with the product installer, or if you install or upgrade with a method other than the product installer, you must do one of the following to license the products:

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 30.
  See the `vxkeyless(1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
  See "Installing Veritas product license keys" on page 32.
  See the `vxlicinst(1m)` manual page.

You can also use the above options to change the product levels to another level that you are authorized to use. For example, you can add the replication option to the installed product. You must ensure that you have the appropriate license for the product level and options in use.

Note: In order to change from one product group to another, you may need to perform additional steps.

Setting or changing the product level for keyless licensing

The keyless licensing method uses product levels to determine the Veritas products and functionality that are licensed.

For more information to use keyless licensing and to download the management server, see the following URL:

http://go.symantec.com/vom

When you set the product license level for the first time, you enable keyless licensing for that system. If you install with the product installer and select the keyless option, you are prompted to select the product and feature level that you want to license.

After you install, you can change product license levels at any time to reflect the products and functionality that you want to license. When you set a product level, you agree that you have the license for that functionality.

To set or change the product level

1 Change your current working directory:

```
# cd /opt/VRTSvlic/bin
```

2 View the current setting for the product level.

```
# ./vxkeyless -v display
```

3 View the possible settings for the product level.

```
# ./vxkeyless displayall
```

4 Set the desired product level.

```
# ./vxkeyless set prod_levels
```

where *prod_levels* is a comma-separated list of keywords. The keywords are the product levels as shown by the output of step 3.

If you want to remove keyless licensing and enter a key, you must clear the keyless licenses. Use the NONE keyword to clear all keys from the system.

Warning: Clearing the keys disables the Veritas products until you install a new key or set a new product level.

To clear the product license level

1 View the current setting for the product license level.

```
# ./vxkeyless [-v] display
```

2 If there are keyless licenses installed, remove all keyless licenses:

```
# ./vxkeyless [-q] set NONE
```

For more details on using the `vxkeyless` utility, see the `vxkeyless(1m)` manual page.

Installing Veritas product license keys

The VRTSvlic package enables product licensing. After the VRTSvlic is installed, the following commands and their manual pages are available on the system:

vxlicinst	Installs a license key for a Symantec product
vxlicrep	Displays currently installed licenses
vxlictest	Retrieves features and their descriptions encoded in a license key

Even though other products are included on the enclosed software discs, you can only use the Symantec software products for which you have purchased a license.

To install a new license

- Run the following commands. In a cluster environment, run the commands on each node in the cluster:

  ```
  # cd /opt/VRTS/bin
  ```

  ```
  # ./vxlicinst -k license key
  ```

To see a list of your vxkeyless keys, enter the following command:

```
# ./vxkeyless display
```

After you upgrade from a previous release, the output you see when you run the `vxkeyless display` command includes the previous release's vxkeyless keys. Each vxkeyless key name includes the suffix _<previous_release_version>. For example, DMP_6.0, or SFENT_VR_5.1SP1, or VCS_GCO_5.1. During the upgrade process, the CPI installer prompts you to update the vxkeyless keys to the current release level. If you update the vxkeyless keys during the upgrade process, you no longer see the _<previous_release_number> suffix after the keys are updated.

Section 2

Installation of Storage Foundation

Chapter 5

Preparing to install Storage Foundation

This chapter includes the following topics:

Installation preparation overview

Table 5-1 provides an overview of an installation using the product installer.

Table 5-1 Installation overview

Installation task	Section
Obtain product licenses.	See "About Veritas product licensing" on page 29.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Download the software, or insert the product DVD.	See "Downloading the Storage Foundation software" on page 27. See "Mounting the product disc" on page 38.
Set environment variables.	See "Setting environment variables" on page 38.
Create the `/opt` directory, if it does not exist.	See "Creating the /opt directory" on page 38.
Configure the secure shell (ssh) or remote shell (rsh) on all nodes.	See "About configuring secure shell or remote shell communication modes before installing products" on page 227.
Verify that hardware, software, and operating system requirements are met.	See "Release notes" on page 19.
Check that sufficient disk space is available.	See "Disk space requirements" on page 21.
Use the installer to install the products.	See "About the Veritas installer" on page 25.

About using ssh or rsh with the Veritas installer

The installer uses passwordless secure shell (ssh) or remote shell (rsh) communications among systems. The installer uses the ssh or rsh daemon that comes bundled with the operating system. During an installation, you choose the communication method that you want to use. You then provide the installer with the superuser passwords for the systems where you plan to install. The ssh or rsh communication among the systems is removed when the installation process completes, unless the installation abruptly terminates. If installation terminated abruptly, use the installation script's `-comcleanup` option to remove the ssh or rsh configuration from the systems.

See "Installation script options" on page 207.

In most installation, configuration, upgrade (where necessary), and uninstallation scenarios, the installer can configure ssh or rsh on the target systems. In the following scenarios, you need to set up ssh or rsh manually:

- When you perform installer sessions using a response file.

See "About configuring secure shell or remote shell communication modes before installing products" on page 227.

Creating root user

On Oracle Solaris 11, you need to change the root role into a user as you cannot directly log in as root user.

To change root role into a user

1 Log in as local user and assume the root role.

```
% su  - root
```

2 Remove the root role from local users who have been assigned the role.

```
# roles admin

root

# usermod -R " " admin
```

3 Change the root role into a user.

```
# rolemod -K type=normal root
```

4 Verify the change.

- `# getent user_attr root`

  ```
  root::::auths=solaris.*;profiles=All;audit_flags=lo\
  :no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
  ```

  If the `type` keyword is missing in the output or is equal to normal, the account is not a role.

- `# userattr type root`

  If the output is empty or lists normal, the account is not a role.

Note: For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

Note: After installation, you may want to change root user into root role to allow local users to assume the root role.

See "Changing root user into root role" on page 177.

Creating the /opt directory

The directory `/opt` must exist, be writable and must not be a symbolic link.

If you are upgrading, you cannot have a symbolic link from `/opt` to an unconverted volume. If you do have a symbolic link to an unconverted volume, the symbolic link will not function during the upgrade and items in `/opt` will not be installed.

Setting environment variables

Most of the commands used in the installation are in the `/sbin` or `/usr/sbin` directory. Add these directories to your `PATH` environment variable as necessary.

After installation, SF commands are in `/opt/VRTS/bin`. SF manual pages are stored in `/opt/VRTS/man`.

Some VCS custom scripts reside in `/opt/VRTSvcs/bin`. If you are installing a high availability product, add /opt/VRTSvcs/bin to the PATH also.

Add the following directories to your `PATH` and `MANPATH` environment variable:

- If you are using Bourne or Korn shell (`sh` or `ksh`), enter the following:

```
$ PATH=$PATH:/usr/sbin:/opt/VRTS/bin
$ MANPATH=/usr/share/man:/opt/VRTS/man:$MANPATH
$ export PATH MANPATH
```

- If you are using a C shell (`csh` or `tcsh`), enter the following:

```
% set path = ( $path /usr/sbin /opt/VRTS/bin )
% setenv MANPATH /usr/share/man:/opt/VRTS/man:$MANPATH
```

Mounting the product disc

You must have superuser (root) privileges to load the SF software.

To mount the product disc

1 Log in as superuser on a system where you want to install SF.

The systems must be in the same subnet.

2 Insert the product disc into a DVD drive that is connected to your system.

3 If Solaris volume management software is running on your system, the software disc automatically mounts as /cdrom/cdrom0.

4 If Solaris volume management software is not available to mount the DVD, you must mount it manually. After you insert the software disc, enter:

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

Where c0t6d0s2 is the default address for the disc drive.

Assessing the system for installation readiness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Storage Foundation 6.0.1.

Symantec Operations Readiness Tools	Symantec Operations Readiness Tools (SORT) is a Web-based application that is designed to support Symantec enterprise products. See "About Symantec Operations Readiness Tools" on page 39.
Prechecking your systems using the installer	Performs a pre-installation check on the specified systems. The Veritas product installer reports whether the specified systems meet the minimum requirements for installing Storage Foundation 6.0.1. See "Prechecking your systems using the Veritas installer" on page 40.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

Among its broad set of features, SORT lets you do the following:

- Generate server-specific reports that describe how to prepare your servers for installation or upgrade of Symantec enterprise products.
- Access a single site with the latest production information, including patches, agents, and documentation.

- Create automatic email notifications for changes in patches, documentation, and array-specific modules.

To access SORT, go to:

https://sort.symantec.com

Prechecking your systems using the Veritas installer

The script-based and Web-based installer's precheck option checks for the following:

- Recommended swap space for installation
- Recommended memory sizes on target systems for Veritas programs for best performance
- Required operating system versions

To use the precheck option

1 Start the script-based or Web-based installer.

See "Installing Storage Foundation using the installer" on page 43.

See "Installing SF with the Web-based installer" on page 50.

2 Select the precheck option:

- From the Web-based installer, select the **Perform a Pre-Installation Check** from the Task pull-down menu.
- In the script-based installer, from root on the system where you want to perform the check, start the installer.

```
# ./installer
```

In the Task Menu, press the p key to start the precheck.

3 Review the output and make the changes that the installer recommends.

Making the IPS publisher accessible

The installation of SF 6.0.1 fails on Solaris 11 if the Image Packaging System (IPS) publisher is inaccessible. The following error message is displayed:

CPI ERROR V-9-20-1273 Unable to contact configured publishers on <node_name>.

Solaris 11 introduces the new Image Packaging System (IPS) and sets a default publisher (solaris) during Solaris installation. When additional packages are being installed, the set publisher must be accessible for the installation to succeed. If the publisher is inaccessible, as in the case of a private network, then package installation will fail. The following commands can be used to display the set publishers:

```
# pkg publisher
```

Example:

```
root@sol11-03:~# pkg publisher
PUBLISHER       TYPE     STATUS   URI
solaris         origin   online   http://pkg.oracle.com/solaris/release/
root@sol11-03:~# pkg publisher solaris             Publisher: solaris
                Alias:
           Origin URI: http://pkg.oracle.com/solaris/release/
              SSL Key: None
             SSL Cert: None
          Client UUID: 00000000-3f24-fe2e-0000-000068120608
      Catalog Updated: October 09:53:00 PM
              Enabled: Yes
     Signature Policy: verify
```

To make the IPS publisher accessible

1. Enter the following to disable the publisher (in this case, solaris):

   ```
   # pkg set-publisher --disable solaris
   ```

2. Repeat the installation of SF 6.0.1.

3. Re-enable the original publisher. If the publisher is still inaccessible (private network), then the `no-refresh` option can be used to re-enable it.

   ```
   # pkg set-publisher --enable solaris
   ```

   or

   ```
   # pkg set-publisher --enable --no-refresh solaris
   ```

Note: Unsetting the publisher will have a similar effect, except that the publisher can only be re-set if it is accessible. See pkg(1) for further information on the pkg utility.

Installing Storage Foundation using the script-based installer

This chapter includes the following topics:

Installing Storage Foundation using the installer

The Veritas product installer is the recommended method to license and install Storage Foundation.

The following sample procedure is based on the installation of Storage Foundation on a single system.

To install Storage Foundation

1 Set up the systems so that the commands execute on remote machines without prompting for passwords or confirmations with remote shell or secure shell communication utilities.

  See "About configuring secure shell or remote shell communication modes before installing products" on page 227.

2 Load and mount the software disc. If you downloaded the software, navigate to the top level of the download directory and skip the next step.

  See "Mounting the product disc" on page 38.

3 Move to the top-level directory on the disc.

```
# cd /cdrom/cdrom0
```

4 From this directory, type the following command to start the installation on the local system. Use this command to install on remote systems if secure shell or remote shell communication modes are configured:

```
# ./installer
```

5 Enter `I` to install and press Return.

6 When the list of available products is displayed, select Storage Foundation, enter the corresponding number, and press Return.

7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA).

```
Do you agree with the terms of the End User License Agreement as
specified in the storage_foundation/EULA/lang/
EULA_SF_Ux_version.pdf file present on the media? [y,n,q,?] y
```

8 Select from one of the following installation options:

- Minimal packages: installs only the basic functionality for the selected product.
- Recommended packages: installs the full feature set without optional packages.
- All packages: installs all available packages.

Each option displays the disk space that is required for installation. Select which option you want to install and press Return.

9 You are prompted to enter the system names where you want to install the software. Enter the system name or names and then press Enter.

```
Enter the system names separated by spaces:
[q,?] sys1
```

10 After the system checks complete, the installer displays a list of the packages to be installed. Press Enter to continue with the installation.

11 The installer can configure remote shell or secure shell communications for you among systems, however each system needs to have RSH or SSH servers installed. You also need to provide the superuser passwords for the systems. Note that for security reasons, the installation program neither stores nor caches these passwords.

12 The installer may prompt to restore previous Veritas Volume Manager configurations.

13 Choose the licensing method. Answer the licensing questions and follow the prompts.

Note: The keyless license option enables you to install without entering a key. However, you still need a valid license to install and use Veritas products. Keyless licensing requires that you manage the systems with a Management Server.

See "About Veritas product licensing" on page 29.

14 The installer prompts you to configure SFHA. You can continue with configuration if you answer **y**.

15 You are prompted to enter the Standard or Enterprise product mode.

```
1) SF Standard
2) SF Enterprise
b) Back to previous menu

Select product mode to license: [1-2,b,q,?] (2) 1
```

16 At the prompt, 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? [y,n,q,?] (y) y
```

Check the log file, if needed, to confirm the installation and configuration.

Installing language packages

To install SF in a language other than English, install the required language packages after installing the English packages.

To install the language packages on the server

1. Insert the "Language" disc into the DVD-ROM or CD-ROM drive. With Solaris volume management software, the disc is automatically mounted as `/cdrom/cdrom0`.

2. Install the language packages using the `install_lp` command.

   ```
   # cd /cdrom/cdrom0
   # ./install_lp
   ```

Installing Storage Foundation using the web-based installer

This chapter includes the following topics:

About the Web-based installer

Use the Web-based installer interface to install Veritas products. The Web-based installer can perform most of the tasks that the script-based installer performs.

You use the `webinstaller` script to start and stop the Veritas XPortal Server `xprtlwid` process. The `webinstaller` script can also be used to check the status of the XPortal Server.

When the `webinstaller` script starts the `xprtlwid` process, the script displays a URL. Use this URL to access the Web-based installer from a Web browser such as Internet Explorer or FireFox.

The Web installer creates log files whenever the Web installer is operating. While the installation processes are operating, the log files are located in a session-based directory under the `/var/tmp` directory. After the install process completes, the log files are located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep these files for auditing, debugging, and future use.

The location of the Veritas XPortal Server configuration file is `/var/opt/webinstaller/xprtlwid.conf`.

See "Before using the Veritas Web-based installer" on page 48.

See "Starting the Veritas Web-based installer" on page 48.

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

Table 7-1 Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Veritas products.	Must be a supported platform for Storage Foundation 6.0.1.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: ■ Internet Explorer 6, 7, and 8 ■ Firefox 3.x and later

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. Note this URL.

Note: If you do not see the URL, run the command again.

The default listening port is 14172. If you have a firewall that blocks port 14172, use the `-port` option to use a free port instead.

---

2 On the administrative server, start the Web browser.

3 Navigate to the URL that the script displayed.

4 Certain browsers may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

When prompted, enter `root` and root's password of the installation server.

5 Log in as superuser.

Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.

The following instructions are general. They may change because of the rapid release cycle of Mozilla browsers.

To obtain a security exception

1 Click **Or you can add an exception** link.

2 Click **I Understand the Risks**, or **You can add an exception**.

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.

Performing a pre-installation check with the Veritas Web-based installer

This section describes performing a pre-installation check with the Veritas Web-based installer.

To perform a pre-installation check

1. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 48.

2. On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list. Select **Veritas Storage Foundation and High Availability** from the **Product** drop-down list and click **Next**.
3. Select the Storage Foundation from the **Product** drop-down list, and click **Next**.
4. Indicate the systems on which to perform the precheck. Enter one or more system names, separated by spaces. Click **Next**.
5. The installer performs the precheck and displays the results.
6. If the validation completes successfully, click **Next**. The installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.
7. Click **Finish**. The installer prompts you for another task.

Installing SF with the Web-based installer

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

To install SF using the Web-based installer

1. Perform preliminary steps.

   See "Performing a pre-installation check with the Veritas Web-based installer" on page 50.

2. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 48.

3. Select **Install a Product** from the **Task** drop-down list.
4. Select **Storage Foundation** from the Product drop-down list, and click Next.
5. On the License agreement page, read the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.

6. Choose minimal, recommended, or all packages. Click **Next**.

7. Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Next**.

8. If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or rsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.

9. After the validation completes successfully, click **Next** to install SF on the selected system.

10. After the installation completes, you must choose your licensing method.

    On the license page, select one of the following tabs:

    - Keyless licensing

      Note: The keyless license option enables you to install without entering a key. However, in order to ensure compliance you must manage the systems with a management server.

      For more information, go to the following website:

      http://go.symantec.com/sfhakeyless

      Complete the following information:

      - Choose whether you want to install Standard or Enterprise mode.
      - Choose whether you want to enable Veritas Replicator.

      Click **Register**.

    - Enter license key

      If you have a valid license key, select this tab. Enter the license key for each system. Click **Register**.

11. For Storage Foundation, click **Next** to complete the configuration and start the product processes.

    Note that you are prompted to configure only if the product is not yet configured.

    If you select n, you can exit the installer. You must configure the product before you can use SF.

    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.

12 To configure Veritas Storage Foundation, start the Web-based installer and select **Configure a product.** Click the **OK** button. The installers checks for updates. Click the **Next** button.

The the installer displays the save location for the task log files, summary file, and response file.

Click **Finish** button. If a message displays requesting a reboot, execute the command to reboot the system.

```
/usr/sbin/shutdown -r now
```

13 If prompted, 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**. The installer asks if you would like to read the summary file. Select **Yes** to read the summary file. If you select **No**, the installer prompts you for another task.

Chapter 8

Performing an automated installation using response files

This chapter includes the following topics:

Installing SF using response files

Typically, you can use the response file that the installer generates after you perform SF installation on a system to install SF on other systems. You can also create a response file using the `-makeresponsefile` option of the installer.

To install SF using response files

1. Make sure the systems where you want to install SF meet the installation requirements.
2. Make sure the preinstallation tasks are completed.
3. Copy the response file to the system where you want to install SF.
4. Edit the values of the response file variables as necessary.

5. Mount the product disc and navigate to the directory that contains the installation program.
6. Start the installation from the system to which you copied the response file. For example:

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

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

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

See "About the Veritas installer" on page 25.

Response file variables to install Storage Foundation

Table 8-1 lists the response file variables that you can define to install SF.

Table 8-1 Response file variables for installing SF

Variable	Description
CFG{opt}{install}	Installs SF packages. Configuration can be performed at a later time using the `-configure` option. List or scalar: scalar Optional or required: optional

CFG{opt}{installallpkgs}
or
CFG{opt}{installrecpkgs}
or
CFG{opt}{installminpkgs}
	Instructs the installer to install SF packages based on the variable that has the value set to 1:
	■ installallpkgs: Installs all packages
	■ installrecpkgs: Installs recommended packages
	■ installminpkgs: Installs minimum packages
	Note: Set only one of these variable values to 1. In addition to setting the value of one of these variables, you must set the variable `$CFG{opt}{install}` to 1.
	List or scalar: scalar
	Optional or required: required

CFG{accepteula}	Specifies whether you agree with the EULA.pdf file on the media. List or scalar: scalar Optional or required: required

Table 8-1 Response file variables for installing SF *(continued)*

Variable	Description
CFG{opt}{vxkeyless}	Installs the product with keyless license. List or scalar: scalar Optional or required: optional
CFG{opt}{license}	Installs the product with permanent license. List or scalar: scalar Optional or required: optional
CFG{keys}{hostname}	List of keys to be registered on the system if the variable `$CFG{opt}{vxkeyless}` is set to 0 or if the variable `$CFG{opt}{licence}` is set to 1. List or scalar: scalar Optional or required: optional
CFG{systems}	List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required
CFG{prod}	Defines the product to be installed or uninstalled. List or scalar: scalar Optional or required: required
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{pkgpath}	Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional

Table 8-1 Response file variables for installing SF *(continued)*

Variable	Description
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{rsh}	Defines that *rsh* must be used instead of ssh as the communication method between systems. List or scalar: scalar Optional or required: optional
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional
CFG{opt}{prodmode}	List of modes for product List or scalar: list Optional or required: optional

Sample response file for SF installation

The following example shows a response file for installing Storage Foundation.

