Veritas Storage Foundation™ Installation Guide

Solaris

6.0 Platform Release 1

March 2012

Symantec

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 PR1

Document version: 6.0PR1.0

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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 Web site 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 Web site.

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

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.

Veritas Storage Foundation has the following products:

- Storage Foundation Standard
- Storage Foundation Standard HA
- Storage Foundation Enterprise
- Storage Foundation Enterprise HA

About Veritas Storage Foundation Basic

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

About Veritas Volume Replicator

Veritas Volume Replicator by Symantec is an optional, separately-licensable feature that is fully integrated with Veritas Volume Manager. This component replicates data to remote locations over any standard IP network to provide continuous data availability.

Volume Replicator is available with Veritas Storage Foundation Standard and Enterprise products.

About Veritas graphical user interfaces

The following are descriptions of Veritas GUIs.

About Veritas Operations Manager

Symantec recommends use of Veritas Operations Manager to manage Storage Foundation and Cluster Server environments.

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.

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

Planning to install Storage Foundation

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: 6.0PR1.0.

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

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.
  See "About the Veritas installer" on page 37.
- 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.
- 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 85.

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. On the bottom of the page, click the **Downloads** link.
3. In the Business field, click **Trialware**.
4. On the next page near the bottom of the page, click **Business Continuity**.
5. Under Cluster Server, click **Download Now**.
6. In the new window, click **Download Now**.

7 You can use existing credentials to log in or create new credentials.

8 Review the terms and conditions, and click **I agree**.

9 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 installation scripts" on page 79.

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 23.

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.

Chapter 3

System requirements

This chapter includes the following topics:

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 0x8000. 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, the installer gives a warning. You need to set the values and reboot the system.

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:

```
# 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 8000, 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:

```
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 script-based installer `-precheck` option to determine if there is sufficient space.

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

If you have downloaded SF, use the following command:

```
# ./installsf -precheck
```

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.

Information 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 Sybase.

Chapter 4

Licensing Veritas products

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 or continue with keyless licensing by managing the server or cluster with a management server, such as Veritas Operations Manager (VOM). 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 product installer does not change the license keys that are already installed. 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 26.
  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 28.
  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. In order to use keyless licensing, you must set up a Management Server to manage your systems.

For more information 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 Show your current working directory:

```
# pwd
```

Output resembles:

```
/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 xxxx-xxxx-xxxx-xxxx-xxxx-xxx
```

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 25.
Download the software, or insert the product DVD.	See "Mounting the product disc" on page 34.
Create root user.	See "Creating root user" on page 33.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Set environment variables.	See "Setting environment variables" on page 34.
Create the `/opt` directory, if it does not exist.	See "Creating the /opt directory" on page 32.
Configure the secure shell (ssh) on all nodes.	
Verify that hardware, software, and operating system requirements are met.	See "Release notes" on page 21.
Check that sufficient disk space is available.	See "Disk space requirements" on page 23.
Use the installer to install the products.	See "About the Veritas installer" on page 37.

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 80.

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 add new nodes to an existing cluster.
- When the nodes are in a subcluster during a phased upgrade.
- When you perform installer sessions using a response file.

See "About configuring secure shell or remote shell communication modes before installing products" on page 105.

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.

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 127.

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 tool for assessing your system, to ensure that the system meets the requirements for installing Storage Foundation 6.0 PR1.

Symantec Operations Readiness Tools	Symantec Operations Readiness Tools (SORT) is a Web-based application that is designed to support Symantec enterprise products. See "Symantec Operations Readiness Tools" on page 35.

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

Chapter 6

Installing Storage Foundation using the script-based installer

This chapter includes the following topics:

About the Veritas installer

The installer enables you to install and configure the product, verify preinstallation requirements, and view the product's description.

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 product.

See "About installation scripts" on page 79.

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 80.

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 105.

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 34.

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

Do you agree with the terms of the End User License Agreement
as  specified in the storage_foundation_high_availability/EULA/
lang/EULA_SFHA_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,?] host1
```

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 You need to synchronize the system clocks of your application servers or have them point to an NTP server. After the system check, if the nodes have time difference, the installer prompts:

```
Do you want to synchronize system clock with NTP server(s)?
[y,n,q] (y)
```

12 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.

13 The installer may prompt for previous Veritas Volume Manager configurations.

14 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 25.

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

See "Configuration for Storage Foundation High Availability" for more information.

16 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
```

17 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. Follow the prompts and reboot as necessary.