```
our %CFG;

$CFG{opt}{configure}=1;
$CFG{opt}{redirect}=1;
$CFG{opt}{vr}=1;
$CFG{prod}="SF601";
$CFG{systems}=[ qw(thoropt89 thoropt90) ];

1;
```

Configuring SF using response files

Typically, you can use the response file that the installer generates after you perform SF configuration on one system to configure SF on other systems. You can also create a response file using the `-makeresponsefile` option of the installer.

To configure SF using response files

1. Make sure the SF packages are installed on the systems where you want to configure SF.
2. Copy the response file to the system where you want to configure SF.
3. Edit the values of the response file variables as necessary.

   To configure optional features, you must define appropriate values for all the response file variables that are related to the optional feature.

   See "Response file variables to configure Storage Foundation" on page 57.
4. Start the configuration from the system to which you copied the response file. For example:

   ```
   # /opt/VRTS/install/installsf<version>
   -responsefile /tmp/response_file
   ```

   Where *<version>* is the specific release version, and /tmp/*response_file* is the response file's full path name.

   See "About the Veritas installer" on page 25.

Response file variables to configure Storage Foundation

Table 8-2 lists the response file variables that you can define to configure SF.

Table 8-2 Response file variables specific to configuring Storage Foundation

Variable	List or Scalar	Description
$CFG{config_cfs}	Scalar	Performs the Cluster File System configuration for SF. (Required) Set the value to 1 to configure Cluster File System for SF.

Table 8-2 Response file variables specific to configuring Storage Foundation *(continued)*

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the packages are already installed. (Required) Set the value to 1 to configure SF.
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{systems}	List	List of systems on which the product is to be configured. (Required)
CFG{prod}	Scalar	Defines the product to be configured. The value is VCS60 for VCS. (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The installer copies the response files and summary files also to the specified *logpath* location. (Optional)

Table 8-2 Response file variables specific to configuring Storage Foundation *(continued)*

Variable	List or Scalar	Description
CFG{uploadlogs}	Scalar	Defines a Boolean value 0 or 1. The value 1 indicates that the installation logs are uploaded to the Symantec Web site. The value 0 indicates that the installation logs are not uploaded to the Symantec Web site. (Optional)

Note that some optional variables make it necessary to define other optional variables. For example, all the variables that are related to the cluster service group (csgnic, csgvip, and csgnetmask) must be defined if any are defined. The same is true for the SMTP notification (smtpserver, smtprecp, and smtprsev), the SNMP trap notification (snmpport, snmpcons, and snmpcsev), and the Global Cluster Option (gconic, gcovip, and gconetmask).

Installing Storage Foundation using operating system-specific methods

This chapter includes the following topics:

Installing SF on Solaris 11 using Automated Installer

You can use the Oracle Solaris Automated Installer (AI) to install the Solaris 11 operating system on multiple client systems in a network. AI performs a hands-free installation (automated installation without manual interactions) of both x86 and SPARC systems. You can also use AI media (AI bootable image, provided by Oracle, which can be downloaded from the Oracle Web site) to install the Oracle Solaris OS on a single SPARC or x86 platform. All cases require access to a package repository on the network to complete the installation.

About Automated Installation

AI automates the installation of the Oracle Solaris 11 OS on one or more SPARC or x86 clients in a network. Automated Installation applies to Solaris 11 only. You can install the Oracle Solaris OS on many different types of clients.The clients can differ in:

- architecture
- memory charecteristics
- MAC address
- IP address
- CPU

The installations can differ depending on specifications including network configuration and packages installed.

An automated installation of a client in a local network consists of the following high-level steps:

1. A client system boots and gets IP information from the DHCP server
2. Characteristics of the client determine which AI service and which installation instructions are used to install the client.
3. The installer uses the AI service instructions to pull the correct packages from the package repositories and install the Oracle Solaris OS on the client.

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 a SPARC or x86 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 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 are installing on the systems. Depending on your configuration and needs, you may want 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, and 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 products

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

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

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

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

2 Set up the Symantec package repository.

  Run the following commands to start up 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 the IPS repository for Symantec Opteron packages:

```
# mkdir -p /ai/repo_symc_x64
# pkgrepo create /ai/repo_symc_x64
# pkgrepo add-publisher -s /ai/repo_symc_x64 Symantec
# pkgrecv -s <media_x64>/pkgs/VRTSpkgs.p5p -d /ai/repo_symc_x64 '*'
# svccfg -s pkg/server add symcx64
# svccfg -s pkg/server list
# svccfg -s pkg/server:symcx64 addpg pkg application
# svccfg -s pkg/server:symcx64 setprop pkg/port=10002
# svccfg -s pkg/server:symcx64 setprop pkg/inst_root=/ai/repo_symc_x64
# svccfg -s pkg/server:symcx64 addpg general framework
# svccfg -s pkg/server:symcx64 addpropvalue
general/complete astring: symcx64
# svccfg -s pkg/server:symcx64 addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcx64
# svcadm enable application/pkg/server:symcx64
```

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

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_x64 -p 10002 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://<host>:10002

4 Run the following commands to setup 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
# pkgrecv -s <media_sparc>/pkgs/VRTSpkgs.p5p -d
/ai/repo_symc_sparc '*'
# 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

5 Run the following commands to setup IPS repository to merge Symantec Sparc and x64 packages:

```
# mkdir /ai/repo_symc
# pkgrepo create /ai/repo_symc
# pkgrepo add-publisher -s /ai/repo_symc Symantec
# pkgmerge -s arch=sparc,/ai/repo_symc_sparc -s arch=i386,
/ai/repo_symc_x64 -d /ai/repo_symc
# svcs -a | grep pkg/server
# svccfg -s pkg/server list
# svccfg -s pkg/server add symcmerged
# svccfg -s pkg/server:symcmerged addpg pkg application
# svccfg -s pkg/server:symcmerged setprop pkg/port=10004
# svccfg -s pkg/server:symcmerged setprop pkg/inst_root=/ai/repo_symc
# svccfg -s pkg/server:symcmerged addpg general framework
# svccfg -s pkg/server:symcmerged addpropvalue general/complete
astring: symcmerged
# svccfg -s pkg/server:symcmerged addpropvalue general/enable
boolean: true
# svcadm refresh application/pkg/server:symcmerged
# svcadm enable application/pkg/server:symcmerged
# svcs -a | grep pkg/server
```

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

```
# # /usr/lib/pkg.depotd -d /ai/repo_symc -p 10004 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://<host>:10004

6 Set up the install service on the AI server.

Run the following command:

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

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

Create an install service.

For example:

To set up the AI install server for Opteron platform::

```
# installadm create-service -n sol11x86 -s
/ai/iso/sol-11-1111-ai-x86.iso -d /ai/aiboot/
```

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

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

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

```
# mkdir /ai/manifests
# <media>/installer -ai /ai/manifests
```

8 For each system, generate the system configuration and include the hostname, 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
```

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

Run the following command to add an Opteron system, for example:

```
# installadm create-client -e "<client_MAC>" -n sol11x86
# installadm add-manifest -n sol11x86 -f
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n sol11x86 -f
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n sol11x86 -m vrts_sfha
-p profile_sc -c mac="<client_MAC>"
# installadm list -m -c -p -n sol11x86
```

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
```

10 For Opteron system, use Preboot Execution Environment(PXE) to reboot the system and install the operating system and Storage Foundation products.

For Sparc system, run the following command to reboot the system and install the operating system and Storage Foundation products:

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

Installing SF on Solaris 10 using JumpStart

This installation method applies only to Solaris 10. These JumpStart instructions assume a working knowledge of JumpStart. See the JumpStart documentation that came with your operating system for details on using JumpStart.

Upgrading is not supported. The following procedure assumes a stand-alone configuration.

For the language pack, you can use JumpStart to install packages. You add the language packages in the script, and put those files in the JumpStart server directory.

You can use a Flash archive to install SF and the operating system in conjunction with JumpStart.

See “Using a Flash archive to install SF and the operating system” on page 73.

Overview of JumpStart installation tasks

Review the summary of tasks before you perform the JumpStart installation.

Summary of tasks

1. Add a client (register to the JumpStart server). See the JumpStart documentation that came with your operating system for details.
2. Read the JumpStart installation instructions.
3. Generate the finish scripts.

   See “Generating the finish scripts” on page 69.
4. Prepare shared storage installation resources.

   See “Preparing installation resources” on page 71.
5. Modify the rules file for JumpStart.

   See the JumpStart documentation that came with your operating system for details.
6. Install the operating system using the JumpStart server.
7. When the system is up and running, run the installer command from the installation media to configure the Veritas software.

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

   See “About the Veritas installer” on page 25.

Generating the finish scripts

Perform these steps to generate the finish scripts to install SF.

To generate the script

1. Run the product installer program to generate the scripts for all products.

   ```
   ./installer -jumpstart directory_to_generate_scripts
   ```

   Or

   ```
   ./install<productname> -jumpstart directory_to_generate_script
   ```

   where <*productname*> is the product's installation command, and *directory_to_generate_scripts* is where you want to put the product's script.

   For example:

   ```
   # ./installsf -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 and encapsulation scripts are generated in the directory you specified in step 1.

Output resembles:

```
The finish scripts for SF is generated at /js_scripts/
jumpstart_sf.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
```

Output resembles:

```
encap_bootdisk_vm.fin jumpstart_sf.fin
```

Preparing installation resources

Prepare resources for the JumpStart installation.

To prepare the resources

1 Copy the pkgs directory of the installation media to the shared storage.

```
# cd /path_to_installation_media
# cp -r pkgs BUILDSRC
```

2 Generate the response file with the list of packages.

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

3 Create the adminfile file under *BUILDSRC*/pkgs/ directory.

```
mail=
instance=overwrite
partial=nocheck
runlevel=quit
idepend=quit
rdepend=nocheck
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

4 If you want to encapsulate the root disk automatically when you perform the JumpStart installation, copy the scripts `encap_bootdisk_vm.fin` generated previously to *ENCAPSRC*.

See "Generating the finish scripts" on page 69.

Adding language pack information to the finish file

To add the language pack information to the finish file, perform the following procedure.

To add the language pack information to the finish file

1 For the language pack, copy the language packages from the language pack installation disc to the shared storage.

```
# cd /cdrom/cdrom0/pkgs
# cp -r * BUILDSRC/pkgs
```

If you downloaded the language pack:

```
# cd /path_to_language_pack_installation_media/pkgs
# cp -r * BUILDSRC/pkgs
```

2 In the finish script, copy the product package information and replace the product packages with language packages.

3 The finish script resembles:

```
. . .
for PKG in product_packages
do
...
done. . .
for PKG in language_packages
do
...
done. . .
```

Using a Flash archive to install SF and the operating system

You can only use Flash archive on the Solaris 10 operating system. In the following outline, refer to Solaris documentation for Solaris-specific tasks.

Note: Symantec does not support Flash Archive installation if the root disk of the master system is encapsulated.

The following is an overview of the creation and installation of a Flash archive with Veritas software.

- If you plan to start flar (flash archive) creation from bare metal, perform step 1 through step 10.
- If you plan to start flar creation from a system where you have installed, but not configured the product, perform step 1 through step 4. Skip step 5 and finish step 6 through step 10.

- If you plan to start flar creation from a system where you have installed and configured the product, perform step 5 through step 10.

Flash archive creation overview

1. Ensure that you have installed Solaris 10 on the master system.
2. Use JumpStart to create a clone of a system.
3. Reboot the cloned system.
4. Install the Veritas products on the master system.

   Perform one of the installation procedures from this guide.
5. If you have configured the product on the master system, create the `vrts_deployment.sh` file and the `vrts_deployment.cf` file and copy them to the master system.

   See “Creating the Veritas post-deployment scripts” on page 74.
6. Use the `flarcreate` command to create the Flash archive on the master system.
7. Copy the archive back to the JumpStart server.
8. Use JumpStart to install the Flash archive to the selected systems.
9. Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:

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

   See “About the Veritas installer” on page 25.
10. Perform post-installation and configuration tasks.

    See the product installation guide for the post-installation and configuration tasks.

Creating the Veritas post-deployment scripts

The generated files vrts_deployment.sh and vrts_post-deployment.cf are customized Flash archive post-deployment scripts. These files clean up Veritas product settings on a cloned system before you reboot it for the first time. Include these files in your Flash archives.

To create the post-deployment scripts

1. Mount the product disc.
2. From the prompt, run the `-flash_archive` option for the installer. Specify a directory where you want to create the files.

   ```
   # ./installer -flash_archive /tmp
   ```

3. Copy the vrts_postedeployment.sh file and the vrts_postedeployment.cf file to the golden system.
4. On the golden system perform the following:
   - Put the vrts_postdeployment.sh file in the /etc/flash/postdeployment directory.
   - Put the vrts_postdeployment.cf file in the /etc/vx directory.
5. Make sure that the two files have the following ownership and permissions:

   ```
   # chown root:root /etc/flash/postdeployment/vrts_postdeployment.sh
   # chmod 755 /etc/flash/postdeployment/vrts_postdeployment.sh
   # chown root:root /etc/vx/vrts_postdeployment.cf
   # chmod 644 /etc/vx/vrts_postdeployment.cf
   ```

   Note that you only need these files in a Flash archive where you have installed Veritas products.

Installing SF using the system command

Installing SF on Solaris 10 using the pkgadd command

On Solaris 10, the packages must be installed while in the global zone.

To install SF on Solaris 10 using the pkgadd command

1. Mount the software disc.

   See "Mounting the product disc" on page 38.

2. Copy the supplied VRTS* files from the installation media to a temporary location. Modify them if needed.

   ```
   # cp /cdrom/cdrom0/pkgs/VRTS* \
       /tmp/pkgs
   ```

3 Create the admin file in the current directory. Specify the `-a adminfile` option when you use the `pkgadd` command:

```
mail=
instance=overwrite
partial=nocheck
 runlevel=quit
idepend=quit
rdepend=nocheck
space=quit
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

4 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

See “About the Veritas installer” on page 25.

See “Installation script options” on page 207.

5 Install the packages listed in step 4.

```
#  pkgadd -a adminfile -d /tmp/pkgs pkgname.pkg
```

On Solaris 10, these packages must be installed while in the global zone. If a package's `pkginfo` file contains the variable SUNW_PKG_ALLZONES set not equal to true, the `-G` option should additionally be specified to the `pkgadd` command.

6 Verify that the packages are installed:

```
# pkginfo -l
  packagename
```

7 Start the processes.

See “Starting and stopping processes for the Veritas products ” on page 180.

Installing SF on Solaris 11 using the pkg install command

To install SF on Solaris 11 using the pkg install command

1 Mount the software disc.

See “Mounting the product disc” on page 38.

2 Copy the supplied VRTS* files from the installation media to a temporary location. Modify them if needed.

```
# cp /cdrom/cdrom0/pkgs/VRTS* \
    /tmp/pkgs
```

3 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

See “About the Veritas installer” on page 25.

See “Installation script options” on page 207.

4 Install the packages listed in step 3.

```
#  /usr/bin/pkg  set-publisher -p /tmp/pkgs/VRTSpkgs.p5p Symantec

#  /usr/bin/pkg  install -accept pkgname

#  /usr/bin/pkg  unset-publisher Symantec
```

5 Verify that the packages are installed:

```
# pkg info packagename
```

6 Start the processes.

See “Starting and stopping processes for the Veritas products ” on page 180.

Manually installing packages on Solaris brand non-global zones

With Oracle Solaris 11, you must manually install SF packages inside non-global zones. The native non-global zones are called Solaris brand zones.

To install packages manually on Solaris brand non-global zones:

1 Ensure that the SMF service svc:/application/pkg/system-repository:default is online on the global zone.

```
# svcs svc:/application/pkg/system-repository
```

2 Log on to the non-global zone as a superuser.

3 Copy the VRTSpkgs.p5p package from the pkgs directory from the installation media to the non-global zone (for example at `/tmp/install` directory).

4 Disable the publishers that are not reachable, as package install may fail if any of the already added repositories are unreachable.

```
#pkg set-publisher --disable <publisher name>
```

5 Add a file-based repository in the non-global zone.

```
# pkg set-publisher -p/tmp/install/VRTSpkgs.p5p Symantec
```

6 Install the required packages.

7 Remove the publisher on the non-global zone.

```
#pkg unset-publisher Symantec
```

8 Clear the state of the SMF service, as setting the file-based repository causes SMF service svc:/application/pkg/system-repository:default to go into maintenance state.

```
# svcadm clear svc:/application/pkg/system-repository:default
```

9 Enable the publishers that were disabled earlier.

```
# pkg set-publisher --enable <publisher>
```

Note: Perform steps 2 through 9 on each non-global zone.

Configuring Storage Foundation

This chapter includes the following topics:

Configuring Storage Foundation using the installer

You can use the installer to configure Storage Foundation, although it requires minimal configuration. You do need to start it.

To start Storage Foundation

1. Go to the installation directory.
2. Run the installer command with the configure option.

```
# ./installer -configure
```

Configuring Storage Foundation manually

You can manually configure different products within Storage Foundation.

Configuring Veritas Volume Manager

Use the following procedures to configure Veritas Volume Manager. If you have installed and configured VxVM using the product installer, you do not need to complete the procedures in this section.

For information on setting up VxVM disk groups and volumes after installation, see "Configuring Veritas Volume Manager" in the *Veritas Storage Foundation Administrator's Guide*.

In releases of VxVM (Volume Manager) before 4.0, a system that was installed with VxVM was configured with a default disk group, `rootdg`. The `rootdg` disk group had to contain at least one disk. By default, operations were directed to the `rootdg` disk group. From release 4.0 onward, VxVM can function without any disk group having been configured.

Starting and enabling the configuration daemon

The VxVM configuration daemon (`vxconfigd`) maintains VxVM disk and disk group configurations. The `vxconfigd` communicates configuration changes to the kernel and modifies configuration information stored on disk.

Startup scripts usually invoke `vxconfigd` at system boot time. The `vxconfigd` daemon must be running for VxVM to operate properly.

The following procedures describe how to check that `vxconfigd` is started, whether it is enabled or disabled, how to start it manually, or how to enable it as required.

To determine whether `vxconfigd` is enabled, use the following command:

```
# vxdctl mode
```

The following message indicates that the `vxconfigd` daemon is running and enabled:

```
mode: enabled
```

This message indicates that `vxconfigd` is not running:

```
mode: not-running
```

This message indicates that `vxconfigd` is running, but not enabled:

```
mode: disabled
```

To start the `vxconfigd` daemon, enter the following command:

```
# vxconfigd
```

To enable the volume daemon, enter the following command:

```
# vxdctl enable
```

Once started, vxconfigd automatically becomes a background process.

By default, vxconfigd writes error messages to the console. However, you can configure it to write errors to a log file. For more information, see the vxconfigd(1M) and vxdctl(1M) manual pages.

Starting the volume I/O daemon

The volume I/O daemon (vxiod) provides extended I/O operations without blocking calling processes. Several vxiod daemons are usually started at system boot time after initial installation, and they should be running at all times. The procedure below describes how to verify that the vxiod daemons are running, and how to start them if necessary.

To verify that vxiod daemons are running, enter the following command:

```
# vxiod
```

The vxiod daemon is a kernel thread and is not visible using the ps command.

If, for example, 16 vxiod daemons are running, the following message displays:

```
16 volume I/O daemons running
```

where 16 is the number of vxiod daemons currently running. If no vxiod daemons are currently running, start some by entering this command:

```
# vxiod set no_of_daemons
```

where the number of daemons ranges from 1 to16. Symantec recommends that at least one vxiod daemon should be run for each CPU in the system.

For more information, see the vxiod(1M) manual page.

Using vxinstall to configure Veritas Volume Manager

If you used the Veritas Installation Menu or the installvm script, you do not need to carry out the instructions in this section. Licensing, configuration of enclosure based naming and creation of a default disk group are managed by the menu installer and the installvm script.

Because you are no longer required to configure VxVM disks immediately, the vxinstall command no longer invokes the vxdiskadm program, making it much simpler than in previous releases.

The utility provides the following functions:

- Licensing VxVM.
- Setting up a system-wide default disk group.
- Starting VxVM daemons in case installation of SF has been done manually.

To run the command, enter

```
# vxinstall
```

which will prompt you to enter a license key:

```
Are you prepared to enter a license key [y,n,q,?] (default: y) y
```

The `vxinstall` program then asks if you want to set up a system-wide default disk group, which is optional:

```
Do you want to setup a system wide default disk group ?
[y,n,q,?] (default: y)
```

VxVM will continue with the question:

```
Which disk group [<group>,list,q,?] ?
```

If you know the name of the disk group that you want to use as the default disk group, enter it at the prompt, or use the `list` option and make a selection.

In releases prior to VxVM 4.0, the default disk group was `rootdg` (the root disk group). For VxVM to function, the `rootdg` disk group had to exist and it had to contain at least one disk. This requirement no longer exists, however you may find it convenient to create a system-wide default disk group. For operations that require a disk group, the system-wide default disk group will be used if the VxVM command is not specified with the `-g` option. The main benefit of creating a default disk group is that VxVM commands default to the default disk group and you will not need to use the `-g` option. To verify the default disk group after it has been created, enter the command:

```
# vxdg defaultdg
```

VxVM does not allow you to use the following names for the default disk group because they are reserved words: `bootdg`, `defaultdg` and `nodg`.

At this stage, the installation of VxVM is complete. To carry out further tasks such as disk encapsulation or initialization, see the *Veritas Storage Foundation Administrator's Guide*.

Configuring Veritas File System

After installing Veritas File System, you can create a file system on a disk slice or Veritas Volume Manager volume with the `mkfs` command. Before you can use this file system, you must mount it with the `mount` command. You can unmount the file system later with the `umount` command. A file system can be automatically mounted at system boot time if you add an entry for it in the following file:

```
/etc/vfstab
```

The Veritas-specific commands are described in the Veritas File System guides and online manual pages.

See the *Veritas File System Administrator's Guide*.

Loading and unloading the file system module

The `vxfs` file system module automatically loads on the first reference to a VxFS file system. This occurs when a user tries to mount a VxFS disk layout. In some instances, you may want to load the file system module manually. To do this, first load `vxfs`, then `vxportal`. `vxportal` is a pseudo device driver that enables VxFS commands to issue ioctls to the VxFS modules even when there are no file systems mounted on the system.

```
# modload /kernel/fs/vxfs
# modload /kernel/drv/vxportal
```

If you have a license for the Veritas Quick I/O feature, you can load its kernel modules:

```
# modload /usr/kernel/drv/sparcv9/fdd
```

To determine if the modules successfully loaded, enter:

```
# modinfo | grep vxportal
# modinfo | grep vxfs
```

The above commands provide information about the modules. The first field in the output is the module ID.

You can unload the module by entering:

```
# modunload -i portal_module_id
# modunload -i vxfs_module_id
```

The `modunload` command fails if any mounted VxFS file systems exist. To determine if any VxFS file systems are mounted, enter:

```
# df -F vxfs
```

vxtunefs command permissions and Cached Quick I/O

By default, you must have superuser (`root`) privileges to use the `/opt/VRTS/bin/vxtunefs` command. The `vxtunefs` command is a tool that lets you change caching policies to enable Cached Quick I/O and change other file system options. Database administrators can be granted permission to change default file system behavior in order to enable and disable Cached Quick I/O. The system administrator must change the `vxtunefs` executable permissions as follows:

```
# chown root /opt/VRTS/bin/vxtunefs
# chgrp dba /opt/VRTS/bin/vxtunefs
# chmod 4550 /opt/VRTS/bin/vxtunefs
```

Setting the permissions for `/opt/VRTS/bin/vxtunefs` to 4550 allows all users in the dba group to use the `vxtunefs` command to modify caching behavior for Quick I/O files.

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

Configuring the Storage Foundation for Databases repository database after installation

If you want to use Storage Foundation for Databases (SFDB), you must set up the SFDB repository after installing and configuring SF and . For SFDB repository set up procedures:

See *Veritas Storage Foundation: Storage and Availability Management for Databases*

Section 3

Upgrade of SF

Planning to upgrade SF

This chapter includes the following topics:

Upgrade methods for SF

Symantec offers you several different ways to upgrade. You need to decide which upgrade method best suits your environment, your expertise, and the downtime required.

Table 11-1 Review this table to determine how you want to perform the upgrade

Upgrade types and considerations	Methods available for upgrade
Typical upgrades—use a Veritas provided tool or you can perform the upgrade manually. Requires some server downtime.	Script-based—you can use this to upgrade for the supported upgrade paths Web-based—you can use this to upgrade for the supported upgrade paths Manual—you can use this to upgrade from the previous release Response file—you can use this to upgrade from the supported upgrade paths

Table 11-1 Review this table to determine how you want to perform the upgrade *(continued)*

Upgrade types and considerations	Methods available for upgrade
Native operating system upgrade—use the upgrade software that comes with the operating system. Note that not all operating systems support native upgrades.	Operating system specific methods Operating system upgrades

Supported upgrade paths for SF 6.0.1

The following tables describe upgrading to 6.0.1.

Table 11-2 Solaris SPARC upgrades using the script- or Web-based installer

Veritas software versions	Solaris 8 or older	Solaris 9	Solaris 10	Solaris 11
3.5 3.5 MP4 4.0 4.0 MP1 4.0 MP2	Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0 MP3. Upgrade to 6.0.1 using the installer script.	Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0 MP3. Upgrade to 6.0.1 using the installer script.	N/A	N/A
4.1 4.1 MP1 4.1 MP2 5.0 5.0 MP1	Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0 MP3. Upgrade to 6.0.1 using the installer script.	Upgrade the operating system to at least Solaris 10, then upgrade product to 5.0MP3. Upgrade to 6.0.1 using the installer script.	Upgrade the product to 5.0 MP3. Upgrade to 6.0.1 using the installer script.	N/A

Table 11-2 Solaris SPARC upgrades using the script- or Web-based installer *(continued)*

Veritas software versions	Solaris 8 or older	Solaris 9	Solaris 10	Solaris 11
5.0 MP3 5.0 MP3 RPx	Upgrade the operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script.	Upgrade operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script.	Upgrade directly to 6.0.1 using the installer script.	N/A
5.1 5.1 RPx 5.1 SP1 5.1 SP1 RPx	N/A	Upgrade the operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script.	Upgrade directly to 6.0.1 using the installer script.	N/A
6.0 6.0 RPx	N/A	Upgrade the operating system to at least Solaris 10. Upgrade to 6.0.1 using the installer script.	Upgrade directly to 6.0.1 using the installer script.	Upgrade directly to 6.0.1 using the installer script.
6.0 PR1	N/A	N/A	N/A	Upgrade directly to 6.0.1 using the installer script.

Table 11-3 Solaris x64 upgrades using the script- or Web-based installer

Veritas software versions	Solaris 10	Solaris 11
4.1 4.1 Phase 2	Upgrade to 5.0 MP3. Upgrade to 6.0.1 using the installer script.	N/A
5.0 5.0 MP3 5.0 MP3 RPx	Upgrade to 5.0 MP3. Upgrade to 6.0.1 using the installer script.	N/A

Table 11-3 Solaris x64 upgrades using the script- or Web-based installer *(continued)*

Veritas software versions	Solaris 10	Solaris 11
5.1 5.1 RPx 5.1 SP1* 5.1 SP1 RPx	Use the installer to upgrade to 6.0.1.	N/A
6.0 6.0 RPx	Use the installer to upgrade to 6.0.1.	Upgrade directly to 6.0.1 using the installer script.
6.0 PR1	N/A	Upgrade directly to 6.0.1 using the installer script.

*When you upgrade to 6.0.1 from 5.1 SP1 using the Web-based installer, you must first upgrade to 5.1 SP1 RP1 if you want the installer to create a backup of the boot disk. You can upgrade directly to 6.0.1 from 5.1 SP1 if you do not want the installer to create a backup of the boot disk.

About using the installer to upgrade when the root disk is encapsulated

In prior versions of SF, when upgrading a system with an encapsulated root disk, you first had to unencapsulate. When upgrading to SF 6.0.1, that is no longer necessary, as shown in the table below.

Table 11-4 Upgrading using installer when the root disk is encapsulated

Starting version	Ending version	Action required
5.0 MP3 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.1 or 5.1 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.1 SP1 or 5.1 SP1 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.

Preparing to upgrade SF

Before you upgrade, you need to prepare the systems and storage. Review the following procedures and perform the appropriate tasks.

Getting ready for the upgrade

Complete the following tasks before you perform the upgrade:

- Review the *Veritas Storage Foundation Release Notes* for any late-breaking information on upgrading your system.
- Review the Symantec Technical Support website for additional information: http://www.symantec.com/techsupp/
- Perform the following system-level settings:
  - Set `diag-level` to `min` to perform the minimum amount of diagnostics when the system boots. Depending on the configuration of your systems you may want to re-enable this after you perform the upgrade.

    ```
    {1} ok setenv diag-level min

     diag-level=min
    ```

  - Set **auto-boot?** to `false`. For tight control when systems reboot, set this variable to false. Re-enable this variable after the upgrade.

    ```
    {1} ok setenv auto-boot? false

    auto-boot?=false
    ```

  - Deactivate cron to make sure that extraneous jobs are not performed while you upgrade the systems. Do one of the following:
    Solaris 9:

    ```
    # /etc/init.d/cron stop
    ```

    Solaris 10:

    ```
     # svcadm disable -t system/cron:default
    ```

    Solaris 11:

    ```
    # ps -ef | grep cron
    # kill cron pid
    # svcadm disable svc:/system/cron:default
    ```

- For Solaris 10, make sure that all non-global zones are booted and in the running state before you use the Veritas product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.

  For Live Upgrade, if the alternative root environment also has a zone, you cannot install `VRTSodm`. You must remove the `VRTSodm` package first then install the Storage Foundation product. After you reboot the alternative root, you can install `VRTSodm`.
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.
- Make sure that all users are logged off and that all major user applications are properly shut down.
- Make sure that you have created a valid backup.

  See "Creating backups" on page 93.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the packages, for example `/packages/Veritas` when the root file system has enough space or `/var/tmp/packages` if the `/var` file system has enough space.

  Do not put the files under `/tmp`, which is erased during a system reboot. Do not put the files on a file system that is inaccessible prior to running the upgrade script.

  You can use a Veritas-supplied disc for the upgrade as long as modifications to the upgrade script are not required. If `/usr/local` was originally created as a slice, modifications are required.
- Unmount all the file systems not on the `root disk`. Comment out their entries in `/etc/vfstab`. Stop the associated volumes and deport the associated disk groups. Any file systems that the Solaris operating system or Storage Foundation assumes should be in `rootdg` but are not, must be unmounted and the associated entry in `/etc/vfstab` commented out.
- For any startup scripts in `/sbin/rcS.d`, comment out any application commands or processes that are known to hang if their file systems are not present.
- Make sure that the current operating system supports version 6.0.1 of the product. If the operating system does not support it, plan for a staged upgrade.
- Schedule sufficient outage time and downtime for the upgrade and any applications that use the Veritas products. Depending on the configuration, the outage can take several hours.

- Any swap partitions not in rootdg must be commented out of /etc/vfstab. If possible, swap partitions other than those on the root disk should be commented out of /etc/vfstab and not mounted during the upgrade. Active swap partitions that are not in rootdg cause upgrade_start to fail.
- Make sure the file systems are clean before upgrading.
  See "Verifying that the file systems are clean" on page 98.
- Symantec recommends that you upgrade VxFS disk layouts to a supported version prior to installing VxFS 6.0.1. Unsupported disk layout versions 4, 5, and 6 can be mounted for the purpose of online upgrading in VxFS 6.0.1. You can upgrade unsupported layout versions online before installing VxFS 6.0.1.
- Upgrade arrays (if required).
  See "Upgrading the array support" on page 99.
- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a failback point.
- Determine if the root disk is encapsulated.
  See "Determining if the root disk is encapsulated" on page 94.

Creating backups

Save relevant system information before the upgrade.

To create backups

1 Log in as superuser.

2 Before the upgrade, ensure that you have made backups of all data that you want to preserve.

Back up the /etc/system file.

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 is displayed.

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

4 Copy the vfstab file to vfstab.orig:

```
# cp /etc/vfstab /etc/vfstab.orig
```

5. Run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands and record the output. Use this information to reconfigure your system after the upgrade.
6. If you are installing the high availability version of the Veritas Storage Foundation 6.0.1 software, follow the guidelines given in the *Veritas Cluster Server Installation Guide* and *Veritas Cluster Server Release Notes* for information on preserving your VCS configuration across the installation procedure.

Tasks for upgrading the Storage Foundation for Databases (SFDB)

Tasks for upgrading SFDB tools to version 6.0.1:

- Preparing to migrate the repository database before upgrading from 5.0x or earlier to 6.0.1
  See "Pre-upgrade tasks for migrating the SFDB repository database" on page 94.
- Migrating the repository database after upgrading from 5.0.x or earlier to 6.0.1
  See "Post upgrade tasks for migrating the SFDB repository database" on page 155.

Determining if the root disk is encapsulated

Before you upgrade, you need to determine if the root disk is encapsulated by running the following command:

```
# mount | grep "/ on"
```

If the output from this command includes a path name that contains `vx` and `rootvol` as in `/dev/vx/dsk/bootdg/rootvol`, then the root disk is encapsulated.

If the root disk is encapsulated, follow the appropriate upgrade procedures.

See "About using the installer to upgrade when the root disk is encapsulated" on page 90.

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, you must prepare to migrate the SFDB repository database to 6.0.1 before upgrading to Storage Foundation or Storage Foundation for Oracle RAC 6.0.1.

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 6.0.1.

Perform the following before upgrading SF.

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 6.0.1.

Pre-upgrade planning for Veritas Volume Replicator

Before installing or upgrading Veritas 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 *Veritas 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 *Veritas 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 *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 11-5, if either the Primary or Secondary are running a version of VVR prior to 6.0.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.0.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

Table 11-5 VVR versions and checksum calculations

VVR prior to 6.0.1 (DG version <= 140)	VVR 6.0.1 (DG version >= 150)	VVR calculates checksum TCP connections?
Primary	Secondary	Yes

Table 11-5 VVR versions and checksum calculations *(continued)*

VVR prior to 6.0.1 (DG version <= 140)	VVR 6.0.1 (DG version >= 150)	VVR calculates checksum TCP connections?
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.

Planning and upgrading VVR to use IPv6 as connection protocol

Storage Foundation supports using IPv6 as the connection protocol.

This release supports the following configurations for VVR:

- VVR continues to support replication between IPv4-only nodes with IPv4 as the internet protocol
- VVR supports replication between IPv4-only nodes and IPv4/IPv6 dual-stack nodes with IPv4 as the internet protocol
- VVR supports replication between IPv6-only nodes and IPv4/IPv6 dual-stack nodes with IPv6 as the internet protocol
- VVR supports replication between IPv6 only nodes
- VVR supports replication to one or more IPv6 only nodes and one or more IPv4 only nodes from a IPv4/IPv6 dual-stack node
- VVR supports replication of a shared disk group only when all the nodes in the cluster that share the disk group are at IPv4 or IPv6

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.

Verifying that the file systems are clean

Verify that all file systems have been cleanly unmounted.

To make sure the file systems are clean

1. Verify that all file systems have been cleanly unmounted:

   ```
   # echo "8192B.p S" | /opt/VRTSvxfs/sbin/fsdb filesystem | \
       grep clean
       flags 0 mod 0 clean clean_value
   ```

   A *clean_value* value of `0x5a` indicates the file system is clean. A value of `0x3c` indicates the file system is dirty. A value of `0x69` indicates the file system is dusty. A dusty file system has pending extended operations.

2. If a file system is not clean, enter the following commands for that file system:

   ```
   # opt/VRTS/bin/fsck -F vxfs filesystem
   # opt/VRTS/bin/mount -F vxfs Block_Device
      mountpoint
   # opt/VRTS/bin/umount mountpoint
   ```

   These commands should complete any extended operations on the file system and unmount the file system cleanly.

   A pending large package clone removal extended operation might be in progress if the `umount` command fails with the following error:

   ```
   file system device busy
   ```

   An extended operation is in progress if the following message is generated on the console:

   ```
   Storage Checkpoint asynchronous operation on file_system
   file system still in progress.
   ```

3. If an extended operation is in progress, you must leave the file system mounted for a longer time to allow the operation to complete. Removing a very large package clone can take several hours.

4. Repeat step 1 to verify that the unclean file system is now clean.

Upgrading the array support

The Storage Foundation 6.0.1 release includes all array support in a single package, VRTSaslapm. The array support package includes the array support previously included in the VRTSvxvm package. The array support package also includes support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

See the 6.0.1 Hardware Compatibility List for information about supported arrays.

See "Hardware compatibility list (HCL)" on page 19.

When you upgrade Storage Foundation products with the product installer, the installer automatically upgrades the array support. If you upgrade Storage Foundation products with manual steps, you should remove any external ASLs or APMs that were installed previously on your system. Installing the VRTSvxvm package exits with an error if external ASLs or APMs are detected.

After you have installed Storage Foundation 6.0.1, Symantec provides support for new disk arrays through updates to the `VRTSaslapm` package.

For more information about array support, see the *Veritas Storage Foundation Administrator's Guide*.

Chapter 12

Upgrading Storage Foundation

This chapter includes the following topics:

Upgrading Storage Foundation with the product installer when OS upgrade is not required

This section describes upgrading to the current Storage Foundation if the root disk is unencapsulated, 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 6.0.1.

To upgrade Storage Foundation

1. Log in as superuser.
2. If the root disk is encapsulated under VxVM, unmirror and unencapsulate the root disk as described in the following steps, to be performed in the order listed:

- 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
  ```

  Warning: 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.

  ```
  # /etc/vx/bin/vxunroot
  ```

  Following the removal of encapsulation, the system is rebooted from the unencapsulated root disk.

  If your system is running VxVM 4.1 MP2, the following remnants of encapsulation will still be present:

  - Partition table entries for the private and public regions
  - GRUB or LILO configuration entries for VxVM

3 Unmount any mounted VxFS file systems.

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 *Storage Foundation Administrator’s Guide* for more information.

4 If your system has separate `/opt` and `/var` file systems, make sure they are mounted before proceeding with installation.

5 If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date:

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

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

6. Load and mount the disc. If you downloaded the software, navigate to the top level of the download directory.

7. From the disc, run the `installer` command. If you downloaded the software, run the `./installer` command.

   ```
   # cd /cdrom/cdrom0
   # ./installer
   ```

8. Enter `G` to upgrade and select the **Full Upgrade**.

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

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

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

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

11. The installer lists the packages to install or to update. You are prompted to confirm that you are ready to upgrade.

12. 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**.

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

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

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

15. Stop the product's processes.

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

    If you select `y`, the installer stops the product processes and makes some configuration updates before upgrading.

16. The installer stops, uninstalls, reinstalls, and starts specified packages.
17. If the upgrade was done from 5.0 or if the Storage Foundation was done without vxkeyless keys, the installer shows the following warning:

    ```
    CPI WARNING V-9-40-5323 SF 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 SF license version 5.0 is not updated
    to 6.0 on sys2. It's recommended to upgrade to a 6.0 key.
    SF is licensed on the systems.
    Do you wish to enter additional licenses? [y,n,q,b] (n) n
    ```

18. The Storage Foundation software is verified and configured.
19. The installer prompts you to provide feedback, and provides the log location for the upgrade.
20. 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 into the upgraded boot disk group. If the upgrade fails, revert the upgrade boot disk group to the backup disk group.

    See "Re-joining the backup boot disk group into the current disk group" on page 154.

    See "Reverting to the backup boot disk group after an unsuccessful upgrade" on page 154.

Upgrading Storage Foundation to 6.0.1 using the product installer or manual steps

This section describes upgrading SF from a prior release to 6.0.1. Symantec recommends that you perform this upgrade from single-user mode.

No VxFS file systems can be in use at the time of the upgrade.

Choose the appropriate procedure for your situation.

- If the current Storage Foundation product is installed on an operating system supported by 6.0.1, you do not need to upgrade the operating system. If you do not plan to upgrade the operating system, use one of the following upgrade procedures:
    - Upgrade SF but not OS with the product installer. This is the recommended upgrade procedure.
      See "Upgrading Storage Foundation with the product installer" on page 105.
    - Upgrade SF but not OS with manual steps (pkgadd command).

See “Upgrading Storage Foundation using manual steps” on page 107.

- If you plan to upgrade the operating system, you must perform additional steps to upgrade. If the current Storage Foundation product is installed on an operating system which is no longer supported by 6.0.1, you must upgrade the operating system. If you plan to upgrade the operating system, use the following upgrade procedure:

  See “Upgrading Veritas Storage Foundation to 6.0.1 using upgrade scripts (OS upgrade)” on page 110.

Upgrading Storage Foundation with the product installer

This section describes upgrading to the current Storage Foundation, 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 6.0.1.

To upgrade Storage Foundation

1. Log in as superuser.
2. Unmount any mounted VxFS file systems.

   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 *Veritas File System Administrator’s Guide* for more information.
3. If your system has separate `/opt` and `/var` file systems, make sure they are mounted before proceeding with installation.
4. 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.
5. Load and mount the disc.

   See “Mounting the product disc” on page 38.

6 To invoke the common installer, run the `installer` command on the disc as shown in this example:

```
# cd /cdrom/cdrom0
# ./installer
```

7 Enter `G` to upgrade and press Return.

8 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 SF:  host1
```

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

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

10 You can perform this step if you upgrading from SF 5.1 SP1 for Solaris; for x64 from SF 5.1 SP1 RP1.

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.

11 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.

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

13 Stop the product's processes.

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

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

15 If the upgrade was done from 5.0 or if the Storage Foundation was done without vxkeyless keys, the installer shows the following warning:

```
CPI WARNING V-9-40-5323 SF 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 SF license version 5.0 is not updated
to 6.0 on sys2. It's recommended to upgrade to a 6.0 key.
SF is licensed on the systems
Do you wish to enter additional licenses? [y,n,q,b] (n) n
```

16 The installer verifies, configures, and starts the Veritas Storage Foundation software.

17 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.

See "Re-joining the backup boot disk group into the current disk group" on page 154.

See "Reverting to the backup boot disk group after an unsuccessful upgrade" on page 154.

Upgrading Storage Foundation using manual steps

This section describes upgrading from a previous version of Storage Foundation to the current Storage Foundation (6.0.1) when 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 6.0.1.

To upgrade Storage Foundation

1. Unmount any mounted VxFS file systems.

   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 *Veritas File System Administrator's Guide* for more information.

2. If the VxFS NetBackup libraries package (`VRTSfsnbl`) is installed, remove it before you install the new packages.

   To remove the package, use the `pkgrm` (Solaris 10) or `pkg uninstall` (Solaris 11) command as follows:

   ```
   # pkgrm VRTSfsnbl
   ```

   or

   ```
   # pkg uninstall VRTSfsnbl
   ```

   Respond to any system messages as needed.

   The libraries contained in this package are included in the `VRTSvxfs` package in 6.0.1.

3. Verify that all the Primary RLINKs are up-to-date on all the hosts.

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

   Caution: Do not continue until the Primary RLINKs are up-to-date.

4. If your system has separate `/opt` and `/var` file systems, make sure they are mounted before proceeding with installation.

5. Load and mount the software disc.

   See "Mounting the product disc" on page 38.

6. Change to the directory containing the SF packages.

   ```
   # cd /dvd_mount
   ```

7. If VVR is configured, run the `vvr_upgrade_start` script on all hosts to save the original VVR configuration:

   ```
   # ./scripts/vvr_upgrade_start
   ```

8 Remove the Veritas packages from your existing installation.

Refer to the *Storage Foundation Installation Guide* for the previous release to obtain the list of packages to remove.

9 Run the following command to obtain a list of recommended packages to install:

```
# ./installsf -recpkgs
```

10 Use the `pkgadd` (Solaris 10) or `pkg install` (Solaris 11) command to install the packages from the previous steps.

On Solaris 10:

```
# pkgadd -d ./package_name.pkg
```

On Solaris 11:

```
# pkg set-publisher -p /dvd_mount/VRTSpkgs.p5p Symantec
# pkg install --accept pkg_name
# pkg unset-publisher Symantec
```

If replication using VVR is configured, ignore the following error messages that appear on the Primary console during the installation process:

```
VxVM VVR vxrlink ERROR V-5-1-3371 Can not recover rlink_name.
rvg_name is in PASSTHRU mode
```

```
VxVM VVR vxrlink ERROR V-5-1-3473 Log header I/O error
```

Also ignore the following error message that appears on the Secondary console:

```
WARNING: VxVM VVR vxio V-5-0-278 Rlink rlink_name is stale and
not replicating
```

11 Configure the SF installation using the `installsf -configure` command.

12 If VVR is configured, issue the following command on all the hosts to complete the upgrade. If a host contains only Secondary RVGs, we recommend that you first run the following command on that host:

```
# /dvd_mount/scripts/vvr_upgrade_finish
```

The `vvr_upgrade_finish` script upgrades only the SRL, after which, the RVG cannot work with the earlier versions of VxVM or VVR.

Upgrading Veritas Storage Foundation to 6.0.1 using upgrade scripts (OS upgrade)

This section describes upgrading to the current Veritas Storage Foundation and need to upgrade the Solaris version. If the operating system is not at a supported Solaris version, you must follow this procedure.

This upgrade procedure allows you to retain existing VxVM and VxFS configurations. After upgrading, you can resume using your file systems and volumes as before (without having to run `vxinstall` again).

It is important that you follow these steps in the specified order.

To begin the upgrade

1 If VCS agents for VVR are configured, you must perform the pre-upgrade steps before proceeding.

2 Load and mount the disc.

See "Mounting the product disc" on page 38.

3 Verify that an upgrade is possible on the system. Enter the following command:

```
# /dvd_mount/scripts/upgrade_start -check
```

4 Run the `upgrade_start` script to preserve the previous configuration of Volume Manager.

```
# /dvd_mount/scripts/upgrade_start
```

5 If the `upgrade_start` script fails for any reason, run the `upgrade_finish` script to undo any changes already made. Verify that the system is restored by comparing `/etc/system`, `/etc/vfstab`, and the output of the `format` command. Then determine and correct the cause of the `upgrade_start` failure. If you cannot correct the problem in a timely manner, restore the `vfstab` file to the version saved, restore any other applications, and perform an `init 6` to completely restore the system.

6 Verify that all the Primary RLINKs are up-to-date on all the hosts.

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

Caution: Do not continue until the Primary RLINKs are up-to-date.

7 If VVR is configured, run the `vvr_upgrade_start` script on all hosts to save the original VVR configuration:

```
# /dvd_mount/scripts/vvr_upgrade_start
```

8 If you have VxFS file systems specified in the `/etc/vfstab` file, comment them out.

9 Remove the existing Storage Foundation packages in one of the following ways:

- using the uninstallsf script
- using pkgrm

For details, refer to the *Storage Foundation Installation Guide* for the existing Storage Foundation version.

After you run the uninstallsf script, verify that all VRTS* packages are removed; otherwise, remove them manually using `pkgrm`.

10 If you are upgrading the operating system, do so now.

Refer to the Solaris installation documentation.

11 Install the Storage Foundation packages in one of the following ways:

- using the common installer
  See "To upgrade the Veritas Storage Foundation packages with the product installer" on page 111.
- using manual steps
  See "To upgrade the Veritas Storage Foundation packages with manual steps" on page 112.

To upgrade the Veritas Storage Foundation packages with the product installer

1 Load and mount the disc.

See "Mounting the product disc" on page 38.

2 To invoke the common installer, run the `installer` command on the disc as shown in this example:

```
# cd /dvd_mount
# ./installer
```

3 Select **I** to upgrade the product. The installer will ask you if you want to use the previous configuration.

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

5 If you commented out VxFS File System entries in the /etc/vfstab file, uncomment them.

6 Complete the upgrade by restoring the configuration.

To upgrade the Veritas Storage Foundation packages with manual steps

1 If you are upgrading from Veritas Storage Foundation for DB2 or Veritas Storage Foundation for Oracle, resynchronize all existing snapshots before upgrading.

For Veritas Storage Foundation for DB2:

```
# /opt/VRTS/bin/db2ed_vmsnap -D DB2DATABASE -f SNAPPLAN \
  -o resync
```

For Veritas Storage Foundation for Oracle:

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

2 Load and mount the software disc.

3 Change to the directory containing the packages.

```
# cd /dvd_mount
```

4 Run the following command to obtain a list of recommended packages to install:

```
./installsf -recpkgs
```

Run the following command to obtain a list of all packages to install:

```
./installsf -allpkgs
```

5 Add packages with the pkgadd command.

6 If you commented out VxFS File System entries in the /etc/vfstab file, uncomment them.

7 Complete the upgrade by restoring the configuration.

Restoring the configuration and completing the upgrade

1 Complete the upgrade using the `upgrade_finish` script.

```
# devlinks
# /dvd_mount/scripts/upgrade_finish
```

2 Configure the product using the following command:

```
# /dvd_mount/installer -configure
```

If some Veritas modules fail to unload, perform the following steps:

- Reboot the systems.

3 Importing a pre-6.0.1 Veritas Volume Manager disk group does not automatically upgrade the disk group version to the VxVM 6.0.1 level. You may need to manually upgrade each of your disk groups following a VxVM upgrade.

See "Upgrading VxVM disk group versions" on page 161.

Upgrading Storage Foundation using the Veritas Web-based installer

This section describes upgrading SF with the Veritas Web-based installer. The installer detects and upgrades the product that is currently installed on the specified system or systems.

To upgrade SF

1 Perform the required steps to save any data that you wish to preserve. For example, make configuration file backups.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 48.

3 On the Select a task and a product page, select **Upgrade a Product** from the Task drop-down menu.

The installer detects the product that is installed on the specified system. Click **Next**.

4 Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click **Next**.

5 On the License agreement page, select whether you accept the terms of the End User License Agreement (EULA). To continue, select **Yes I agree** and click **Next**.

6 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 book disk group. To create the backup, check the **Split mirrors on all the systems** box. Check the appropriate box to use the same name for the backup disk group on all systems--you can use the default name or choose a new one. Check the systems where you want to create the backup. When you are ready, click the **Next** button.

7 Click **Next** to complete the upgrade.

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

8 If you are prompted to reboot the systems, enter the following reboot command:

```
# /usr/sbin/shutdown -r now
```

9 After the upgrade, if the product is not configured, the Web-based installer asks: "Do you want to configure this product?" If the product is already configured, it will not ask any questions.

10 Click **Finish**. The installer prompts you for another task.

11 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 into the upgraded boot disk group. If the upgrade fails, revert the upgrade boot disk group to the backup disk group.

See "Re-joining the backup boot disk group into the current disk group" on page 154.

See "Reverting to the backup boot disk group after an unsuccessful upgrade" on page 154.

Upgrading the Solaris operating system

If you are running Storage Foundation 6.0.1 with an earlier release of the Solaris operating system, you can upgrade the Solaris operating system using the following procedure.

Warning: You should only use this procedure to upgrade the Solaris operating system if you are running Storage Foundation 6.0.1.

The directory /opt must exist, be writable, and must not be a symbolic link. This is because the volumes not temporarily converted by the upgrade_start are unavailable during the upgrade process. If you have a symbolic link from /opt to one of the unconverted volumes, the symbolic link will not function during the upgrade and items in /opt will not be installed.

To upgrade the Solaris operating system only

1 Bring the system down to single-user mode using the following command:

```
# init S
```

You must mount /opt manually if /opt is on its own partition.

2 Load and mount the software disc from the currently installed version of Storage Foundation.

See "Mounting the product disc" on page 38.

3 Change directory:

```
# cd /mount_point/scripts
```

4 Run the upgrade_start with the -check argument to detect any problems that exist which could prevent a successful upgrade. Use the upgrade_start script that was supplied with the currently installed SF release. If this command reports success, you can proceed with running the upgrade_start script, but if it reports errors, correct the problem(s) and rerun upgrade_start -check.

```
# ./upgrade_start -check
```

5 Run the upgrade_start script so that the system can come up with partitions. The upgrade_start script searches for volumes containing file systems, and if any are found, converts them to partitions:

```
# ./upgrade_start
```

6 Bring the system down to run level 0.

```
# init 0
```

7. Upgrade the operating system to a supported version of Solaris.

   You should boot up the system from run level 0 depending on the Solaris upgrade procedure that you want to follow. Refer to the Solaris installation documentation for instructions on how to upgrade the Solaris operating system.

8. After installing the Solaris operating system, install any Solaris patches required by Storage Foundation 6.0.1.

   See the *Storage Foundation Release Notes*.

9. After the system is up with the upgraded Solaris operating system, bring the system down to single-user mode by entering:

   ```
   # init S
   ```

10. Ensure that `/opt` is mounted.

11. Load and mount the software disc from the currently installed version of Storage Foundation.

12. If you upgraded to Solaris 10, you must reinstall certain Storage Foundation packages in order to support Solaris 10 functionality.

    To reinstall the required packages, follow the steps below:

    - Remove the existing packages in the reverse order of their installation. For example, if you chose the installation of all packages then uninstall those in the following order.
      For Storage Foundation:

      ```
      # pkgrm VRTSat VRTSodm VRTSdbed
      VRTSfssdk VRTSvxfs VRTSsfmh VRTSob VRTSaslapm
      VRTSvxvm VRTSspt VRTSperl VRTSvlic
      ```

    - Run the following commands.
      To obtain a list of recommended packages to install:

      ```
      # ./installsf -recpkgs
      ```

      Or
      To obtain a list of all packages to install:

      ```
      # ./installsf -allpkgs
      ```

    - Change to the directory containing the appropriate packages.

      ```
      # cd /mount_point/pkgs
      ```

- Use the pkgadd command to install the packages from the list you generated.
- Reboot the system.

13 Complete the upgrade from the software disc from the currently installed version of Storage Foundation by entering:

```
# devlinks
# ./upgrade_finish
```

Upgrading Veritas Volume Replicator

If a previous version of Veritas Volume Replicator (VVR) is configured, the product installer upgrades VVR automatically when you upgrade the Storage Foundation products.

When upgrading from 4.1 MP1 or later, you have the option to upgrade without disrupting replication.

See “Upgrading VVR without disrupting replication” on page 117.

Upgrading VVR without disrupting replication

This section describes the upgrade procedure from an earlier version of VVR to the current version of VVR when replication is in progress, assuming that you do not need to upgrade all the hosts in the RDS simultaneously.

You may also need to set up replication between versions.

See “Planning an upgrade from the previous VVR version” on page 96.

When both the Primary and the Secondary have the previous version of VVR installed, the upgrade can be performed either on the Primary or on the Secondary. We recommend that the Secondary hosts be upgraded before the Primary host in the RDS. This section includes separate sets of steps, for the Primary upgrade and for the Secondary upgrade.

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

Upgrading VVR on the Secondary

Follow these instructions to upgrade the Secondary hosts.

To upgrade the Secondary

1 Stop replication to the Secondary host by initiating a Primary pause using the following command:

```
# vradmin -g diskgroup pauserep local_rvgname
```

2 Upgrade from VVR 5.1 or later to VVR 6.0.1 on the Secondary.

3 Do one of the following:

- Upgrade the disk group now. Enter the following:

  ```
  # vxdg upgrade dgname
  ```

- Upgrade the disk group later.
  If you upgrade the disk group later, be sure to pause replication before you upgrade the disk group.

4 Resume the replication from the Primary using the following command:

```
# vradmin -g diskgroup resumerep local_rvgname sec_hostname
```

Upgrading VVR on the Primary

After you upgrade the Secondary, use the Veritas product installer to upgrade the Primary.

To upgrade the Primary

1 Stop replication to the Primary host by initiating a Primary pause using the following command:

```
# vradmin -g diskgroup pauserep local_rvgname
```

2 Upgrade from VVR 5.1 or later to VVR 6.0.1 on the Secondary.

3 Do one of the following:

- Upgrade the disk group now. Enter the following:

  ```
  # vxdg upgrade dgname
  ```

- Upgrade the disk group later.

If you upgrade the disk group later, be sure to pause replication before you upgrade the disk group.

4 Resume the replication from the Primary using the following command:

```
# vradmin -g diskgroup resumerep local_rvgname
    sec_hostname
```

See “Planning an upgrade from the previous VVR version” on page 96.

Upgrading language packages

If you are upgrading Veritas products in a language other than English, you must install the required language packages after installing the English packages.Verify that the English installation is correct before proceeding.

Install the language packages as for an initial installation.

See “Installing language packages” on page 45.

Chapter 13

Performing an automated SF upgrade using response files

This chapter includes the following topics:

- Upgrading SF using response files
- Response file variables to upgrade Storage Foundation
- Sample response file for SF upgrade

Upgrading SF using response files

Typically, you can use the response file that the installer generates after you perform SF upgrade on one system to upgrade SF on other systems. You can also create a response file using the `makeresponsefile` option of the installer.

To perform automated SF upgrade

1. Make sure the systems where you want to upgrade SF 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 SF.
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 which you copied the response file. For example:

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

```
# ./installsf<version> -responsefile /tmp/response_file
```

Where /tmp/*response_file* is the response file's full path name and <*version*> is the specific release version.

See "About the Veritas installer" on page 25.

Response file variables to upgrade Storage Foundation

Table 13-1 lists the response file variables that you can define to configure SF.

Table 13-1 Response file variables for upgrading SF

Variable	Description
CFG{accepteula}	Specifies whether you agree with the EULA.pdf file on the media. List or scalar: scalar Optional or required: required
CFG{systems}	List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional

Table 13-1 Response file variables for upgrading SF *(continued)*

Variable	Description
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional
CFG{opt}{upgrade}	Upgrades all packages installed, without configuration. List or scalar: list Optional or required: optional
CFG{mirrordgname}{system}	If the root dg is encapsulated and you select split mirror is selected: Splits the target disk group name for a system. List or scalar: scalar Optional or required: optional
CFG{splitmirror}{system}	If the root dg is encapsulated and you select split mirror is selected: Indicates the system where you want a split mirror backup disk group created. List or scalar: scalar Optional or required: optional

Sample response file for SF upgrade

The following example shows a response file for upgrading Storage Foundation.

```
our %CFG;

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
```

```
$CFG{systems}=[ qw(system01) ];
1;
```

Upgrading SF using Live Upgrade

This chapter includes the following topics:

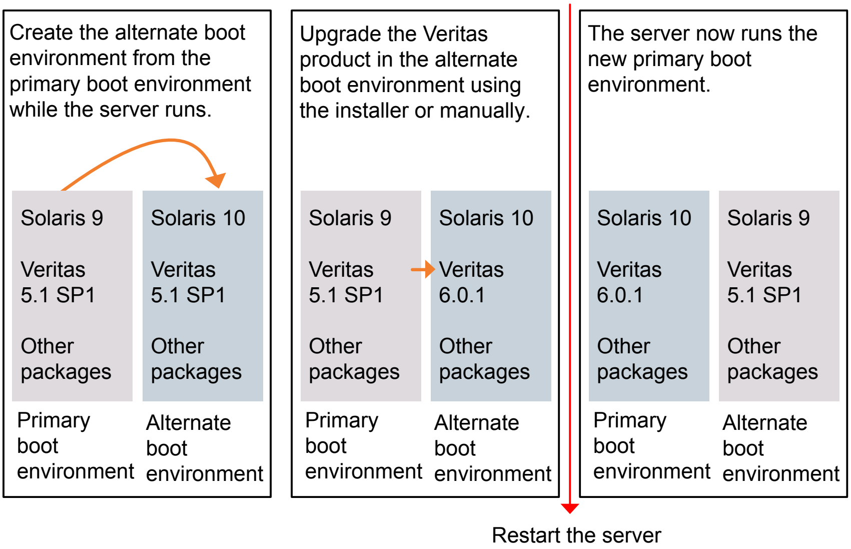
About Live Upgrade

You can use Live Upgrade on Solaris 10 systems to perform the following types of upgrade:

- Upgrade the operating system and SF.
  See "Upgrading SF and Solaris using Live Upgrade" on page 133.
- Upgrade the operating system.
  See "Upgrading Solaris using Live Upgrade" on page 140.
- Upgrade SF.
  See "Upgrading SF using Live Upgrade" on page 142.

Figure 14-1 illustrates an example of an upgrade of Veritas products from 5.1 SP1 to 6.0.1, and the operating system from Solaris 9 to Solaris 10.

Figure 14-1 Live Upgrade process


Create the alternate boot environment from the primary boot environment while the server runs.
Solaris 9
Veritas 5.1 SP1
Other packages
Solaris 10
Veritas 5.1 SP1
Other packages
Primary boot environment
Alternate boot environment
Upgrade the Veritas product in the alternate boot environment using the installer or manually.
Solaris 9
Veritas 5.1 SP1
Other packages
Solaris 10
Veritas 6.0.1
Other packages
Primary boot environment
Alternate boot environment
The server now runs the new primary boot environment.
Solaris 10
Veritas 6.0.1
Other packages
Solaris 9
Veritas 5.1 SP1
Other packages
Primary boot environment
Alternate boot environment
Restart the server

Some service groups (failover and parallel) may be online in this cluster and they are not affected by the Live Upgrade process. The only downtime experienced is when the server is rebooted to boot into the alternate boot disk.

About Live Upgrade in a Veritas Volume Replicator (VVR) environment

In a SF environment that uses Veritas Volume Replicator, the following scripts provide the means to upgrade the VVR configuration:

- vvr_upgrade_lu_start
- vvr_upgrade_lu_finish

This section provides an overview of the VVR upgrade process. See the Live Upgrade procedures for SF for the complete procedure.

See "Upgrading SF and Solaris using Live Upgrade" on page 133.

- Use the `vxlustart` script to perform upgrade steps for SF.
- Immediately before rebooting the system to switch over to the alternate boot environment, run the `vvr_upgrade_lu_start` script.

Note: Use the `vvr_upgrade_lu_start` script only when the applications are stopped and the next step is to switch over to the alternate boot environment.

- After the `vvr_upgrade_lu_start` script completes successfully, reboot the system. This reboot results in the system booting from the alternate boot environment.
- After the objects are recovered, and the disk group version is upgraded (if desired), run the `vvr_upgrade_lu_finish` script.

Supported upgrade paths for Live Upgrade

The systems where you plan to use Live Upgrade must run Solaris 9 or Solaris 10. You can upgrade from systems that run Solaris 9, but SF 6.0.1 is not supported on Solaris 9. Live Upgrade is not supported on Solaris 11.

For Solaris 10, make sure that all non-global zones are booted and in the installed state before you use the Symantec product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.

For Live Upgrade, if the alternative root environment also has a zone, you cannot install `VRTSodm`. You must remove the `VRTSodm` package first then install the Storage Foundation product. After you reboot the alternative root, you can install `VRTSodm`.

SF version must be at least 5.0 MP3.

Symantec requires that both global and non-global zones run the same version of Veritas products.

Note: If you use Live Upgrade on a system where non-global zones are configured, make sure that all the zones are in the `installed` state before you start Live Upgrade.

You can use Live Upgrade in the following virtualized environments:

Table 14-1 Live Upgrade support in virtualized environments

Environment	Procedure
Solaris native zones	Perform Live Upgrade to upgrade both global and non-global zones. If you have a zone root that resides on a VxVM volume, use the following procedure. See "Performing Live Upgrade in a Solaris zone environment" on page 128. Use the standard procedure for the other standby nodes. See "Upgrading SF and Solaris using Live Upgrade" on page 133.
Solaris branded zones (BrandZ)	Perform Live Upgrade to upgrade the global zone. See "Upgrading SF and Solaris using Live Upgrade" on page 133. Manually upgrade the branded zone separately. Note that while you can perform a Live Upgrade in the presence of branded zones, the branded zones are not upgraded.
Oracle VM Server for SPARC	Perform Live Upgrade on the Control domain only. Perform Live Upgrade on the Guest domain only. Use the standard Live Upgrade procedure for both types of logical domains. See "Upgrading SF and Solaris using Live Upgrade" on page 133.

Performing Live Upgrade in a Solaris zone environment

If you have a zone root that resides on a VxVM volume, then you must use the following procedure to perform a Live Upgrade on the nodes where zones are online.

Use the standard procedure for the other standby nodes.

See "Upgrading SF and Solaris using Live Upgrade" on page 133.

To perform a Live Upgrade on a node that has a zone root on a VxVM volume

1 Unmount all file systems that do not contain local zone root.

2 By default, Zone agent `BootState` is set to "multi-user."

Shut down any application that runs on local zone. Leave the zone running.

Note: Symantec recommends that you set `BootState` to "multi-user-server" to run applications inside non-global zones.

---

3 Make sure that the boot environment disk has enough space for local zone root being copied over during the Live Upgrade.

4 Follow the instruction to upgrade using Live Upgrade (which includes vxlustart, the product upgrade, and vxlufinish).

Before rebooting the systems to complete the Live Upgrade, perform the following steps.

5 On the system that houses the local zone, copy all files and directories before the upgrade on the local zone root to another location.

```
# zoneadm list -cv
  ID NAME              STATUS     PATH             BRAND    IP
   0 global            running    /                native   shared
   6 ora-lzone         running    /oralzones       native   shared
# zoneadm -z ora-lzone halt
# cd /oralzones
# ls
dev  lost+found root SUNWattached.xml
# mv dev dev.41
# mv root root.41
# mv SUNWattached.xml SUNWattached.xml.41
```

6. Migrate all files and directories after the upgrade on the local zone root on BE using the tar utility:

   ```
   # cd /altroot.5.10/oralzones
   # ls
   dev  lost+found lu root SUNWattached.xml
   # tar cf - . | (cd /oralzones; tar xfBp -)
   # cd /oralzones
   # ls
   dev .41 lost+found root.41  SUNWattached.xml.41
   dev  lost+found lu root SUNWattached.xml
   ```

7. Shut down the system.

Before you upgrade SF using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

Note: Upgrade of SF using Solaris Live Upgrade is not suported with Solaris 11.

To prepare for the Live Upgrade

1. Make sure that the SF 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.
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. 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.

The `vxlustart` script is located on the distribution media, in the scripts directory.

```
# cd /cdrom/scripts
```

```
# ./vxlustart -V -u targetos_version -s osimage_path -d diskname
```

-V Lists the commands to be executed during the upgrade process without executing them and pre-checks the validity of the command.

If the operating system is being upgraded, the user will be prompted to compare the patches that are installed on the image with the patches installed on the primary boot disk to determine if any critical patches are missing from the new operating system image.

-u Specifies the operating system version for the upgrade on the alternate boot disk. For example, use `5.10` for Solaris 10.

-U Specifies that only the Storage Foundation products are upgraded. The operating system is cloned from the primary boot disk.

-s Indicates the path of the operating system image to be installed on the alternate boot disk. If this option is omitted, you are prompted to insert the discs that contain the operating system image.

If the `-U` option is specified, you can omit the **-s** option. The operating system is cloned from the primary boot disk.

-d Indicates the name of the alternate boot disk on which you intend to upgrade. If you do not specify this option with the script, you are prompted for the disk information.

-v Indicates verbose, the executing commands display before they run.

-Y Indicates a default yes with no questions asked.

-D Prints with debug option on, and is for debugging.

-F Specifies the rootdisk's file system, where the default is `ufs`.

-t Specifies the number of CDs involved in upgrade.

-r Specifies that if the machine crashes or reboots before the `vxlufinish` command is run, the alternate disk is remounted using this option.

For example, to preview the commands to upgrade only the Veritas 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.

In the procedure examples, the primary or current boot environment resides on Disk0 (c0t0d0s0) and the alternate or inactive boot environment resides on Disk1 (c0t1d0s0).

Upgrading SF and Solaris using Live Upgrade

Perform the Live Upgrade manually or use the installer.

Upgrading SF using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See "Before you upgrade SF using Solaris Live Upgrade" on page 130.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 134.
- Upgrade to Storage Foundation 6.0.1 on the alternate boot environment manually or using the installer.

  To upgrade SF manually, refer to the following procedure:

  - See "Upgrading SF manually" on page 136.

  To upgrade SF using the installer, refer to the following procedure:

  - See “Upgrading SF using the installer for a Live Upgrade” on page 135.
- Switch the alternate boot environment to be the new primary.
  See “Completing the Live Upgrade ” on page 138.
- Verify Live Upgrade of SF.
  See “Verifying Live Upgrade of SF” on page 140.

Creating a new boot environment on the alternate boot disk

Run the `vxlustart` command to create a new boot environment on the alternate boot disk.

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

1 Navigate to the install media for the Symantec products:

```
# cd /cdrom/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 Veritas 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 Veritas product only:

```
# ./vxlustart -v -u 5.10 -U -d disk_name
```

The options to the `vxlustart` command are listed in the preupgrade section.

See "Before you upgrade SF using Solaris Live Upgrade" on page 130.

For example, to upgrade to Solaris 10 update 6:

```
# ./vxlustart -v -u 5.10 -s /mnt/Solaris_10u6
```

4 Review the output 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 Veritas product installation:

```
# pkgadd -R /altroot.5.10 -d pkg_dir
```

Upgrading SF using the installer for a Live Upgrade

You can use the Veritas product installer to upgrade SF as part of the Live Upgrade.

At the end of the process the following occurs:

- Storage Foundation 6.0.1 is installed on the alternate boot disk.

To perform Live Upgrade of SF using the installer

1. Insert the product disc with Storage Foundation 6.0.1 or access your copy of the software on the network.

2. Run the installer script specifying the root path as the alternate boot disk:

   ```
   # ./installsf -upgrade -rootpath /altroot.5.10
   ```

   See "Removing and reinstalling SF using the installer" on page 141.

3. Enter the names of the nodes that you want to upgrade to Storage Foundation 6.0.1.

   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 installation.

   The installer displays the list of packages to be installed or upgraded on the nodes.

4. Press **Return** to continue with the installation.

5. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.1.

   ```
   # 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`.

Upgrading SF manually

You can perform a manual upgrade of SF using Live Upgrade.

At the end of the process the following occurs:

- Storage Foundation 6.0.1 is installed on the alternate boot disk.

To perform Live Upgrade of SF manually

1. Remove the SF packages on the alternate boot disk in the reverse order in which they were installed:

   -
     ```
     # pkgrm -R /altroot.5.10 \
     VRTSmapro VRTSgapms VRTSvxmsa VRTSfasag VRTSfas VRTSvail \
     VRTSfsmnd VRTSfssdk VRTSfsman VRTSvrw VRTSweb VRTSjre15 \
     ```

```
VRTSvcsvr VRTSvrpro VRTSddlpr VRTSvdid VRTSalloc VRTSdcli \
VRTSvmpro VRTSvmman VRTSfspro VRTSdsa VRTSvxvm VRTSvxfs \
VRTSspt VRTSaa VRTSmh VRTSccg VRTSobgui VRTSob VRTSobc33 \
VRTSat VRTSpbx VRTSicsco VRTSvlic VRTSperl
```

Note that this package list is an example. Full package lists vary from release to release and by product option.

- For Storage Foundation:

```
# pkgrm -R /altroot.5.10 \
VRTSmapro VRTSgapms VRTSvxmsa VRTSfasag VRTSfas VRTSvail \
VRTScmccc VRTScmcs VRTSacclib VRTScssim VRTScscm VRTScscw \
VRTSvcsmn VRTSvcsag VRTSvcsmg VRTSvcs VRTSvxfen VRTSgab \
VRTSllt VRTSfsmnd VRTSfssdk VRTSfsman VRTSvrw VRTSjre15 \
VRTSvcsvr VRTSvrpro VRTSddlpr VRTSvdid VRTSalloc VRTSdcli \
VRTSvmpro VRTSvmman VRTSfspro VRTSdsa VRTSvxvm VRTSvxfs \
VRTSspt VRTSaa VRTSmh VRTSccg VRTSobgui VRTSob VRTSobc33 \
VRTSat VRTSpbx VRTSicsco VRTSvlic VRTSperl
```

Note that this package list is an example. Full package lists vary from release to release and by product option.

The `-R` option removes the packages from the root path `/altroot.5.10` on the alternate boot disk.

2 Install the SF packages from the pkgs directory. You must install the packages in the following order one at a time to the alternate boot disk using the `pkgadd` command:

- For Storage Foundation:

```
VRTSvlic.pkg VRTSperl.pkg VRTSspt.pkg VRTSvxvm.pkg VRTSaslapm.pkg
VRTSob.pkg VRTSsfmh.pkg VRTSvxfs.pkg VRTSfssdk.pkg VRTSdbed.pkg
VRTSodm.pkg VRTSsfcpi601.pkg
```

For example:

```
# pkgadd -R /altroot.5.10 -d package_name.pkg
```

Where you replace *package_name.pkg* with a package's name, for example `VRTSperl.pkg`.

```
# pkgadd -R /altroot.5.10 -d VRTSperl.pkg
```

3 Verify that the version of the Veritas packages on the alternate boot disk is 6.0.1.

```
# pkginfo -R /altrootpath -l VRTSpkgname
```

For example:

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

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.