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
```

Manually installing packages on solaris10 brand zones

You need to manually install SF 6.0 packages inside the solaris10 brand zones.

1. Boot the zone.
2. Log on to the solaris10 brand zone as a super user.
3. Install the following SF packages on the brand zone.
   - `VRTSperl`
   - `VRTSvcs`
   - `VRTSvcsag`
   - `VRTSvcsea`

Note: Perform Steps 1 through 3 on each solaris10 brand zone.

Manually installing packages on solaris brand non-global zones

With Oracle Solaris 11, you need to manually install SF packages inside non-global zones. The native non-global zones are called solaris brand 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.
4. Add a file-based repository in the non-global zone.

   ```
   # pkg set-publisher -P -g /<packagelocationpath>/VRTSpkgs.p5p Symantec
   ```

5. Install the required packages.

   ```
   # pkg install VRTSperl VRTSvlic VRTSvcs VRTSvcsag VRTSvcsea
   ```

6. Remove the publisher on the non-global zone.

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

Note: Perform Steps 2 through 6 on each non-global zone.

Section 3

Configuration of Storage Foundation

Chapter 7

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

- Run the installer command with the configure option.

```
# ./installsf -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*.

Excluding a device that VxVM controls

This section describes how to exclude a device that is under VxVM control. The option to prevent paths from being multi-pathed by the Dynamic Multi-Pathing (DMP) driver, vxdmp, is deprecated.

To suppress devices from being seen by VxVM

1 Enter the command

```
# vxdiskadm
```

2 Select menu item `VolumeManager/Disk/ExcludeDevices` from the `vxdiskadm` main menu.

The following message displays:

```
VxVM INFO V-5-2-5950 This operation might lead to
some devices being suppressed from VxVM's view. (This operation
can be reversed using the vxdiskadm command).

Do you want to continue? [y,n,q,?] (default: n) y
```

3 Enter `y`.

4 Select one of the following operations:

- Suppress all paths through a controller from VxVM's view:
  Select Option 1.
  Enter a controller name when prompted:

  ```
  Enter a controller name:[ctlr_name,all,list,list-exclude,q,?]
  ```

- Suppress a path from VxVM's view:
  Select Option 2.
  Enter a path when prompted.

  ```
  Enter a pathname or pattern:[<Pattern>,all,list,list-exclude,q?]
  ```

- Suppress disks from VxVM's view by specifying a VID:PID combination:
  Select Option 3 and read the messages displayed on the screen.
  Enter a VID:PID combination when prompted.

  ```
  Enter a VID:PID combination:[<Pattern>,all,list,exclude,q,?]
  ```

  The disks that match the VID:PID combination are excluded from VxVM. Obtain the Vendor ID and Product ID from the Standard SCSI inquiry data returned by the disk.

If you selected any of the options, reboot the system for device exclusion to take effect.

Enabling optional cluster support in VxVM

An optional cluster feature enables you to use VxVM in a cluster environment. The cluster functionality in VxVM allows multiple hosts to simultaneously access and manage a set of disks under VxVM control. A cluster is a set of hosts sharing a set of disks; each host is referred to as a node in the cluster.

Converting existing VxVM disk groups to shared disk groups

If you want to convert existing private disk groups to shared disk groups, use the following procedure. Use these steps if you are moving from a single node to a cluster, or if you are already in a cluster and have existing private disk groups.

To convert existing disk groups to shared disk groups

1. Ensure that all systems that are running are part of the same cluster.
2. Start the cluster on all of the nodes on which you are converting the disk groups.

3 Configure the disk groups using the following procedure.

To list all disk groups, use the following command:

```
# vxdg list
```

To deport disk groups to be shared, use the following command:

```
# vxdg deport disk_group_name
```

Make sure that CVM is started. To check the master node:

```
# vxdctl -c mode
```

To import disk groups to be shared, use the following command on the master node:

```
# vxdg -s import disk_group_name
```

This procedure marks the disks in the shared disk groups as shared and stamps them with the ID of the cluster, enabling other nodes to recognize the shared disks.