   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. 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.

3 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 2

```
# ./vxlufinish -u target_os_version
```

4 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.

---

5 Reboot the system. The boot environment on the alternate disk is activated when you restart the it.

Reboot 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.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

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

6 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.

See “Administering boot environments” on page 142.

7 After the upgrade, perform any required post-upgrade tasks such as upgrading the disk group.

8 After the objects are recovered, and the disk group version is upgraded (if desired), run the `vvr_upgrade_lu_finish` script.

Verifying Live Upgrade of SF

To ensure that Live Upgrade has completed successfully, vverify that the system have booted from the alternate boot environment.

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 "Reverting to the primary boot environment" on page 142.

2. Perform other verification as required to ensure that the new boot environment is configured correctly.

3. In a zone environment, verify the zone configuration.

Upgrading Solaris using Live Upgrade

If you are upgrading Solaris only, you must remove and reinstall SF from the alternate boot environment prior to completing the Live Upgrade. You must remove and reinstall because SF has kernel components that are specific to Solaris operating system versions. The correct version of the SF packages must be installed.

Upgrading Solaris using Live Upgrade involves the following steps:

- Preparing to upgrade using Solaris Live Upgrade.
  See "Before you upgrade SF using Solaris Live Upgrade" on page 130.
- Creating a new boot environment on the alternate boot disk
  See "Creating a new boot environment on the alternate boot disk" on page 134.
- Removing and reinstalling Storage Foundation 6.0.1 on the alternate boot environment:
  Using manual steps:
  See "Upgrading SF manually" on page 136.
  Using the installer:
  See "Removing and reinstalling SF using the installer" on page 141.

  Note: Do NOT configure the Storage Foundation 6.0.1

- Switching the alternate boot environment to be the new primary

See “Completing the Live Upgrade ” on page 138.

- Verifying Live Upgrade of SF.
  See “Verifying Live Upgrade of SF” on page 140.

Removing and reinstalling SF using the installer

SF has kernel components that are specific for Solaris operating system versions. When you use Solaris Live Upgrade to upgrade the Solaris operating system, you must complete these steps to ensure the correct version of SF components are installed.

Run the installer on the alternate boot disk to remove and reinstall Storage Foundation 6.0.1.

At the end of the process the following occurs:

- Storage Foundation 6.0.1 is installed on the alternate boot disk, with the correct binaries for the new operating system version

To remove and reinstall SF using the installer

1. Uninstall using the installer script, specifying the alternate boot disk as the root path:

   ```
   # /opt/VRTS/install/uninstallsf<version>
   -rootpath altrootpath
   ```

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

   See “About the Veritas installer” on page 25.

2. Enter the names of the nodes that you want to uninstall.

   The installer displays the list of packages that will be uninstalled.

3. Press **Return** to continue.

4. Install using the installer script, specifying the root path as the alternate boot disk as follows:

   ```
   # /cdrom/storage_foundation/installsf -install \
   -rootpath /altrootpath
   ```

5. Press **Return** to continue.

6. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.1.

   ```
   # 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/log`.

Upgrading SF using Live Upgrade

Perform the Live Upgrade manually or use the installer. The nodes will not form a cluster until all of the nodes are upgraded to Storage Foundation 6.0.1. 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 SF using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See "Before you upgrade SF using Solaris Live Upgrade" on page 130.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 134.
- Upgrade to Storage Foundation 6.0.1 on the alternate boot environment manually or using the installer. Refer to one of the following:

  To upgrade SF manually:

  - See "Upgrading SF manually" on page 136.

  To upgrade SF using the installer:

  - See "Upgrading SF using the installer for a Live Upgrade" on page 135.
- Switch the alternate boot environment to be the new primary.
  See "Completing the Live Upgrade " on page 138.
- Verify Live Upgrade of SF.
  See "Verifying Live Upgrade of SF" on page 140.

Administering boot environments

Use the following procedures to perform relevant administrative tasks for boot environments.

Reverting to the primary boot environment

If the alternate boot environment fails to start, you can revert to the primary boot environment.

Start the system from the primary boot environment in the PROM monitor mode.

```
ok> boot disk0
```

where *disk0* is the primary boot disk.

Switching the boot environment for Solaris SPARC

You do not have to perform the following procedures to switch the boot environment when you use the `vxlufinish` scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

Two different procedures exist to switch the boot environment, choose one of the following procedures based on the encapsulation of the root disk:

- See “To switch the boot environment if the root disk is not encapsulated” on page 144.
- See “To switch the boot environment if the root disk is encapsulated” on page 145.

The switching procedures for Solaris SPARC vary, depending on whether VxVM encapsulates the root disk.

To switch the boot environment if the root disk is not encapsulated

1 Display the status of Live Upgrade boot environments.

```
# lustatus

Boot Environment  Is       Active Active    Can    Copy
Name              Complete Now    On Reboot Delete Status
----------------  -------- ------ --------- ------ ------
source.2657       yes      yes    yes       no     -
dest.2657         yes      no     no        yes    -
```

In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657)

2 Unmount any file systems that are mounted on the alternate root disk (dest.2657).

```
# lufslist dest.2657

               boot environment name: dest.2657

Filesystem        fstype device size  Mounted on Mount Options
----------------- ------ ------------ ---------- -------------
/dev/dsk/c0t0d0s1 swap     4298342400 -          -
/dev/dsk/c0t0d0s0 ufs     15729328128 /          -
/dev/dsk/c0t0d0s5 ufs      8591474688 /var       -
/dev/dsk/c0t0d0s3 ufs      5371625472 /vxfs      -

# luumount dest.2657
```

3 Activate the Live Upgrade boot environment.

```
# luactivate dest.2657
```

4 Reboot the system.

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

The system automatically selects the boot environment entry that was activated.

To switch the boot environment if the root disk is encapsulated

1. Display the current boot disk device and device aliases

   ```
   # eeprom
   boot-device=vx-rootdg vx-int_disk
   use-nvramrc?=true
   nvramrc=devalias vx-int_disk /pci@1c,600000/scsi@2/disk@0,0:a
   devalias vx-rootdg01 /pci@1c,600000/scsi@2/disk@1,0:a
   ```

2. Set the device from which to boot using the eeprom command. This example shows booting from the primary root disk.

   ```
   # eeprom boot-device=vx-rootdg01
   ```

3. Reboot the system.

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

Switching the boot environment for Solaris x86-64

You do not have to perform the following procedures to switch the boot environment when you use the `vxlufinish` scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

Two different procedures exist to switch the boot environment, choose one of the following procedures based on the encapsulation of the root disk:

- See "To switch the boot environment if root disk is not encapsulated" on page 146.
- See "To switch the boot environment if root disk is encapsulated" on page 147.

To switch the boot environment if root disk is not encapsulated

1 Display the status of Live Upgrade boot environments.

```
# lustatus

Boot Environment Is       Active Active    Can    Copy
Name             Complete Now    On Reboot Delete Status
---------------- -------- ------ --------- ------ ------
source.2657      yes      yes    yes       no     -
dest.2657        yes      no     no        yes    -
```

In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657)

2 Unmount any file systems that are mounted on the alternate root disk (dest.2657).

```
# lufslist dest.2657

               boot environment name: dest.2657

Filesystem        fstype device size  Mounted on Mount Options
----------------- ------ ------------ ---------- --------------
/dev/dsk/c0t0d0s1 swap    4298342400  -          -
/dev/dsk/c0t0d0s0 ufs    15729328128  /          -
/dev/dsk/c0t0d0s5 ufs     8591474688  /var       -
/dev/dsk/c0t0d0s3 ufs     5371625472  /vxfs      -
```

```
# luumount dest.2657
```

3 Activate the Live Upgrade boot environment.

```
# luactivate dest.2657
```

4 Reboot the system.

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

When the system boots up, the GRUB menu displays the following entries for the Live Upgrade boot environments:

```
source.2657
dest.2657
```

The system automatically selects the boot environment entry that was activated.

To switch the boot environment if root disk is encapsulated

◆ If the root disk is encapsulated, for releases before Solaris 10 update 6 (2.10u6), you can use the `luactivate` method. For Solaris 10 update 6 and subsequent Solaris 10 updates, do one of the following:

- Select the GRUB entry for the source boot environment or destination boot environment when the system is booted. You can also use the following procedure to manually set the default GRUB menu.lst entry to the source (PBE) or destination (ABE) grub entry:
- If the system is booted from the alternate boot environment, perform the following steps to switch to the primary boot environment:

  ```
  # mkdir /priroot
  # mount rootpath /priroot
  # bootadm list-menu -R /priroot
  # bootadm list-menu
  # bootadm set-menu -R /priroot default=PBE_menu_entry
  # bootadm set-menu default=PBE_menu_entry
  # shutdown -g0 -i6 -y
  ```

  Where:
  rootpath is the path to the root device, such as `/dev/vx/dsk/rootdg/rootvol`
  priroot is the primary root device
  PBE_menu_entry is the number of the primary boot environment in the GRUB menu.

- If the system is booted from the primary boot environment, perform the following steps to switch to the alternate boot environment:

  ```
  # bootadm list-menu
  # bootadm set-menu default=ABE_menu_entry
  ABE booting
  ```

Migrating from Storage Foundation Basic to Storage Foundation Standard

This chapter includes the following topics:

Migrating from Storage Foundation Basic to Storage Foundation Standard

Use this procedure to migrate from Storage Foundation (SF) Basic to Storage Foundation Standard.

To migrate from Storage Foundation Basic to Storage Foundation Standard

1 Log in as superuser on a system where you want to install Storage Foundation Standard.

2 Use the following command to confirm that you are currently running Storage Foundation Basic.

```
# /opt/VRTSvlic/bin/vxlicrep | grep  Basic
```

You should see the following output:

```
Product Name = VERITAS Storage Foundation Basic
```

3 Mount the installation media for Storage Foundation.

4 Run the installer command.

```
# ./installer
```

The installer will first execute a set of prechecks.

5 Make sure that the prechecks complete successfully. Make any changes that the installer recommends.

6 On the Installer Task menu, select **Install a Product**.

7 On the Product Selection menu, select **Veritas Storage Foundation**.

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

9 Select the package level to be installed.

From the menu, select the option that corresponds to **Install Recommended**.

10 You are prompted to enter the system names on which to install Storage Foundation Standard.

11 The installer prompts with a warning that Storage Foundation is already installed, and asks for confirmation to continue. Press **y** to continue the installation.

12 The installer will identify two additional packages to be installed, `VRTSodm` and `VRTSdbed`. Press Enter to continue.

13 After installing the packages in step 12, the installer will prompt if additional licenses need to be installed. Press **y** to continue.

You will be provided two options:

- `Enter a license key`
- `Utilize Keyless licensing`

14 If you chose to enter a license key, you should install the Storage Foundation Standard license key.

15 If you chose to utilize a keyless license, you will be asked to choose the version of Storage Foundation (Standard or Enterprise). Choose **Standard** to install a Storage Foundation Standard license.

The installer will go through the configuration and startup process.

16 Confirm if you want to send information about this installation to Symantec to help improve the installation in the future.

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

17 If desired, press **y** to view the summary file.

The migration is complete.

Chapter 16

Performing post-upgrade tasks

This chapter includes the following topics:

Optional configuration steps

After the upgrade is complete, additional tasks may need to be performed.

You can perform the following optional configuration steps:

- If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:
  - Reattach the RLINKs.
  - Associate the SRL.
- To encapsulate and mirror the boot disk, follow the procedures in the "Administering Disks" chapter of the *Veritas Storage Foundation Administrator's Guide*.
- To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.
  See "Upgrading VxVM disk group versions" on page 161.

Re-joining the backup boot disk group into the current disk group

Perform this procedure to rejoin the backup boot disk if you split the mirrored boot disk during upgrade. After a successful upgrade and reboot, you no longer need to keep the boot disk group backup.

To re-join the backup boot disk group

◆ Re-join the *backup_bootdg* disk group to the boot disk group.

```
# /etc/vx/bin/vxrootadm -Y join backup_bootdg
```

where the -Y option indicates a silent operation, and *backup_bootdg* is the name of the backup boot disk group that you created during the upgrade.

Reverting to the backup boot disk group after an unsuccessful upgrade

Perform this procedure if your upgrade was unsuccessful and you split the mirrored boot disk to back it up during upgrade. You can revert to the backup that you created when you upgraded.

To revert the backup boot disk group after an unsuccessful upgrade

1 To determine the boot disk groups, look for the *rootvol* volume in the output of the `vxprint` command.

```
# vxprint
```

2 Use the `vxdg` command to find the boot disk group where you are currently booted.

```
# vxdg bootdg
```

3 Boot the operating system from the backup boot disk group.

4 Join the original boot disk group to the backup disk group.

```
# /etc/vx/bin/vxrootadm -Y join original_bootdg
```

where the `-Y` option indicates a silent operation, and *original_bootdg* is the boot disk group that you no longer need.

Post upgrade tasks for migrating the SFDB repository database

Database Storage Checkpoints that have been created by using the SFDB tools before upgrade are visible using the `vxsfadm` CLI, and you can mount these Database Storage Checkpoints and roll back to them, if required. However, creating clones by using migrated Database Storage Checkpoints is not supported.

If you want to continue using previously created FlashSnap snapplans to take snapshots, you must validate them by using the `-o validate` option of the `vxsfadm` command.

To continue using the Database Storage Checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle, you must perform one of the following procedures after upgrading SF to 6.0.1:

- Rename startup script after upgrading from 5.0x and before migrating the SFDB repository
  See "After upgrading from 5.0.x and before migrating SFDB" on page 160.
- Migrate from a 5.0x SFDB repository database to 6.0.1
  See "Migrating from a 5.0 repository database to 6.0.1" on page 156.
- Migrate from a 5.1 or 5.1SP1 repository database to 6.0.1
  See "Migrating from a 5.1 or higher repository database to 6.0.1" on page 158.

Migrating from a 5.0 repository database to 6.0.1

To migrate from a 5.0 repository database to 6.0.1

1 Rename the startup script NO_S*vxdbms3 to S*vxdbms3.

See "After upgrading from 5.0.x and before migrating SFDB" on page 160.

2 As root, dump out the old 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
```

3 On the same node that you ran `sfua_rept_migrate` run the following command as Oracle user. For each Oracle instance, migrate the old repository data to the SQLite repository.

```
$ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

4 By default, the repository is created on the file system which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- Repository path has to be a directory writable by Oracle user.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

Create an alternate repository path.

```
$ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \
Alternate_path
```

5 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform the previous steps on the secondary host.

6 On the primary host, edit your snapplans to remove the "SNAPSHOT_DG=SNAP_*" parameter and add “SNAPSHOT_DG_PREFIX=SNAP_*". The parameter can be any PREFIX value and not necessarily "SNAP_*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=system1_data
SNAPSHOT_DG=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=judge_data
SNAPSHOT_DG_PREFIX=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

7. On the primary host, revalidate your snapshots using the following command:

   ```
   $ /opt/VRTS/bin/vxsfadm -s flashsnap \
   -a oracle -c SNAPPLAN -o validate
   ```

   This completes the migration of the repository for Database Storage Checkpoints and Database Tiered Storage parameters.

To begin using the Storage Foundation for Databases (SFDB) tools:

See *Storage Foundation: Storage and Availability Management for Oracle Databases*

Migrating from a 5.1 or higher repository database to 6.0.1

To migrate from a 5.0 repository database to 6.0.1

1. Run the following command as Oracle user. For each Oracle instance, migrate the old repository data to the SQLite repository.

   ```
   $ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME
   ```

2. By default, the repository is created on the file system which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

   - Repository path has to be a directory writable by Oracle user.
   - The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

   Create an alternate repository path.

   ```
   $ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \
   Alternate_path
   ```

3. If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform the previous steps on the secondary host.

4 On the primary host, edit your snapplans to remove the "SNAPSHOT_DG=SNAP_*" parameter and add “SNAPSHOT_DG_PREFIX=SNAP_*". The parameter can be any PREFIX value and not necessarily "SNAP_*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=system1_data
SNAPSHOT_DG=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=judge_data
SNAPSHOT_DG_PREFIX=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

5 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/vxsfadm -s flashsnap \
-a oracle -c SNAPPLAN -o validate
```

This completes the migration of the repository for Database Storage Checkpoints and Database Tiered Storage parameters.

To begin using the Storage Foundation for Databases (SFDB) tools:

See *Storage Foundation: Storage and Availability Management for Oracle Databases*

After upgrading from 5.0.x and before migrating SFDB

When upgrading from SF version 5.0 to SF 6.0.1 the S*vxdbms3 startup script is renamed to NO_S*vxdbms3. The S*vxdbms3 startup script is required by `sfua_rept_migrate`. Thus when `sfua_rept_migrate` is run, it is unable to find the S*vxdbms3 startup script and gives the error message:

```
/sbin/rc3.d/S*vxdbms3 not found
SFORA sfua_rept_migrate ERROR V-81-3558 File:  is missing.
SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.
```

To prevent S*vxdbms3 startup script error

◆ Rename the startup script NO_S*vxdbms3 to S*vxdbms3.

Recovering VVR if automatic upgrade fails

If the upgrade fails during the configuration phase, after displaying the VVR upgrade directory, the configuration needs to be restored before the next attempt. Run the scripts in the upgrade directory in the following order to restore the configuration:

```
# restoresrl
# adddcm
# srlprot
# attrlink
# start.rvg
```

After the configuration is restored, the current step can be retried.

Upgrading disk layout versions

In this release, you can create and mount only file systems with disk layout Version 7, 8, and 9. You can only local mount disk layout Version 6 only to upgrade to a later disk layout version.

Disk layout Version 6 has been deprecated and you cannot cluster mount an existing file system that has disk layout Version 6. To upgrade a cluster file system with disk layout Version 6, you must local mount the file system and then upgrade the file system using the `vxupgrade` utility to a later version.

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

Support for disk layout Version 4 and 5 has been removed. You must upgrade any existing file systems with disk layout Version 4 or 5 to disk layout Version 7 or later using the `vxfsconvert` command.

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

Note: Symantec recommends that you upgrade existing file systems to the highest supported disk layout version prior to upgrading to this release.

You can check which disk layout version your file system has by using the following command:

```
# fstyp -v /dev/vx/dsk/dg1/vol1 | grep -i version
```

For more information about disk layout versions, see the *Veritas Storage Foundation Administrator's Guide*.

Upgrading VxVM disk group versions

All Veritas Volume Manager disk groups have an associated version number. Each VxVM release supports a specific set of disk group versions. VxVM can import and perform tasks on disk groups with those versions. Some new features and tasks work only on disk groups with the current disk group version. Before you can perform the tasks or use the features, upgrade the existing disk groups.

For 6.0.1, the Veritas Volume Manager disk group version is different than in previous VxVM releases. Symantec recommends that you upgrade the disk group version if you upgraded from a previous VxVM release.

After upgrading to SF 6.0.1, you must upgrade any existing disk groups that are organized by ISP. Without the version upgrade, configuration query operations continue to work fine. However, configuration change operations will not function correctly.

For more information about ISP disk groups, refer to the *Veritas Storage Foundation Administrator's Guide*.

Use the following command to find the version of a disk group:

```
# vxdg list diskgroup
```

To upgrade a disk group to the current disk group version, use the following command:

```
# vxdg upgrade diskgroup
```

For more information about disk group versions, see the *Veritas Storage Foundation Administrator's Guide*.

Updating variables

In `/etc/profile`, update the `PATH` and `MANPATH` variables as needed.

MANPATH could include `/opt/VRTS/man` and PATH `/opt/VRTS/bin`.

Setting the default disk group

You may find it convenient to create a system-wide default disk group. The main benefit of creating a default disk group is that VxVM commands default to the default disk group. You do not need to use the `-g` option.

You can set the name of the default disk group after installation by running the following command on a system:

```
# vxdctl defaultdg diskgroup
```

See the *Veritas Storage Foundation Administrator’s Guide*.

Upgrading the Array Support Library

VxVM provides support for new disk arrays in the form of Array Support Library (ASL) software package.

Adding JBOD support for storage arrays for which there is not an ASL available

If an array is of type A/A-A, A/P or ALUA and a suitable ASL is not available, the array must be claimed as an JBOD of type A/P. This is to prevent path delays and

I/O failures arising. As JBODs are assumed to be type A/A by default, you must create appropriate JBOD entries for such arrays.

To configure an A/A-A, A/P or ALUA array as a JBOD

1. Stop all applications, such as databases, from accessing VxVM volumes that are configured on the array, and unmount all VxFS file systems and Storage Checkpoints that are configured on the array.
2. Add the array as a JBOD of type A/P:

   ```
   # vxddladm addjbod vid=SUN pid=T300 policy=ap
   ```

3. If you have not already done so, upgrade the Storage Foundation or VxVM software to 6.0.1. Device discovery will be performed during the upgrade, and the array will be claimed as a JBOD of appropriate type.

   If you have already upgraded your system to 6.0.1, run the following command to perform device discovery:

   ```
   # vxdctl enable
   ```

4. Verify that the array has been added with the policy set to `APdisk`:

   ```
   # vxddladm listjbod
   VID   PID     Opcode Page Code Page Offset SNO length Policy
   ============================================================
   SUN   T300    18     -1        36          12         APdisk
   ```

5. Check that the correct devices are listed for the array:

   ```
   # vxdisk list
   DEVICE     TYPE           DISK    GROUP    STATUS
   APdisk_0   auto:cdsdisk   -       -        online invalid
   APdisk_1   auto:cdsdisk   -       -        online invalid
   APdisk_2   auto:cdsdisk   -       -        online invalid
   ...
   ```

Unsuppressing DMP for EMC PowerPath disks

This section is only applicable if you are upgrading a system that includes EMC PowerPath disks.

In releases of VxVM before 4.1, a combination of DMP subpaths and the controllers of DMP subpaths were usually suppressed to prevent interference between DMP and the EMC PowerPath multi-pathing driver. Suppression has the effect of hiding these subpaths and their controllers from DMP, and as a result the disks on these subpaths and controllers cannot be seen by VxVM.

VxVM 4.1 and later releases have the ability to discover EMCpower disks, and configure them as autodiscovered disks that DMP recognizes are under the control of a separate multi-pathing driver. This has the benefit of allowing such disks to reconfigured in cluster-shareable disk groups. Before upgrading to VxVM 6.0.1, you must remove the suppression of the subpaths and controllers so that DMP can determine the association between EMCpower metadevices and `c#t#d#` disk devices.

In the following scenarios, you may need to unsuppress DMP subpaths and controllers:

- Converting a foreign disk
  See "Converting a foreign disk to auto:simple" on page 164.
- Converting a defined disk
  See "Converting a defined disk to auto:simple" on page 167.
- Converting a powervxvm disk
  See "Converting a powervxvm disk to auto:simple" on page 170.

Because emcpower disks are auto-discovered, the powervxvm script should be disabled and removed from the startup script. To remove the powervxvm script, use the command:

```
# powervxvm remove
```

Converting a foreign disk to auto:simple

Release 4.0 of VxVM provided the `vxddladm addforeign` command to configure foreign disks with default disk offsets for the private and public regions, and to define them as simple disks. A foreign disk must be manually converted to `auto:simple` format before upgrading to VxVM 6.0.1.

If the foreign disk is defined on a slice other than `s2`, you must copy the partition entry for that slice to that for `s0` and change the tag. If the tag of the original slice is changed, the status of the disk is seen as `online:aliased` after the upgrade.

The following example is used to illustrate the procedure. The `vxdisk list` command can be used to display the EMCpower disks that are known to VxVM:

```
# vxdisk list
DEVICE          TYPE            DISK     GROUP    STATUS
c6t0d12s2       auto:sliced     -        -        online
emcpower10c     simple          fdisk    fdg      online
...
```

The `vxprint` command is used to display information about the disk group, `fdg`:

```
# vxprint
Disk group: fdg
TY NAME   ASSOC       KSTATE  LENGTH    PLOFFS  STATE TUTIL0 PUTIL0
dg fdg    fdg         -       -         -       -     -      -
dm fdisk  emcpower10c -       17673456  -       -     -      -
...
```

To convert a foreign disk to `auto:simple` format

1. Stop all the volumes in the disk group, and then deport it:

   ```
   # vxvol -g fdg stopall
   # vxdg deport fdg
   ```

2. Use the `vxddladm` command to remove definitions for the foreign devices:

   ```
   # vxddladm rmforeign blockpath=/dev/dsk/emcpower10c \
     charpath=/dev/rdsk/emcpower10c
   ```

   If you now run the `vxdisk list` command, the EMCpower disk is no longer displayed:

   ```
   # vxdisk list
   DEVICE       TYPE           DISK    GROUP    STATUS
   c6t0d12s2    auto:sliced    -       -        online
   ...
   ```

3. Run the `vxprtvtoc` command to retrieve the partition table entry for the device:

   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/vtoc /dev/rdsk/emcpower10c
   ```

4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```
# /etc/vx/bin/vxedvtoc -f /tmp/vtoc /dev/rdsk/emcpower10c

# THE ORIGINAL PARTITIONING IS AS FOLLOWS:
# SLICE     TAG  FLAGS   START  SIZE
  0         0x0  0x201   0      0
  1         0x0  0x200   0      0
  2         0x5  0x201   0      17675520

# THE NEW PARTITIONING WILL BE AS FOLLOWS:
# SLICE     TAG  FLAGS    START  SIZE
  0         0xf  0x201    0      17675520
  1         0x0  0x200    0      0
  2         0x5  0x201    0      17675520

DO YOU WANT TO WRITE THIS TO THE DISK ? [Y/N] :Y
WRITING THE NEW VTOC TO THE DISK #
```

5 Upgrade to VxVM 6.0.1 using the appropriate upgrade procedure.

6. After upgrading VxVM, use the `vxdisk list` command to validate the conversion to `auto:simple` format:

```
# vxdisk list
DEVICE         TYPE           DISK    GROUP    STATUS
c6t0d12s2      auto:sliced    -       -        online
emcpower10s2   auto:simple    -       -        online
...
```

   To display the physical device that is associated with the metadevice, `emcpower10s2`, enter the following command:

```
# vxdmpadm getsubpaths dmpnodename=emcpower10s2
```

7. Import the disk group and start the volumes:

```
# vxdg import fdg
# vxvol -g fdg startall
```

   You can use the `vxdisk list` command to confirm that the disk status is displayed as `online:simple`:

```
# vxdisk list
DEVICE         TYPE           DISK    GROUP    STATUS
c6t0d12s2      auto:sliced    -       -        online
emcpower10s2   auto:simple    fdisk   fdg      online
```

Converting a defined disk to auto:simple

In VxVM 4.0, and particularly in prior releases, EMCpower disks could be defined by a persistent disk access record (`darec`), and identified as simple disks. If an EMCpower disk is defined with a persistent `darec`, it must be manually converted to `auto:simple` format before upgrading to VxVM 6.0.1.

If the defined disk is defined on a slice other than `s2`, you must copy the partition entry for that slice to that for `s0` and change the tag. If the tag of the original slice is changed, the status of the disk is seen as `online:aliased` after the upgrade.

The following example is used to illustrate the procedure. The `ls` command shows the mapping of the EMC disks to persistent disk access records:

```
# ls -l /dev/vx/dmp/emcdisk1
lrwxrwxrwx 1 root other 36 Sep 24 17:59 /dev/vx/dmp/emcdisk1->
/dev/dsk/c6t0d11s5
# ls -l /dev/vx/rdmp/emcdisk1
```

```
lrwxrwxrwx 1 root other 40Sep 24 17:59 /dev/vx/rdmp/emcdisk1->
/dev/dsk/c6t0d11s5
```

Here the fifth partition of `c6t0d11s5` is defined as the persistent disk access record `emcdisk1`.

The `vxdisk list` command can be used to display the EMCpower disks that are known to VxVM:

```
# vxdisk list
DEVICE        TYPE           DISK   GROUP   STATUS
c6t0d12s2     auto:sliced    -      -       online
emcdisk1      simple         fdisk  fdg     online
...
```

The `vxprint` command is used to display information about the disk group, `fdg`:

```
# vxprint
Disk group: fdg
TY NAME    ASSOC     KSTATE  LENGTH    PLOFFS  STATE TUTIL0 PUTIL0
dg fdg     fdg       -       -         -       -     -      -
dm fdisk   emcdisk1  -       17673456  -       -     -      -
...
```

To convert a disk with a persistent disk access record to auto:simple format

1. Stop all the volumes in the disk group, and then deport it:

   ```
   # vxvol -g fdg stopall
   # vxdg deport fdg
   ```

2. Use the `vxdisk rm` command to remove the persistent record definitions:

   ```
   # vxdisk rm emcdisk1
   ```

   If you now run the `vxdisk list` command, the EMCpower disk is no longer displayed:

   ```
   # vxdisk list
   DEVICE        TYPE           DISK   GROUP   STATUS
   c6t0d12s2     auto:sliced    -      -       online
   ...
   ```

3. Use the `vxprtvtoc` command to retrieve the partition table entry for the device:

   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/hdisk /dev/rdsk/c6t0d11s2
   ```

4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```
# /etc/vx/bin/vxedvtoc -f /tmp/hdisk /dev/rdsk/c6t0d11s2

# THE ORIGINAL PARTITIONING IS AS FOLLOWS:
# SLICE     TAG  FLAGS    START   SIZE
  4         0x0  0x200    0       0
  5         0x0  0x200    3591000 2100375
  6         0x0  0x200    0       0

# THE NEW PARTITIONING WILL BE AS FOLLOWS:
# SLICE     TAG  FLAGS    START   SIZE
  4         0x0  0x200    0       0
  5         0xf  0x200    3591000 2100375
  6         0x0  0x200    0       0

DO YOU WANT TO WRITE THIS TO THE DISK ? [Y/N] :Y
WRITING THE NEW VTOC TO THE DISK #
```

5 Upgrade to VxVM 6.0.1 using the appropriate upgrade procedure.

6. After upgrading VxVM, use the `vxdisk list` command to validate the conversion to `auto:simple` format:

   ```
   # vxdisk list
   DEVICE           TYPE           DISK  GROUP  STATUS
   c6t0d12s2        auto:sliced    -     -      online
   emcpower10s2     auto:simple    -     -      online:aliased
   ...
   ```

   To display the physical device that is associated with the metadevice, `emcpower10s2`, enter the following command:

   ```
   # vxdmpadm getsubpaths dmpnodename=emcpower10s2
   ```

7. Import the disk group and start the volumes:

   ```
   # vxdg import fdg
   # vxvol -g fdg startall
   ```

   You can use the `vxdisk list` command to confirm that the disk status is displayed as `online:simple`:

   ```
   # vxdisk list
   DEVICE            TYPE            DISK    GROUP  STATUS
   c6t0d12s2         auto:sliced     -       -      online
   emcpower10s2      auto:simple     fdisk   fdg    online:aliased
   ```

   To allow DMP to receive correct enquiry data, the common Serial Number (C-bit) Symmetrix Director parameter must be set to enabled.

Converting a powervxvm disk to auto:simple

In VxVM 4.0, and particularly in prior releases, EMCpower disks could be defined by a persistent disk access record (darec) using powervxvm script, and identified as simple disks. If an EMCpower disk is used using powervxvm, it must be manually converted to auto:simple format before upgrading to VxVM 6.0.1.

If there are any controllers or devices that are suppressed from VxVM as powervxvm requirement, then such controllers/disks must be unsuppressed. This is required for Veritas DMP to determine the association between PowerPath metanodes and their subpaths. After the conversion to auto:simple is complete, the powervxvm script is no longer useful, and should be disabled from startup script.

The following example is used to illustrate the procedure. The `ls` command shows the mapping of the EMC disks to persistent disk access records:

```
# ls -l /dev/vx/rdmp/
crw-------   1 root     root     260, 76 Feb  7 02:36 emcpower0c

# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
emcpower0c   simple          ppdsk01      ppdg         online

# vxprint
Disk group: fdg
TY NAME     ASSOC      KSTATE  LENGTH   PLOFFS STATE  TUTIL0 PUTIL0
dg ppdg     ppdg       -       -        -      -      -      -
dm ppdsk01  emcpower0c -       2094960  -      -      -      -
```

To convert an EMCpower disk (defined using powervxvm) to auto:simple format

1. Stop all the volumes in the disk group, and then deport it:

   ```
   # vxvol -g ppdg stopall
   # vxdg deport ppdg
   ```

2. Use the `vxdisk rm` command to remove all emcpower disks from VxVM:

   ```
   # vxdisk rm emcpower0c
   ```

   If you now run the `vxdisk list` command, the EMCpower disk is no longer displayed:

   ```
   # vxdisk list
   DEVICE       TYPE            DISK         GROUP        STATUS
   c6t0d12s2    auto:sliced       -            -          online
   ```

3. Use the `vxprtvtoc` command to retrieve the partition table entry for this device:

   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/vtoc /dev/vx/rdmp/emcpower0c
   ```

4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```
# /etc/vx/bin/vxedvtoc -f /tmp/vtoc /dev/vx/rdmp/emcpower0c
# THE ORIGINAL PARTITIONING IS AS FOLLOWS:
# SLICE     TAG  FLAGS   START  SIZE
  0         0x0  0x201   0      0
  1         0x0  0x200   0      0
  2         0x5  0x201   0      17675520

# THE NEW PARTITIONING WILL BE AS FOLLOWS:
# SLICE     TAG  FLAGS   START  SIZE
  0         0xf  0x201   0      17675520
  1         0x0  0x200   0      0
  2         0x5  0x201   0      17675520

DO YOU WANT TO WRITE THIS TO THE DISK ? [Y/N] :Y
WRITING THE NEW VTOC TO THE DISK #
```

5 Upgrade to VxVM 6.0.1 using the appropriate upgrade procedure.

6 After upgrading VxVM, use the `vxdisk list` command to validate the conversion to auto:simple format:

```
# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
emcpower0s2  auto:simple       -            -          online
```

7 Import the disk group and start the volumes.

```
# vxdg import ppdg
# vxvol -g ppdg startall
# vxdisk list

DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
emcpower0s2  auto:simple     ppdsk01       ppdg        online
```

Converting from QuickLog to Multi-Volume support

The 4.1 release of the Veritas File System is the last major release to support QuickLog. The Version 6 and later disk layouts do not support QuickLog. The functionality provided by the Veritas Multi-Volume Support (MVS) feature replaces most of the functionality provided by QuickLog.

The following procedure describes how to convert from QuickLog to MVS. Unlike QuickLog, which allowed logging of up to 31 VxFS file systems to one device, MVS allows intent logging of only one file system per device. Therefore, the following procedure must be performed for each file system that is logged to a QuickLog device if the Version 6 or later disk layout is used.

The QuickLog device did not need to be related to the file system. For MVS, the log volume and the file system volume must be in the same disk group.

To convert Quicklog to MVS

1. Select a QuickLog-enabled file system to convert to MVS and unmount it.

   ```
   # umount myfs
   ```

2. Detach one of the QuickLog volumes from the QuickLog device that the file system had been using. This volume will be used as the new intent log volume for the file system.

   ```
   # qlogdetach -g diskgroup log_vol
   ```

3. Create the volume set.

   ```
   # vxvset make myvset myfs_volume
   ```

4. Mount the volume set.

   ```
   # mount -F vxfs /dev/vx/dsk/rootdg/myvset /mnt1
   ```

5. Upgrade the volume set’s file system to the Version 7 or later disk layout.

   For example:

   ```
   # vxupgrade -n 9 /mnt1
   ```

6. Add the log volume from step 2 to the volume set.

   ```
   # vxvset addvol myvset log_vol
   ```

7 Add the log volume to the file system. The size of the volume must be specified.

```
# fsvoladm add /mnt1 log_vol 50m
```

8 Move the log to the new volume.

```
# fsadm -o logdev=log_vol,logsize=16m /mnt1
```

Verifying the Storage Foundation upgrade

Refer to the section about verifying the installation to verify the upgrade.

See "Verifying that the products were installed" on page 179.

Section 4

Post-installation tasks

Chapter 17

Performing post-installation tasks

This chapter includes the following topics:

- Changing root user into root role

Changing root user into root role

On Oracle Solaris 11, to perform installation, you need to create root user. This means that a local user cannot assume the root role. After installation, you may want to turn root user into root role for a local user, who can log in as root.

1. Log in as root user.
2. Change the root account into role:

```
# rolemod -K type=role root
# getent user_attr root

root::::type=role;auths=solaris.*;profiles=All;audit_flags=lo\
:no;lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

3. Assign the root role to a local user who was unassigned the role:

```
# usermod -R root admin
```

For more information, see the Oracle documentation on Oracle Solaris 11 operating system.

Chapter 18

Verifying the SF installation

This chapter includes the following topics:

Verifying that the products were installed

Verify that the SF products are installed.

Use the pkginfo (Solaris 10) or pkg info (Solaris 11) command to check which packages have been installed.

Solaris 10:

```
# pkginfo -l VRTSvlic package_name package_name ...
```

Solaris 11:

```
# pkg info -| VRTSvlic package_name package_name
```

You can verify the version of the installed product. Use the following command:

```
# /opt/VRTS/install/installsf<version>
```

Where <version> is the specific release version.

See "About the Veritas installer" on page 25.

Use the following sections to further verify the product installation.

Installation log files

After every product installation, the installer creates three text files:

- Installation log file
- Response file
- Summary file

The name and location of each file is displayed at the end of a product installation, and are always located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep the files for auditing, debugging, and future use.

Using the installation log file

The installation log file contains all commands executed during the procedure, their output, and errors generated by the commands. This file is for debugging installation problems and can be used for analysis by Veritas Support.

Using the summary file

The summary file contains the results of the installation by the installer or product installation scripts. The summary includes the list of the packages, and the status (success or failure) of each package. The summary also indicates which processes were stopped or restarted during the installation. After installation, refer to the summary file to determine whether any processes need to be started.

Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

To stop the processes

- Use the `-stop` option to stop the product installation script.

  For example, to stop the product's processes, enter the following command:

  ```
  # ./installer -stop
  ```

  or

  ```
  # /opt/VRTS/install/installsf<version> -stop
  ```

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

  See "About the Veritas installer" on page 25.

To start the processes

- Use the `-start` option to start the product installation script.

  For example, to start the product's processes, enter the following command:

  ```
  # ./installer -start
  ```

  or

  ```
  # /opt/VRTS/install/installsf<version> -start
  ```

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

  See "About the Veritas installer" on page 25.

Checking Veritas Volume Manager processes

Use the following procedure to verify that Volume Manager processes are running.

To confirm that key Volume Manager processes are running

- Type the following command:

  ```
  # ps -ef | grep vx
  ```

  Entries for the `vxconfigd`, `vxnotify`, `vxesd`, `vxrelocd`, `vxcached`, and `vxconfigbackupd` processes should appear in the output from this command. If you disable hot-relocation, the `vxrelocd` and `vxnotify` processes are not displayed.

  For more details on hot relocation, see *Veritas Storage Foundation Administrator's Guide*.

Checking Veritas File System installation

The Veritas File System package consists of a kernel component and administrative commands.

Verifying Veritas File System kernel installation

To ensure that the file system driver is loaded, enter:

```
# modinfo | grep vxfs
```

The modinfo command displays information about all modules loaded on the system. If the vxfs module is loaded, you will see an entry corresponding to vxfs. If not, follow the instructions load and then unload the file system module to complete the process.

See "Loading and unloading the file system module" on page 83.

Verifying command installation

Table 18-1 lists the directories with Veritas File System commands.

Table 18-1 VxFS command locations

Location	Contents
/etc/fs/vxfs	Contains the Veritas mount command and QuickLog commands required to mount file systems.
/usr/lib/fs/vxfs/bin	Contains the VxFS type-specific switch-out commands.
/opt/VRTSvxfs/sbin	Contains the Veritas-specific commands.
/opt/VRTS/bin	Contains symbolic links to all Veritas-specific commands installed in the directories listed above.

Determine whether these subdirectories are present:

```
# ls /etc/fs/vxfs
# ls /usr/lib/fs/vxfs/bin
# ls /opt/VRTSvxfs/sbin
# ls /opt/VRTS/bin
```

Make sure you have adjusted the environment variables accordingly.

See "Setting environment variables" on page 38.

Section 5

Uninstallation of SF

Chapter 19

Uninstalling Storage Foundation

This chapter includes the following topics:

About removing Storage Foundation

This section covers uninstallation requirements and steps to uninstall the Veritas software.

Only users with superuser privileges can uninstall Storage Foundation.

Warning: Failure to follow the instructions in the following sections may result in unexpected behavior.

Preparing to uninstall

Review the following removing the Veritas software.

Preparing to remove Veritas Volume Manager

This section describes the steps you need to take before removing Veritas Volume Manager (VxVM) to preserve the contents of the volumes.

Warning: Failure to follow the preparations in this section might result in unexpected behavior.

Moving volumes from an encapsulated root disk

Use the following procedure to move volumes from an encapsulated root disk.

To uninstall VxVM if root, swap, usr, or var is a volume under Volume Manager control

1 Ensure that the `rootvol`, `swapvol`, `usr`, and `var` volumes have only one associated plex each.

   The plex must be contiguous, non-striped, non-spanned, and non-sparse. To obtain this information, enter the following:

   ```
   # vxprint -ht rootvol swapvol usr var
   ```

   If any of these volumes have more than one associated plex, remove the unnecessary plexes using the following command:

   ```
   # vxplex -o rm dis plex_name
   ```

2 Run the `vxunroot` command:

   ```
   # /etc/vx/bin/vxunroot
   ```

   The `vxunroot` command changes the volume entries in `/etc/vfstab` to the underlying disk partitions for `rootvol`, `swapvol`, `usr`, and `var`. It also modifies `/etc/system` and prompts for a reboot so that disk partitions are mounted instead of volumes for `root`, `swap`, `usr`, and `var`.

3 Once you have changed the `root`, `swap`, `usr`, and `var` volumes, move all remaining volumes to disk partitions.

   You can do this using one of the following procedures:

   - Back up the entire system to tape and then recover from tape.

- Back up each file system individually and then recover them all after creating new file systems on disk partitions.
- Move volumes incrementally to disk partitions.
  See "Moving volumes to disk partitions" on page 187.
  Otherwise, shut down VxVM.

Moving volumes to disk partitions

Use the following procedure to move volumes incrementally to disk partitions.

To move volumes incrementally to disk partitions

1. Evacuate disks using `vxdiskadm`, the VOM GUI, or the `vxevac` utility.

   Evacuation moves subdisks from the specified disks to target disks. The evacuated disks provide the initial free disk space for volumes to be moved to disk partitions.

2. Remove the evacuated disks from VxVM control by entering:

   ```
   # vxdg rmdisk diskname
   # vxdisk rm devname
   ```

3. Decide which volume to move first, and if the volume is mounted, unmount it.

4. If the volume is being used as a raw partition for database applications, make sure that the application is not updating the volume and that you have applied the `sync` command to the data on the volume.

5. Create a partition on free disk space of the same size as the volume using the `format` command.

   If there is not enough free space for the partition, add a new disk to the system for the first volume removed. Subsequent volumes can use the free space generated by the removal of this first volume.

6. Copy the data on the volume onto the newly created disk partition using a command such as `dd`.

   ```
   # dd if=/dev/vx/dsk/diskgroup/lhome of=/dev/dsk/c2t2d2s7
   ```

   where `c2t2d2` is the disk outside of Volume Manager and `s7` is the newly created partition.

7. Replace the entry for that volume (if present) in `/etc/vfstab` with an entry for the newly created partition.

8. Mount the disk partition if the corresponding volume was previously mounted.

9 Stop and remove the volume from VxVM using the commands.

```
# vxvol -g diskgroup stop volume_name
# vxedit -rf rm volume_name
```

10 Remove any free disks (those having no subdisks defined on them) by removing the volumes from VxVM control.

To check if there are still some subdisks remaining on a particular disk, use the `vxprint` command.

```
# vxprint -g diskgroup -F '%sdnum' diskname
```

If the output is not 0, there are still some subdisks on this disk that you need to remove. If the output is 0, remove the disk from VxVM control.

```
# vxdg rmdisk diskname
# vxdisk rm devname
```

Use the free space created for adding the data from the next volume you want to remove.

11 After you successfully convert all volumes into disk partitions, reboot the system.

12 After the reboot, make sure none of the volumes are open by using the `vxprint` command.

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

13 If any volumes remain open, repeat the steps listed above.

Example of moving volumes to disk partitions on Solaris

This example shows how to move the data on a volume to a disk partition. In the example, there are three disks: `disk1` and `disk2` are subdisks on volume `vol01` and `disk3` is a free disk. The data on `vol01` is copied to `disk3` using `vxevac`.

These are the contents of the disk group `voldg` before the data on `vol01` is copied to `disk3`.

```
# vxprint -g voldg -ht
DG NAME   NCONFIG   NLOG     MINORS   GROUP-ID
DM NAME   DEVICE    TYPE     PRIVLEN  PUBLEN   STATE
RV NAME   RLINK_CNT KSTATE   STATE    PRIMARY  DATAVOLS  SRL
RL NAME   RVG       KSTATE   STATE    REM_HOST REM_DG    REM_RLNK
V  NAME   RVG       KSTATE   STATE    LENGTH   READPOL   PREFPLEX UTYPE
```

```
PL NAME  VOLUME    KSTATE  STATE    LENGTH   LAYOUT    NCOL/WID MODE
SD NAME  PLEX      DISK    DISKOFFS LENGTH   [COL/]OFF DEVICE   MODE
SV NAME  PLEX      VOLNAME NVOLLAYR LENGTH   [COL/]OFF AM/NM    MODE
DC NAME  PARENTVOL LOGVOL
SP NAME  SNAPVOL   DCO

dg voldg default   default 115000
1017856044.1141.hostname.veritas.com

dm disk1 c1t12d0s2 sliced  2591     17900352 -
dm disk2 c1t14d0s2 sliced  2591     17899056 -
dm disk3 c1t3d0s2  sliced  2591     17899056 -

v  vol1  -         ENABLED ACTIVE   4196448  ROUND     -        fsgen
pl pl1   vol1      ENABLED ACTIVE   4196448  CONCAT    -        RW
sd sd1   pl1       disk1   0        2098224  0         c1t12d0  ENA
sd sd2   pl1       disk2   0        2098224  2098224   c1t14d0  ENA
```

Evacuate `disk1` to `disk3`.