If dirty region logs exist, ensure they are active. If not, replace them with larger ones.

To display the shared flag for all the shared disk groups, use the following command:

```
# vxdg list disk_group_name
```

The disk groups are now ready to be shared.

4 If the cluster is only running with one node, bring up the other cluster nodes. Enter the `vxdg list` command on each node to display the shared disk groups. This command displays the same list of shared disk groups displayed earlier.

Configuring shared disks

This section describes how to configure shared disks. If you are installing VxVM for the first time or adding disks to an existing cluster, you need to configure new shared disks. If you are upgrading VxVM, verify that your shared disks still exist.

The shared disks should be configured from one node only. Since the VxVM software cannot tell whether a disk is shared or not, you must specify which are the shared disks.

Make sure that the shared disks are not being accessed from another node while you are performing the configuration. If you start the cluster on the node where

you perform the configuration only, you can prevent disk accesses from other nodes because the quorum control reserves the disks for the single node.

Also, hot-relocation can be configured.

Verifying existing shared disks

If you are upgrading from a previous release of VxVM, verify that your shared disk groups still exist.

To verify that your shared disk groups exist

1. Start the cluster on all nodes.
2. Enter the following command on all nodes:

   ```
   # vxdg -s list
   ```

   This displays the existing shared disk groups.

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 SFDB repository database after installation

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

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

Section 4

Verification of the installation

Chapter 8

Verifying the installation

This chapter includes the following topics:

Verifying that the products were installed

Verify that the SF products are installed.

Use the pkg info command to check which packages have been installed.

```
# pkg info -l VRTSvlic package_name package_name ...
```

You can verify the version of the installed product. Use the following command:

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

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
  ```

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
  ```

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.

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 52.

Verifying command installation

Table 8-1 lists the directories with Veritas File System commands.

Table 8-1 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 34.

Section 5

Uninstallation of Storage Foundation

Chapter 9

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 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 disk3-0111       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 PR1 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 64.
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
   ```

   For Veritas Storage Foundation

   ```
   # ./uninstallsf
   ```

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, `host1`:

   ```
   Enter the system names separated by spaces: [q?] host1 host2
   ```

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
```

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

 {
    "sfae_rept_version" : 1,
    "oracle" : {
       "SFAEDB" : {
          "location" : "/data/sfaedb/.sfae",
          "old_location" : "",
          "alias" : [
             "sfaedb"
          ]
       }
    }
 }
```

2 Remove the directory identified by the `location` key.

```
# rm -rf /data/sfaedb/.sfae
```

3 Remove the repository location file.

```
# rm -rf /var/vx/vxdba/rep_loc
```

This completes the removal of the SFDB repository.

Manually uninstalling Storage Foundation packages on non-global zones

1. Log on to the non-global zone as a super user.
2. Uninstall SF packages from Solaris brand zones.

```
# pkg uninstall VRTSperl VRTSvlic VRTSvcs VRTSvcsag VRTSvcsea
```

3. Uninstall SF packages from solaris10 brand zones.