```
# /etc/vx/bin/vxevac -g voldg disk1 disk3
# vxprint -g voldg -ht

DG NAME  NCONFIG    NLOG     MINORS   GROUP-ID
DM NAME  DEVICE     TYPE     PRIVLEN  PUBLEN   STATE
RV NAME  RLINK_CNT  KSTATE   STATE    PRIMARY  DATAVOLS  SRL
RL NAME  RVG        KSTATE   STATE    REM_HOST REM_DG    REM_RLNK
V  NAME  RVG        KSTATE   STATE    LENGTH   READPOL   PREFPLEX  UTYPE
PL NAME  VOLUME     KSTATE   STATE    LENGTH   LAYOUT    NCOL/WID  MODE
SD NAME  PLEX       DISK     DISKOFFS LENGTH   [COL/]OFF DEVICE    MODE
SV NAME  PLEX       VOLNAME  NVOLLAYR LENGTH   [COL/]OFF AM/NM     MODE
DC NAME  PARENTVOL  LOGVOL
SP NAME  SNAPVOL    DCO

dg voldg default    default  115000
1017856044.1141.hostname.veritas.com

dm disk1 c1t12d0s2  sliced   2591     17900352 -
dm disk2 c1t14d0s2  sliced   2591     17899056 -
dm disk3 c1t3d0s2   sliced   2591     17899056 -

v  vol1  -          ENABLED  ACTIVE   4196448  ROUND     -         fsgen
pl pl1   vol1       ENABLED  ACTIVE   4196448  CONCAT    -         RW
```

```
sd disk3-01l1       disk3    0        2098224  0         c1t3d0    ENA
sd sd2   pl1        disk2    0        2098224  2098224   c1t14d0   ENA
```

Evacuate `disk2` to `disk3`.

```
# /etc/vx/bin/vxevac -g voldg disk2 disk3
# vxprint -g voldg -ht

DG NAME      NCONFIG   NLOG    MINORS   GROUP-ID
DM NAME      DEVICE    TYPE    PRIVLEN  PUBLEN   STATE
RV NAME      RLINK_CNT KSTATE  STATE    PRIMARY  DATAVOLS  SRL
RL NAME      RVG       KSTATE  STATE    REM_HOST REM_DG    REM_RLNK
V  NAME      RVG       KSTATE  STATE    LENGTH   READPOL   PREFPLEX UTYPE
PL NAME      VOLUME    KSTATE  STATE    LENGTH   LAYOUT    NCOL/WID MODE
SD NAME      PLEX      DISK    DISKOFFS LENGTH   [COL/]OFF DEVICE   MODE
SV NAME      PLEX      VOLNAME NVOLLAYR LENGTH   [COL/]OFF AM/NM    MODE
DC NAME      PARENTVOL LOGVOL
SP NAME      SNAPVOL   DCO

dg voldg    default   default 115000
1017856044.1141.hostname.veritas.com

dm disk1    c1t12d0s2 sliced  2591    17900352 -
dm disk2    c1t14d0s2 sliced  2591    17899056 -
dm disk3    c1t3d0s2  sliced  2591    17899056 -

v  vol1     -         ENABLED ACTIVE  4196448  ROUND   -      fsgen
pl pl1      vol1      ENABLED ACTIVE  4196448  CONCAT  -      RW
sd disk3-01 pl1       disk3   0       2098224  0       c1t3d0 ENA
sd disk3-02 pl1       disk3   2098224 2098224  2098224 c1t3d0 ENA
```

Remove the evacuated disks from VxVM control.

```
# vxdisk -g voldg list
DEVICE      TYPE      DISK         GROUP        STATUS
c1t3d0s2    sliced    disk3        voldg        online
c1t12d0s2   sliced    disk1        voldg        online
c1t14d0s2   sliced    disk2        voldg        online

# vxdg rmdisk disk1
# vxdg rmdisk disk2
# vxdisk rm c1t12d0
# vxdisk rm c1t14d0
```

Verify that the evacuated disks have been removed from VxVM control.

```
# vxdisk -g voldg list
DEVICE       TYPE      DISK         GROUP        STATUS
c1t3d0s2     sliced    disk3        voldg        online
```

Check to see whether the volume you want to move first is mounted.

```
# mount | grep vol1
/vol1 on /dev/vx/dsk/voldg/vol1
read/write/setuid/log/nolargefiles/dev=12dc138 on Wed Apr
3 10:13:11 2002
```

Create a partition on free disk space of the same size as the volume. In this example, a 2G partition is created on `disk1` (`c1t12d0s1`).

```
# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
     0. c0t0d0 <SUN9.0G cyl 4924 alt 2 hd 27 sec 133>
        /sbus@1f,0/SUNW,fas@e,8800000/sd@0,0
     1. c1t3d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@3,0
     2. c1t9d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@9,0
     3. c1t10d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@a,0
     4. c1t11d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@b,0
     5. c1t12d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@c,0
     6. c1t14d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@e,0
     7. c1t15d0 <QUANTUM-ATLASIV9SCA-0808 cyl 13814 alt 2 hd 4 sec 324>
        /sbus@1f,0/SUNW,fas@2,8800000/sd@f,0
Specify disk (enter its number): 5
selecting c1t12d0
[disk formatted]

FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
        save       - save new disk/partition definitions
        inquiry    - show vendor, product and revision
        volname    - set 8-character volume name
        !<cmd>     - execute <cmd>, then return
        quit
format> p

PARTITION MENU:
        0      - change '0' partition
        1      - change '1' partition
        2      - change '2' partition
        3      - change '3' partition
        4      - change '4' partition
        5      - change '5' partition
        6      - change '6' partition
        7      - change '7' partition
        select - select a predefined table
        modify - modify a predefined partition table
        name   - name the current table
        print  - display the current table
        label  - write partition map and label to the disk
        !<cmd> - execute <cmd>, then return
        quit
partition> 1
Part      Tag    Flag    Cylinders     Size          Blocks
  1 unassigned    wm      0            0       (0/0/0)            0
Enter partition id tag[unassigned]:
Enter partition permission flags[wm]:
Enter new starting cyl[0]:
Enter partition size[0b, 0c, 0.00mb, 0.00gb]: 2.00gb
partition> l
Ready to label disk, continue? y

partition> p
Current partition table (unnamed):
```

```
Total disk cylinders available: 13814 + 2 (reserved cylinders)
Part      Tag    Flag    Cylinders     Size          Blocks
  0 unassigned    wm      0            0       (0/0/0)           0
  1 unassigned    wm      0 -  3236    2.00GB  (3237/0/0)   4195152
partition> q
```

Copy the data on vol01 to the newly created disk partition.

```
# dd if=/dev/vx/dsk/voldg/vol01 of=/dev/dsk/c1t12d0s1
```

In the /etc/vfstab file, remove the following entry.

```
/dev/vx/dsk/voldg/vol1 /dev/vx/rdsk/voldg/vol1 /vol1 vxfs 4 yes rw
```

Replace it with an entry for the newly created partition.

```
/dev/dsk/c1t12d0s1 /dev/rdsk/c1t12d0s1 /vol01 vxfs 4  yes rw
```

Mount the disk partition.

```
# mount -F vxfs /dev/dsk/c1t12d0s1 /vol01
```

Remove vol01 from VxVM.

```
# vxedit -rf rm /dev/vx/dsk/voldg/vol01
```

To complete the procedure, follow the remaining steps.

Preparing to remove Veritas File System

The VRTSvxfs package cannot be removed if there are any mounted VxFS file systems or Storage Checkpoints. Unmount the VxFS file systems and Storage Checkpoints before uninstalling Veritas Storage Foundation. After you remove the VRTSvxfs package, VxFS file systems are not mountable or accessible until another VRTSvxfs package is installed.

To unmount a file system

1. Check if any VxFS file systems are mounted.

   ```
   # cat /etc/mnttab | grep vxfs
   ```

2. Unmount any file systems.

   ```
   # umount special | mount_point
   ```

   Specify the file system to be unmounted as a *mount_point* or *special* (the device on which the file system resides). See the `umount_vxfs`(1M) manual page for more information about this command and its available options.

   You can use the `-a` option to unmount all file systems except `/`, `/usr`, `/usr/kvm`, `/var`, `/proc`, `/dev/fd`, and `/tmp`.

To unmount a Storage Checkpoint

1. Check if any Storage Checkpoints are mounted.

   ```
   # cat /etc/mnttab | grep vxfs
   ```

2. Unmount any Storage Checkpoints.

   ```
   # umount /checkpoint_name
   ```

Removing the Replicated Data Set

If you use VVR, you need to perform the following steps. This section gives the steps to remove a Replicated Data Set (RDS) when the application is either active or stopped.

Note: If you are upgrading Veritas Volume Replicator, do not remove the Replicated Data Set.

To remove the Replicated Data Set

1. Verify that all RLINKs are up-to-date:

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

   If the Secondary is not required to be up-to-date, proceed to 2 and stop replication using the `-f` option with the `vradmin stoprep` command.

2. Stop replication to the Secondary by issuing the following command on any host in the RDS:

   The `vradmin stoprep` command fails if the Primary and Secondary RLINKs are not up-to-date. Use the `-f` option to stop replication to a Secondary even when the RLINKs are not up-to-date.

   ```
   # vradmin -g diskgroup stoprep local_rvgname sec_hostname
   ```

   The argument `local_rvgname` is the name of the RVG on the local host and represents its RDS.

   The argument `sec_hostname` is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

3. Remove the Secondary from the RDS by issuing the following command on any host in the RDS:

   ```
   # vradmin -g diskgroup delsec local_rvgname sec_hostname
   ```

   The argument local_rvgname is the name of the RVG on the local host and represents its RDS.

   The argument sec_hostname is the name of the Secondary host as displayed in the output of the `vradmin printrvg` command.

4. Remove the Primary from the RDS by issuing the following command on the Primary:

   ```
   # vradmin -g diskgroup delpri local_rvgname
   ```

   When used with the `-f` option, the `vradmin delpri` command removes the Primary even when the application is running on the Primary.

   The RDS is removed.

5. If you want to delete the SRLs from the Primary and Secondary hosts in the RDS, issue the following command on the Primary and all Secondaries:

   ```
   # vxedit -r -g diskgroup rm srl_name
   ```

Uninstalling SF packages using the script-based installer

Use the following procedure to remove SF products.

Not all packages may be installed on your system depending on the choices that you made when you installed the software.

Note: After you uninstall the product, you cannot access any file systems you created using the default disk layout version in SF 6.0.1 with a previous version of SF.

Language packages are uninstalled when you uninstall the English language packages.

To shut down and remove the installed SF packages

1. Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/vfstab`. Failing to remove these entries could result in system boot problems later.
2. Unmount all mount points for VxFS file systems.

   ```
   # umount /mount_point
   ```

3. If the VxVM package (`VRTSvxvm`) is installed, read and follow the uninstallation procedures for VxVM.

   See "Preparing to remove Veritas Volume Manager" on page 186.
4. Make sure you have performed all of the prerequisite steps.
5. Move to the `/opt/VRTS/install` directory and run the uninstall script.

   ```
   # cd /opt/VRTS/install
   ```

   ```
   # ./uninstallsf<version>
   ```

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

   Or, if you are using ssh or rsh, use one of the following:

   - `# ./uninstallsf<version> -rsh`
   - `# ./uninstallsf<version> -ssh`

   See "About the Veritas installer" on page 25.

6 The uninstall script prompts for the system name. Enter one or more system names, separated by a space, from which to uninstall SF, for example, `sys1`:

```
Enter the system names separated by spaces: [q?] sys1 sys2
```

7 The uninstall script prompts you to stop the product processes. If you respond yes, the processes are stopped and the packages are uninstalled.

The uninstall script creates log files and displays the location of the log files.

8 Most packages have kernel components. In order to ensure complete removal, a system reboot is recommended after all packages have been removed.

9 To verify the removal of the packages, use the `pkginfo` command.

```
# pkginfo | grep VRTS
```

Uninstalling SF with the Veritas Web-based installer

This section describes how to uninstall using the Veritas Web-based installer.

Note: After you uninstall the product, you cannot access any file systems you created using the default disk layout Version in SF 6.0.1 with a previous version of SF.

To uninstall SF

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 48.

3 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.

4 Select **Storage Foundation** from the Product drop-down list, and click **Next**.

5 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Next**.

6 After the validation completes successfully, click **Next** to uninstall SF 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 products from the specified system.

Click **Next**.

9 After the uninstall 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.

10 Click **Finish**.

Most packages have kernel components. In order to ensure their complete removal, a system reboot is recommended after all the packages have been removed.

Uninstalling Storage Foundation using the pkgrm or pkg uninstall command

Use the following procedure to uninstall Storage Foundation using the pkgrm command.

If you are uninstalling Storage Foundation using the pkgrm command, the packages must be removed in a specific order, or else the uninstallation will fail. Removing the packages out of order will result in some errors, including possible core dumps, although the packages will still be removed.

To uninstall Storage Foundation

1 Unmount all VxFS file systems and Storage Checkpoints, and close all VxVM volumes.

Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/vfstab`. Failing to remove these entries could result in system boot problems later.

2 Unmount all mount points for VxFS file systems and Storage Checkpoints.

```
# umount /mount_point
```

3 Stop all applications from accessing VxVM volumes, and close all VxVM volumes.

4 Stop various daemons, if applicable.

```
# /opt/VRTS/bin/vxsvcctrl stop
```

5 Remove the packages in the following order:

- For Storage Foundation (Solaris 10):

```
# pkgrm VRTSodm VRTSdbed VRTSfssdk \
VRTSvxfs VRTSsfmh VRTSob VRTSaslapm VRTSvxvm \
VRTSspt VRTSperl VRTSvlic
```

- For Storage Foundation (Solaris 11):

```
# pkg uninstall VRTSodm VRTSdbed VRTSfssdk \
VRTSvxfs VRTSsfmh VRTSob VRTSaslapm VRTSvxvm \
VRTSspt VRTSperl VRTSvlic
```

Uninstalling the language packages using the pkgrm command

If you would like to remove only the language packages, you can do so with the `pkgrm` command.

If you use the product installer menu or the uninstallation script, you can remove the language packages along with the English packages.

To remove the language packages

◆ Use the `pkgrm` command to remove the appropriate packages.

See "Chinese language packages" on page 238.

See "Japanese language packages" on page 238.

```
# pkgrm package_name package_name ...
```

Because the packages do not contain any dependencies, you can remove them in any order.

Removing the Storage Foundation for Databases (SFDB) repository after removing the product

After removing the product, you can remove the SFDB repository file and any backups.

Removing the SFDB repository file disables the SFDB tools.

To remove the SFDB repository

1 Identify the SFDB repositories created on the host.

```
# cat /var/vx/vxdba/rep_loc
```

2 Remove the directory identified by the `location` key.

3 Remove the repository location file.

```
# rm -rf /var/vx/vxdba/rep_loc
```

This completes the removal of the SFDB repository.

Uninstalling SF using response files

This chapter includes the following topics:

Uninstalling SF using response files

Typically, you can use the response file that the installer generates after you perform SF uninstallation on one system to uninstall SF on other systems.

To perform an automated uninstallation

1. Make sure that you meet the prerequisites to uninstall SF.
2. Copy the response file to one of the cluster systems where you want to uninstall SF.
3. Edit the values of the response file variables as necessary.
4. Start the uninstallation from the system to which you copied the response file. For example:

   ```
   # /opt/VRTS/install/uninstallsf<version>
    -responsefile /tmp/response_file
   ```

   Where <version> is the specific release version, and /tmp/*response_file* is the response file's full path name.

   See "About the Veritas installer" on page 25.

Response file variables to uninstall Storage Foundation

Table 20-1 lists the response file variables that you can define to configure SF.

Table 20-1 Response file variables for uninstalling SF

Variable	Description
CFG{systems}	List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required
CFG{prod}	Defines the product to be installed or uninstalled. List or scalar: scalar Optional or required: required
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional
CFG{opt}{uninstall}	Uninstalls SF packages. List or scalar: scalar Optional or required: optional

Sample response file for SF uninstallation

The following example shows a response file for uninstalling Storage Foundation.

```
our %CFG;

$CFG{opt}{redirect}=1;
$CFG{opt}{uninstall}=1;
$CFG{prod}="SF601";
$CFG{systems}=[ qw(thoropt89 thoropt90) ];

1;
```

Section 6

Installation reference

Appendix A

Installation scripts

This appendix includes the following topics:

- Installation script options

Installation script options

Table A-1 shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Veritas Storage Foundation product scripts, except where otherwise noted.

See "About the Veritas installer" on page 25.

Table A-1 Available command line options

Commandline Option	Function
-allpkgs	Displays all packages required for the specified product. The packages are listed in correct installation order. The output can be used to create scripts for command line installs, or for installations over a network.
-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.
-configure	Configures the product after installation.
–hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.

Table A-1 Available command line options *(continued)*

Commandline Option	Function
-installallpkgs	The `-installallpkgs` option is used to select all packages.
-installrecpkgs	The `-installrecpkgs`option is used to select the recommended packages set.
–installminpkgs	The `-installminpkgs`option is used to select the minimum packages set.
-ignorepatchreqs	The `-ignorepatchreqs` option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
–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.
–keyfile *ssh_key_file*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
-license	Registers or updates product licenses on the specified systems.
–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.
-makeresponsefile	Use the `-makeresponsefile` option only to generate response files. No actual software installation occurs when you use this option.
-minpkgs	Displays the minimal packages required for the specified product. The packages are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
-nolic	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.

Table A-1 Available command line options *(continued)*

Commandline Option	Function
–pkginfo	Displays a list of packages and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS packages.
–pkgpath *package_path*	Designates the path of a directory that contains all packages to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–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.
–postcheck	Checks for different HA and file system-related processes, the availability of different ports, and the availability of cluster-related service groups.
-precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.
–recpkgs	Displays the recommended packages required for the specified product. The packages are listed in correct installation order. Optional packages are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See `allpkgs` option.
-redirect	Displays progress details without showing the progress bar.
-requirements	The `-requirements` option displays required OS version, required packages and patches, file system space, and other system requirements in order to install the product.

Table A-1 Available command line options *(continued)*

Commandline Option	Function
–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.
–rootpath *root_path*	Specifies an alternative root directory on which to install packages. On Solaris operating systems, `-rootpath` passes `-R path` to `pkgadd` command.
-rsh	Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP. See “About configuring secure shell or remote shell communication modes before installing products” on page 227.
–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.
-settunables	Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the `-tunablesfile` option.
-start	Starts the daemons and processes for the specified product.
-stop	Stops the daemons and processes for the specified product.

Table A-1 Available command line options *(continued)*

Commandline Option	Function
-timeout	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 prevents the script from timing out. The `-timeout` option does not work with the `-serial option`
–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.
-tunables	Lists all supported tunables and create a tunables file template.
-tunables_file *tunables_file*	Specify this option when you specify a tunables file. The tunables file should include tunable parameters.
-upgrade	Specifies that an existing version of the product exists and you plan to upgrade it.
-version	Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.

Tunable files for installation

This appendix includes the following topics:

About setting tunable parameters using the installer or a response file

You can set non-default product and system tunable parameters using a tunables file. With the file, you can set tunables such as the I/O policy or toggle native multi-pathing. The tunables file passes arguments to the installer script to set tunables. With the file, you can set the tunables for the following operations:

- When you install, configure, or upgrade systems.

  ```
  # ./installer -tunablesfile tunables_file_name
  ```

  See "Setting tunables for an installation, configuration, or upgrade" on page 214.

- When you apply the tunables file with no other installer-related operations.

  ```
  # ./installer -tunablesfile tunables_file_name -settunables [
  system1 system2 ...]
  ```

See “Setting tunables with no other installer-related operations” on page 215.

- When you apply the tunables file with an un-integrated response file.

  ```
  # ./installer -responsefile response_file_name -tunablesfile
  tunables_file_name
  ```

  See “Setting tunables with an un-integrated response file” on page 216.

See “About response files” on page 24.

You must select the tunables that you want to use from this guide.

See “Tunables value parameter definitions” on page 218.

Setting tunables for an installation, configuration, or upgrade

You can use a tunables file for installation procedures to set non-default tunables. You invoke the installation script with the `tunablesfile` option. The tunables file passes arguments to the script to set the selected tunables. You must select the tunables that you want to use from this guide.

See “Tunables value parameter definitions” on page 218.

Note: Certain tunables only take effect after a system reboot.

To set the non-default tunables for an installation, configuration, or upgrade

1. Prepare the tunables file.

   See “Preparing the tunables file” on page 217.

2. Make sure the systems where you want to install SF meet the installation requirements.

3. Complete any preinstallation tasks.

4. Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.

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

6. Start the installer for the installation, configuration, or upgrade. For example:

   ```
   # ./installer -tunablesfile /tmp/tunables_file
   ```

   Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with no other installer-related operations

You can use the installer to set tunable parameters without any other installer-related operations. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 218.

Note: Certain tunables only take effect after a system reboot.

To set tunables with no other installer-related operations

1 Prepare the tunables file.

See "Preparing the tunables file" on page 217.

2 Make sure the systems where you want to install SF meet the installation requirements.

3 Complete any preinstallation tasks.

4 Copy the tunables file to one of the systems that you want to tune.

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

6 Start the installer with the `-settunables` option.

```
# ./installer -tunablesfile tunables_file_name -settunables [
sys123 sys234 ...]
```

Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 218.

Note: Certain tunables only take effect after a system reboot.

To set tunables with an un-integrated response file

1 Make sure the systems where you want to install SF meet the installation requirements.

2 Complete any preinstallation tasks.

3 Prepare the tunables file.

See "Preparing the tunables file" on page 217.

4 Copy the tunables file to one of the systems that you want to tune.

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

6 Start the installer with the `-responsefile` and `-tunablesfile` options.

```
# ./installer -responsefile response_file_name -tunablesfile
tunables_file_name
```

Where *response_file_name* is the full path name for the response file and *tunables_file_name* is the full path name for the tunables file.

7 Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

You can use the installer to create a tunables file template, or manually format tunables files you create.

To create a tunables file template

- Start the installer with the `-tunables` option. Enter the following:

```
# ./installer -tunables
```

You see a list of all supported tunables, and the location of the tunables file template.

To manually format tunables files

- Format the tunable parameter as follows:

```
$TUN{"tunable_name"}{"system_name"|"*"}=value_of_tunable;
```

For the *system_name*, use the name of the system, its IP address, or a wildcard symbol. The *value_of_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```
#
# Tunable Parameter Values:
#
our %TUN;

$TUN{"tunable1"}{"*"}=1024;
$TUN{"tunable3"}{"sys123"}="SHA256";

1;
```

Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See "Tunables value parameter definitions" on page 218.