```
# pkgrm VRTSperl VRTSvlic VRTSvcs VRTSvcsag VRTSvcsea
```

Section 6

Installation reference

Appendix A

Installation scripts

This appendix includes the following topics:

About installation scripts

Veritas Storage Foundation and High Availability Solutions products 6.0 PR1 provides several installation scripts. You can find these scripts at the root of the product media in the scripts directory.

An alternative to the `installer` script is to use a product-specific installation script. If you obtained a Veritas product from the Symantec download site, which does not include the installer, use the appropriate product installation script.

The following product installation scripts are available:

Veritas Cluster Server (VCS)	`installvcs`
Veritas Storage Foundation (SF)	`installsf`
Veritas Storage Foundation and High Availability (SFHA)	`installsfha`
Veritas Storage Foundation Cluster File System High Availability (SFCFSHA)	`installsfcfsha`
Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`
Veritas Storage Foundation for Sybase ASE CE (SF Sybase CE)	`installsfsybasece`
Veritas Volume Manager	`installvm`

Veritas File System	`installfs`
Veritas Dynamic Multi-pathing	`installdmp`
Symantec VirtualStore	`installsvs`

To use the installation script, enter the script name at the prompt. For example, to install Veritas Storage Foundation, type `./installsf` at the prompt.

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 installation scripts" on page 79.

Table A-1 Available command line options

Command Line Option	Function
system1 system2...	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
–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.
–install	The `-install` option is used to install products on systems.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–installallpkgs	Specifies that all packages are installed.
–installminpkgs	Specifies that the minimum package set is installed.
–installrecpkgs	Specifies that the required package set is installed.
–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.
–pkg info	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 -pkg info option with the installvcs script to display VCS packages.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–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, file system space, and other system requirements in order to install the product.
–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.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–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.
–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.
–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.
–uninstall	The `-uninstall` option is used to uninstall products from systems.
-tunablesfile	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.

Table A-1 Available command line options *(continued)*

Command Line Option	Function
–version	Checks and reports the installed products and their versions. Identifies the installed and missing packages where applicable for the product. Provides a summary that includes the count of the installed and any missing packages where applicable. Lists the installed hotfixes and available updates for the installed product if an Internet connection is available.

Appendix B

Response files

This appendix includes the following topics:

About response files

The installer or product installation script generates a response file during any installation, configuration, 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.

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.

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 90.

4 Start the configuration from the system to which you copied the response file. For example:

```
# /opt/VRTS/install/installsf -responsefile /tmp/response_file
```

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

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 -responsefile /tmp/response_file
```

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

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"];
```

Response file variables to install, upgrade, or uninstall Storage Foundation

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

Table B-1 Response file variables specific to installing, upgrading, or uninstalling 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{accepteula}	Specifies whether you agree with the EULA.pdf file on the media. List or scalar: scalar Optional or required: required
$CFG{opt}{vxkeyless}	Installs the product with keyless license. 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

Table B-1 Response file variables specific to installing, upgrading, or uninstalling SF *(continued)*

Variable	Description
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
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{donotinstall} {package}	Instructs the installation to not install the optional packages in the list. List or scalar: list Optional or required: optional
CFG{donotremove} {package}	Instructs the uninstallation to not remove the optional packages in the list. List or scalar: list 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

Table B-1 Response file variables specific to installing, upgrading, or uninstalling SF *(continued)*

Variable	Description
CFG{opt}{upgrade}	Upgrades all packages installed, without configuration. List or scalar: list Optional or required: optional
CFG{opt}{uninstall}	Uninstalls SF packages. List or scalar: scalar Optional or required: optional
CFG{mirrordgname}{system}	Splits the target disk group name for a system. List or scalar: scalar Optional or required: optional
CFG{splitmirror}{system}	Indicates the system where you want a split mirror backup disk group created. List or scalar: scalar Optional or required: optional

Response file variables to configure Storage Foundation

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

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

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)

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

Variable	List or Scalar	Description
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)
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).

Appendix C

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 94.

- 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 95.

- 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 96.

See "About response files" on page 85.

You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 98.

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 98.

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 97.

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 98.

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 97.

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 98.

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 97.

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 -responsefile response_file_name -tunablesfile
tunables_file_name -settunables
```

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 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.

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.

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 98.

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 C-1 describes the supported tunable parameters that can be specified in a tunables file.

Table C-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.
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.

Table C-1 Supported tunable parameters *(continued)*

Tunable	Description
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.
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.

Table C-1 Supported tunable parameters *(continued)*

Tunable	Description
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.
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.

Table C-1 Supported tunable parameters *(continued)*

Tunable	Description
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.
vol_checkpt_default	(Veritas File System) Size of VxVM 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.

Table C-1 Supported tunable parameters *(continued)*

Tunable	Description
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.
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.

Table C-1 Supported tunable parameters *(continued)*

Tunable	Description
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.
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.

Table C-1 Supported tunable parameters *(continued)*

Tunable	Description
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_mbuf	(Veritas File System) Maximum memory used for VxFS buffer cache. 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.
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 D

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.

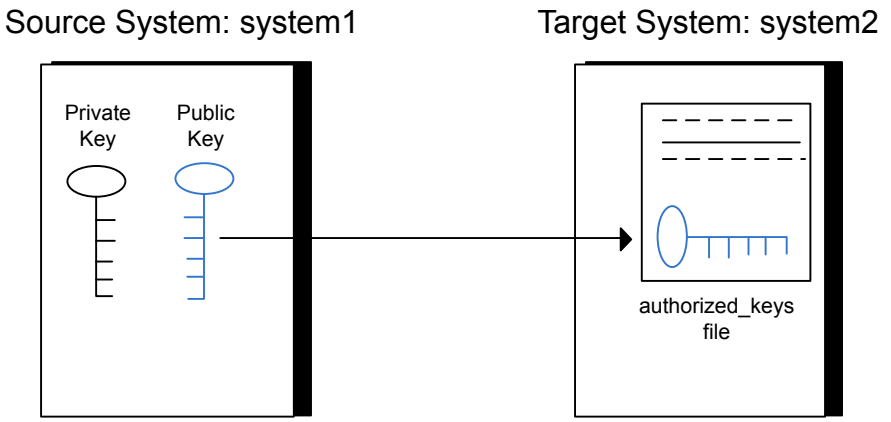
Manually configuring and passwordless ssh

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 D-1 illustrates this procedure.

Figure D-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. 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):
   ```

3. Press Enter to accept the default location of `/.ssh/id_dsa`.
4. 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.
5. 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:

   ```
   system2 # mkdir /.ssh
   ```

   Change the permissions of this directory, to secure it.

   ```
   system2 # chmod go-w /.ssh
   ```

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, 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 106.

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 E

Storage Foundation components

This appendix includes the following topics:

Storage Foundation installation packages

Table E-1shows 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 E-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
VRTSperl	Perl 5.12.2 for Veritas	Minimum

Table E-1 Storage Foundation packages *(continued)*

packages	Contents	Configuration
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
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
VRTSsfcpi60	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

Table E-1 Storage Foundation packages *(continued)*

packages	Contents	Configuration
VRTSsfmh	Veritas Storage Foundation Managed Host Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at:	Recommended
VRTSspt	Veritas Software Support Tools	Recommended
VRTSfsadv	Minimum Veritas File System Advanced Solutions by Symantec (Solaris SPARC only).	Minimum
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 E-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 E-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
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 E-4 lists the packages that are obsolete or reorganized for Storage Foundation.

Table E-4 Veritas Storage Foundation obsolete and reorganized packages

package	Description
Obsolete and reorganized for 6.0	
VRTSat	Obsolete
VRTSatZH	Obsolete
VRTSatJA	Obsolete
Obsolete and reorganized for 5.1	
Infrastructure	

Table E-4 Veritas Storage Foundation obsolete and reorganized packages *(continued)*

package	Description
SYMClma	Obsolete
VRTSaa	Included in VRTSsfmh
VRTSccg	Included in VRTSsfmh
VRTSdbms3	Obsolete
VRTSicsco	Obsolete
VRTSjre	Obsolete
VRTSjre15	Obsolete
VRTSmh	Included in VRTSsfmh
VRTSpbx	Obsolete
VRTSsfm	Obsolete
VRTSweb	Obsolete
Product packages	
VRTSacclib	Obsolete The following information is for installations, upgrades, and uninstallations using the script-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

Table E-4 Veritas Storage Foundation obsolete and reorganized packages *(continued)*

package	Description
VRTScscw	Obsolete
VRTScsocw	Obsolete
VRTScssim	Obsolete
VRTScutil	Obsolete
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

Table E-4 Veritas Storage Foundation obsolete and reorganized packages *(continued)*

package	Description
VRTSvcssy	Included in VRTSvcsea
VRTSvcsvr	Included in VRTSvcs
VRTSvdid	Obsolete
VRTSvmman	Included in the product's main package.
VRTSvmpro	Included in VRTSsfmh
VRTSvrw	Obsolete
VRTSvxmsa	Obsolete
Documentation	All Documentation packages obsolete

Appendix F

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 28.
  After you install the license key, you must validate the license key using the following command:

  ```
  # /opt/VRTS/bin/vxkeyless
  ```

- 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

Troubleshooting information

The VRTSspt package provides a group of tools for troubleshooting a system and collecting information on its configuration. 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. If you are unfamiliar with their use and purpose, use caution when using them or use them 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`.

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.

Appendix G

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 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.

Appendix H

Changing root user into role

This appendix includes the following topics:

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.

Index