Each line for the parameter value starts with $TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{"dmp_daemon_count"}{"node123"}=16;
```

In this example, you are changing the dmp_daemon_count value from its default of 10 to 16. You can use the wildcard symbol "*" for all systems. For example:

```
$TUN{"dmp_daemon_count"}{"*"}=16;
```

Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Veritas Storage Foundation and High Availability Solutions Tuning Guide* for detailed information on product tunable ranges and recommendations .

Table B-1 describes the supported tunable parameters that can be specified in a tunables file.

Table B-1 Supported tunable parameters

Tunable	Description
dmp_cache_open	(Veritas Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_daemon_count	(Veritas Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_delayq_interval	(Veritas Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
dmp_fast_recovery	(Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_health_time	(Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_log_level	(Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_low_impact_probe	(Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_lun_retry_timeout	(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_fabric	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_ownership	(Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_multipathing	(Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
dmp_native_support	(Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_path_age	(Veritas Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_pathswitch_blks_shift	(Veritas Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_idle_lun	(Veritas Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_threshold	(Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_cycles	(Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_interval	(Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_policy	(Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_state	(Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
dmp_retry_count	(Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_scsi_timeout	(Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_sfg_threshold	(Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_stat_interval	(Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
max_diskq	(Veritas File System) Specifies the maximum disk queue generated by a single file. The installer sets only the system default value of max_diskq. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_ahead	(Veritas File System) The 0 value disables read ahead functionality, the 1 value (default) retains traditional sequential read ahead behavior, and the 2 value enables enhanced read ahead for all reads. The installer sets only the system default value of read_ahead. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_nstream	(Veritas File System) The number of parallel read requests of size read_pref_io that can be outstanding at one time. The installer sets only the system default value of read_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_pref_io	(Veritas File System) The preferred read request size. The installer sets only the system default value of read_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
vol_checkpt_default	(Veritas File System) Size of VxVM storage checkpoints (sectors). This tunable requires system reboot to take effect.
vol_cmpres_enabled	(Veritas Volume Manager) Allow enabling compression for VERITAS Volume Replicator.
vol_cmpres_threads	(Veritas Volume Manager) Maximum number of compression threads for VERITAS Volume Replicator.
vol_default_iodelay	(Veritas Volume Manager) Time to pause between I/O requests from VxVM utilities (10ms units). This tunable requires system reboot to take effect.
vol_fmr_logsz	(Veritas Volume Manager) Maximum size of bitmap Fast Mirror Resync uses to track changed blocks (KBytes). This tunable requires system reboot to take effect.
vol_max_adminio_poolsz	(Veritas Volume Manager) Maximum amount of memory used by VxVM admin I/O's (bytes). This tunablle rquires system reboot to take effect.
vol_max_nmpool_sz	(Veritas Volume Manager) Maximum name pool size (bytes).
vol_max_rdback_sz	(Veritas Volume Manager) Storage Record readback pool maximum (bytes).
vol_max_wrspool_sz	(Veritas Volume Manager) Maximum memory used in clustered version of VERITAS Volume Replicator (bytes).
vol_maxio	(Veritas Volume Manager) Maximum size of logical VxVM I/O operations (sectors). This tunable requires system reboot to take effect.
vol_maxioctl	(Veritas Volume Manager) Maximum size of data passed into the VxVM ioctl calls (bytes). This tunable requires system reboot to take effect.
vol_maxparallelio	(Veritas Volume Manager) Number of I/O operations vxconfigd can request at one time. This tunable requires system reboot to take effect.
vol_maxspecialio	(Veritas Volume Manager) Maximum size of a VxVM I/O operation issued by an ioctl call (sectors). This tunable requires system reboot to take effect.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
vol_min_lowmem_sz	(Veritas Volume Manager) Low water mark for memory (bytes).
vol_nm_hb_timeout	(Veritas Volume Manager) Veritas Volume Replicator timeout value (ticks).
vol_rvio_maxpool_sz	(Veritas Volume Manager) Maximum memory requested by VERITAS Volume Replicator (bytes).
vol_stats_enable	(Veritas Volume Manager) Enable VxVM I/O stat collection.
vol_subdisk_num	(Veritas Volume Manager) Maximum number of subdisks attached to a single VxVM plex. This tunable requires system reboot to take effect.
voldrl_max_drtregs	(Veritas Volume Manager) Maximum number of dirty VxVM regions that can exist on a non-sequential DRL. This tunable requires system reboot to take effect.
voldrl_max_seq_dirty	(Veritas Volume Manager) Maximum number of dirty regions in sequential mode. This tunable requires system reboot to take effect.
voldrl_min_regionsz	(Veritas Volume Manager) Minimum size of a VxVM Dirty Region Logging (DRL) region (sectors). This tunable requires system reboot to take effect.
voldrl_volumemax_drtregs	(Veritas Volume Manager) Max per volume dirty regions in log-plex DRL.
voldrl_volumemax_drtregs_20	(Veritas Volume Manager) Max per volume dirty regions in DCO version 20.
voldrl_dirty_regions	(Veritas Volume Manager) Number of regions cached for DCO version 30.
voliomem_chunk_size	(Veritas Volume Manager) Size of VxVM memory allocation requests (bytes). This tunable requires system reboot to take effect.
voliomem_maxpool_sz	(Veritas Volume Manager) Maximum amount of memory used by VxVM (bytes). This tunable requires system reboot to take effect.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
voliot_errbuf_dflt	(Veritas Volume Manager) Size of a VxVM error trace buffer (bytes). This tunable requires system reboot to take effect.
voliot_iobuf_default	(Veritas Volume Manager) Default size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect.
voliot_iobuf_limit	(Veritas Volume Manager) Maximum total size of all VxVM I/O trace buffers (bytes). This tunable requires system reboot to take effect.
voliot_iobuf_max	(Veritas Volume Manager) Maximum size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect.
voliot_max_open	(Veritas Volume Manager) Maximum number of VxVM trace channels available for vxtrace commands. This tunable requires system reboot to take effect.
volpagemod_max_memsz	(Veritas Volume Manager) Maximum paging module memory used by Instant Snapshots (Kbytes).
volraid_rsrtransmax	(Veritas Volume Manager) Maximum number of VxVM RAID-5 transient reconstruct operations in parallel. This tunable requires system reboot to take effect.
vx_era_nthreads	(Veritas File System) Maximum number of threads VxFS will detect read_ahead patterns on. This tunable requires system reboot to take effect.
vx_bc_bufhwm	(Veritas File System) VxFS metadata buffer cache high water mark. This tunable requires system reboot to take effect.
vxfs_ninode	(Veritas File System) Number of entries in the VxFS inode table. This tunable requires system reboot to take effect.
write_nstream	(Veritas File System) The number of parallel write requests of size write_pref_io that can be outstanding at one time. The installer sets only the system default value of write_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.

Table B-1 Supported tunable parameters *(continued)*

Tunable	Description
write_pref_io	(Veritas File System) The preferred write request size. The installer sets only the system default value of write_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.

Appendix C

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

About configuring secure shell or remote shell communication modes before installing products

Establishing communication between nodes is required to install Veritas software from a remote system, or to install and configure a system. The system from which the installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Veritas software.

You can install products to remote systems using either secure shell (ssh) or remote shell (rsh). Symantec recommends that you use ssh as it is more secure than rsh.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (system1) that contains the installation directories, and a target system (system2). This procedure also applies to multiple target systems.

Note: The script- and Web-based installers support establishing passwordless communication for you.

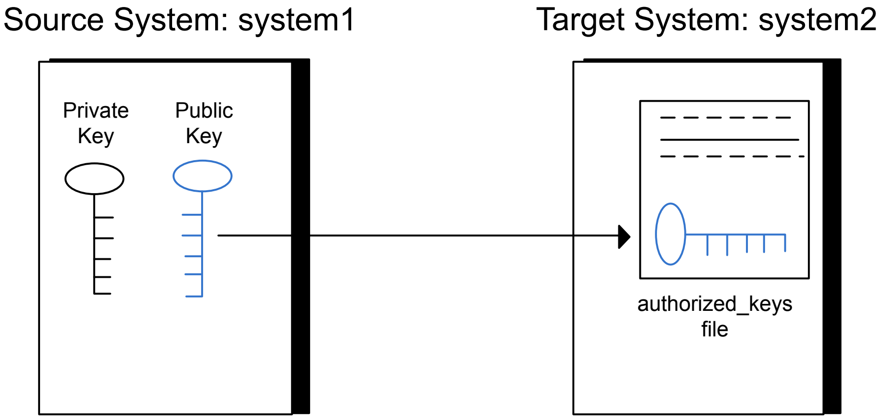
Manually configuring and passwordless ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the authorized_keys file on the target systems.

Figure C-1 illustrates this procedure.

Figure C-1 Creating the DSA key pair and appending it to target systems



Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: http://openssh.org to access online manuals and other resources.

To create the DSA key pair

1 On the source system (system1), log in as root, and navigate to the root directory.

```
system1 # cd /
```

2 Make sure the `/.ssh` directory is on all the target installation systems (system2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

Solaris 10:

```
system2 # mkdir /.ssh
```

Solaris 11:

```
system2 # mkdir /root/.ssh
```

Change the permissions of this directory, to secure it.

Solaris 10:

```
system2 # chmod go-w /.ssh
```

Solaris 11:

```
system2 # chmod go-w /root/.ssh
```

3 To generate a DSA key pair on the source system, type the following command:

```
system1 # ssh-keygen -t dsa
```

System output similar to the following is displayed:

```
Generating public/private dsa key pair.
Enter file in which to save the key (//.ssh/id_dsa):
```

For Solaris 11:

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
```

4 Press Enter to accept the default location of `/.ssh/id_dsa`.

5 When the program asks you to enter the passphrase, press the Enter key twice.

```
Enter passphrase (empty for no passphrase):
```

Do not enter a passphrase. Press Enter.

```
Enter same passphrase again:
```

Press Enter again.

To append the public key from the source system to the authorized_keys file on the target system, using secure file transfer

1 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (system2 in this example).

To enable SFTP, the `/etc/ssh/sshd_config` file must contain the following two lines:

```
PermitRootLogin           yes
  Subsystem          sftp      /usr/lib/ssh/sftp-server
```

2 If the lines are not there, add them and restart ssh.

To restart ssh on Solaris 10 and Solaris 11, type the following command:

```
system1 # svcadm restart ssh
```

3 From the source system (system1), move the public key to a temporary file on the target system (system2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
system1 # sftp system2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to system2 ...
The authenticity of host 'system2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

4 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'system2,10.182.00.00'
(DSA) to the list of known hosts.
root@system2 password:
```

5 Enter the root password of system2.

6 At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

7 To quit the SFTP session, type the following command:

```
sftp> quit
```

8 To begin the ssh session on the target system (system2 in this example), type the following command on system1:

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

9 After you log in to system2, enter the following command to append the id_dsa.pub file to the authorized_keys file:

```
system2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

10 After the id_dsa.pub public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the id_dsa.pub public key file, enter the following command on system2:

```
system2 # rm /id_dsa.pub
```

11 To log out of the ssh session, enter the following command:

```
system2 # exit
```

12 When you install from a source system that is also an installation target, also add the local system id_dsa.pub key to the local authorized_keys file. The installation can fail if the installation source system is not authenticated.

To add the local system id_dsa.pub key to the local authorized_keys file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

13 Run the following commands on the source installation system. If your ssh session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user root:

```
system1 # exec /usr/bin/ssh-agent $SHELL
system1 # ssh-add

  Identity added: //.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

1. On the source system (system1), enter the following command:

   ```
   system1 # ssh -l root system2 uname -a
   ```

   where system2 is the name of the target system.

2. The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.

3. Repeat this procedure for each target system.

Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

To restart ssh

1. On the source installation system (system1), bring the private key into the shell environment.

   ```
   system1 # exec /usr/bin/ssh-agent $SHELL
   ```

2. Make the key globally available for the user `root`

   ```
   system1 # ssh-add
   ```

Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system.

Veritas recommends configuring a secure shell environment for Veritas product installations.

See “Manually configuring and passwordless ssh” on page 228.

See the operating system documentation for more information on configuring remote shell.

To enable rsh

1. To determine the current status of `rsh` and `rlogin`, type the following command:

   ```
   # inetadm | grep -i login
   ```

   If the service is enabled, the following line is displayed:

   ```
   enabled online svc:/network/login:rlogin
   ```

   If the service is not enabled, the following line is displayed:

   ```
   disabled disabled svc:/network/login:rlogin
   ```

2. To enable a disabled `rsh`/`rlogin` service, type the following command:

   ```
   # inetadm -e rlogin
   ```

3. To disable an enabled `rsh`/`rlogin` service, type the following command:

   ```
   # inetadm -d rlogin
   ```

4. Modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. This file must be modified for each user who remotely accesses the system using rsh. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access `system1` from `system2`, you must add an entry for `system2.`*`companyname`*`.com` in the `.rhosts` file on `system1`.

   ```
   # echo "system2.companyname.com" >> $HOME/.rhosts
   ```

5. After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

   ```
   # rm -f $HOME/.rhosts
   ```

Appendix D

Storage Foundation components

This appendix includes the following topics:

- Storage Foundation installation packages
- Chinese language packages
- Japanese language packages
- Veritas Storage Foundation obsolete and reorganized installation packages

Storage Foundation installation packages

Table D-1 shows the package name and contents for each English language package for Storage Foundation. The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and Veritas Cluster Server (VCS) packages, the combined functionality is called Storage Foundation and High Availability.

Table D-1 Storage Foundation packages

packages	Contents	Configuration
VRTSaslapm	Veritas Array Support Library (ASL) and Array Policy Module(APM) binaries Required for the support and compatibility of various storage arrays.	Minimum

Table D-1 Storage Foundation packages *(continued)*

packages	Contents	Configuration
VRTSperl	Perl 5.14.2 for Veritas	Minimum
VRTSvlic	Veritas License Utilities Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.	Minimum
VRTSvxfs	Veritas File System binaries Required for VxFS file system support.	Minimum
VRTSvxvm	Veritas Volume Manager binaries, scripts, and utilities. Required for VxVM volume manager support.	Minimum
VRTSdbed	Veritas Storage Foundation for Databases	Recommended
VRTSob	Veritas Enterprise Administrator	Recommended
VRTSodm	Veritas ODM Driver for VxFS Veritas Extension for Oracle Disk Manager is a custom storage interface designed specifically for Oracle9i and 10g. Oracle Disk Manager allows Oracle 9i and 10g to improve performance and manage system bandwidth.	Recommended

Table D-1 Storage Foundation packages *(continued)*

packages	Contents	Configuration
VRTSsfcpi601	Veritas Storage Foundation Common Product Installer The Storage Foundation Common Product installer package contains the installer libraries and product scripts that perform the following: ■ installation ■ configuration ■ upgrade ■ uninstallation ■ adding nodes ■ removing nodes ■ etc. You can use these script to simplify the native operating system installations, configurations, and upgrades.	Minimum
VRTSsfmh	Veritas Storage Foundation Managed Host Veritas Storage Foundation Managed Host is now called Veritas Operations Manager (VOM). Discovers configuration information on a Storage Foundation managed host. If you want a central server to manage and monitor this managed host, download and install the VRTSsfmcs package on a server, and add this managed host to the Central Server. The VRTSsfmcs package is not part of this release. You can download it separately from: http://www.symantec.com/veritas-operations-manager	Recommended
VRTSspt	Veritas Software Support Tools	Recommended
VRTSfsadv	Minimum Veritas File System Advanced Solutions by Symantec (Solaris SPARC only).	Minimum

Table D-1 Storage Foundation packages *(continued)*

packages	Contents	Configuration
VRTSfssdk	Veritas File System Software Developer Kit For VxFS APIs, the package contains the public Software Developer Kit (headers, libraries, and sample code). It is required if some user programs use VxFS APIs.	All

Chinese language packages

The following table shows the package name and contents for each Chinese language package.

Table D-2 Chinese language packages

package	Contents
VRTSzhvm	Chinese Veritas Volume Manager by Symantec – Message Catalogs and Manual Pages

Japanese language packages

The following table show the package name and contents for each Japanese language package.

Table D-3 Japanese language packages

package	Contents
VRTSjacav	Japanese Veritas Cluster Server Agents for Storage Foundation Cluster File System – Manual Pages and Message Catalogs by Symantec
VRTSjacs	Veritas Cluster Server Japanese Message Catalogs by Symantec
VRTSjacse	Japanese Veritas High Availability Enterprise Agents by Symantec
VRTSjadba	Japanese Veritas Oracle Real Application Cluster Support package by Symantec
VRTSjadbe	Japanese Veritas Storage Foundation for Oracle from Symantec – Message Catalogs

Table D-3 Japanese language packages *(continued)*

package	Contents
VRTSjafs	Japanese Veritas File System – Message Catalog and Manual Pages
VRTSjaodm	Veritas Oracle Disk Manager Japanese Message Catalog and Manual Pages by Symantec
VRTSjavm	Japanese Veritas Volume Manager by Symantec – Message Catalogs and Manual Pages
VRTSmulic	Multi-language Symantec License Utilities

Veritas Storage Foundation obsolete and reorganized installation packages

Table D-4 lists the packages that are obsolete or reorganized for Storage Foundation.

Table D-4 Veritas Storage Foundation obsolete and reorganized packages

package	Description
Obsolete and reorganized for 6.0.1	
VRTSat	Obsolete
VRTSatZH	Obsolete
VRTSatJA	Obsolete
Obsolete and reorganized for 5.1	
Infrastructure	
SYMClma	Obsolete
VRTSaa	Included in VRTSsfmh
VRTSccg	Included in VRTSsfmh
VRTSdbms3	Obsolete
VRTSicsco	Obsolete
VRTSjre	Obsolete
VRTSjre15	Obsolete

Table D-4 Veritas Storage Foundation obsolete and reorganized packages *(continued)*

package	Description
VRTSmh	Included in VRTSsfmh
VRTSobc33	Obsolete
VRTSobweb	Obsolete
VRTSobgui	Obsolete
VRTSpbx	Obsolete
VRTSsfm	Obsolete
VRTSweb	Obsolete
Product packages	
VRTSacclib	Obsolete The following information is for installations, upgrades, and uninstallations using the script- or Web-based installer. ■ For fresh installations VRTSacclib is not installed. ■ For upgrades, the existing VRTSacclib is uninstalled and a new VRTSacclib is installed. ■ For uninstallation, VRTSacclib is not uninstalled.
VRTSalloc	Obsolete
VRTScmccc	Obsolete
VRTScmcm	Obsolete
VRTScmcs	Obsolete
VRTScscm	Obsolete
VRTScscw	Obsolete
VRTScsocw	Obsolete
VRTScssim	Obsolete
VRTScutil	Obsolete

Table D-4 Veritas Storage Foundation obsolete and reorganized packages *(continued)*

package	Description
VRTSd2gui	Included in VRTSdbed
VRTSdb2ed	Included in VRTSdbed
VRTSdbcom	Included in VRTSdbed
VRTSdbed	Included in VRTSdbed
VRTSdcli	Obsolete
VRTSddlpr	Obsolete
VRTSdsa	Obsolete
VRTSfas	Obsolete
VRTSfasag	Obsolete
VRTSfsman	Included in the product's main package.
VRTSfsmnd	Included in the product's main package.
VRTSfspro	Included in VRTSsfmh
VRTSgapms	Obsolete
VRTSmapro	Included in VRTSsfmh
VRTSorgui	Obsolete
VRTSsybed	Included in VRTSdbed
VRTSvail	Obsolete
VRTSvcsdb	Included in VRTSvcsea
VRTSvcsmn	Included in VRTSvcs
VRTSvcsor	Included in VRTSvcsea
VRTSvcssy	Included in VRTSvcsea
VRTSvcsvr	Included in VRTSvcs
VRTSvdid	Obsolete
VRTSvmman	Included in the product's main package.

Table D-4 Veritas Storage Foundation obsolete and reorganized packages *(continued)*

package	Description
VRTSvmpro	Included in VRTSsfmh
VRTSvrpro	Included in VRTSob
VRTSvrw	Obsolete
VRTSvxmsa	Obsolete
Documentation	All Documentation packages obsolete

Troubleshooting installation issues

This appendix includes the following topics:

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

What to do if you see a licensing reminder

In this release, you can install without a license key. In order to comply with the End User License Agreement, you must either install a license key or make the host managed by a Management Server. If you do not comply with these terms within 60 days, the following warning messages result:

```
WARNING V-365-1-1 This host is not entitled to run Veritas Storage
Foundation/Veritas Cluster Server.As set forth in the End User
License Agreement (EULA) you must complete one of the two options
set forth below. To comply with this condition of the EULA and
stop logging of this message, you have <nn> days to either:
- make this host managed by a Management Server (see
  http://go.symantec.com/sfhakeyless for details and free download),
  or
- add a valid license key matching the functionality in use on this host
  using the command 'vxlicinst'
```

To comply with the terms of the EULA, and remove these messages, you must do one of the following within 60 days:

- Install a valid license key corresponding to the functionality in use on the host.
  See "Installing Veritas product license keys" on page 32.
  After you install the license key, you must validate the license key using the following command:

  ```
  # /opt/VRTS/bin/vxlicrep
  ```

- Continue with keyless licensing by managing the server or cluster with a management server.
  For more information about keyless licensing, see the following URL:
  http://go.symantec.com/sfhakeyless

About the VRTSspt package troubleshooting tools

The VRTSspt package provides a group of tools for troubleshooting a system and collecting information on its configuration. If you install and use the VRTSspt package, it will be easier for Symantec Support to diagnose any issues you may have.

The tools can gather Veritas File System and Veritas Volume Manager metadata information and establish various benchmarks to measure file system and volume manager performance. Although the tools are not required for the operation of any Veritas product, Symantec recommends installing them should a support case be needed to be opened with Symantec Support. Use caution when you use the VRTSspt package, and always use it in concert with Symantec Support.

Incorrect permissions for root on remote system

The permissions are inappropriate. Make sure you have remote root access permission on each system to which you are installing.

```
Failed to setup rsh communication on 10.198.89.241:
'rsh 10.198.89.241 <command>' failed
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied

Failed to login to remote system(s) 10.198.89.241.
Please make sure the password(s) are correct and superuser(root)
can login to the remote system(s) with the password(s).
If you want to setup rsh on remote system(s), please make sure
rsh with command argument ('rsh <host> <command>') is not
denied by remote system(s).

Either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication

Would you like the installer to setup ssh/rsh communication
automatically between the nodes?
Superuser passwords for the systems will be asked. [y,n,q] (y) n

System verification did not complete successfully

The following errors were discovered on the systems:

The ssh permission denied on 10.198.89.241
rsh exited 1 on 10.198.89.241
either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication
```

Suggested solution: You need to set up the systems to allow remote access using `ssh` or `rsh`.

See “About configuring secure shell or remote shell communication modes before installing products” on page 227.

Note: Remove remote shell permissions after completing the SF installation and configuration.

Inaccessible system

The system you specified is not accessible. This could be for a variety of reasons such as, the system name was entered incorrectly or the system is not available over the network.

```
 Verifying systems: 12% ....................................
 Estimated time remaining: 0:10 1 of 8
 Checking system communication .............................. Done
System verification did not complete successfully
The following errors were discovered on the systems:
cannot resolve hostname host1
Enter the  system names separated by spaces: q,? (host1)
```

Suggested solution: Verify that you entered the system name correctly; use the `ping`(1M) command to verify the accessibility of the host.

Troubleshooting the webinstaller

This section provides possible solutions to problems that may occur when using the `webinstaller` script:

- Issue: The `webinstaller` script may report an error.
  You may receive a similar error message when using the webinstaller:

  ```
  Error: could not get hostname and IP address
  ```

  Solution: Check whether `/etc/hosts` and `/etc/resolv.conf` file are correctly configured.
- Issue: The hostname is not a fully qualified domain name.
  You must have a fully qualified domain name for the hostname in https://<*hostname*>:<*port*>/.
  Solution: Check whether the `domain` section is defined in `/etc/resolv.conf` file.
- Issue: FireFox 3 may report an error.
  You may receive a similar error message when using FireFox 3:

  ```
  Certificate contains the same serial number as another certificate.
  ```

  Solution: Visit FireFox knowledge base website:

http://support.mozilla.com/en-US/kb/Certificate+contains+the+same+serial+number+as+another+certificate

Appendix F

Compatability issues when installing Storage Foundation with other products

This appendix includes the following topics:

- Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present
- Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present
- Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx, VRTSicsco, and VRTSat.

Index