

# Veritas Storage Foundation™ Installation Guide

Linux

6.0.1

# Veritas Storage Foundation™ Installation Guide

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

Product version: 6.0.1

Document version: 6.0.1 Rev 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](http://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](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>

## 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](mailto:doc_feedback@symantec.com)

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

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

## About Symantec Connect

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

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

# Contents

Technical Support .....	4
Section 1    Installation overview and planning .....	13
Chapter 1    Introducing Storage Foundation .....	15
About Veritas products .....	15
About Storage Foundation .....	15
About Veritas Replicator Option .....	16
About Veritas graphical user interfaces .....	16
About Veritas Operations Manager .....	16
Chapter 2    System requirements .....	19
Release notes .....	19
Hardware compatibility list (HCL) .....	20
Supported operating systems .....	20
Storage Foundation memory requirements .....	20
Disk space requirements .....	20
Discovering product versions and various requirement information .....	21
Database requirements .....	21
VxVM licenses .....	21
Cross-Platform Data Sharing licensing .....	22
Chapter 3    Planning to install SF .....	23
About planning for SF installation .....	23
About installation and configuration methods for SF .....	24
About response files .....	24
About the Veritas installer .....	25
Downloading the Storage Foundation software .....	27
Chapter 4    Licensing SF .....	29
About Veritas product licensing .....	29
Setting or changing the product level for keyless licensing .....	30

	Installing Veritas product license keys .....	32
<b>Section 2</b>	<b>Installation of Storage Foundation .....</b>	<b>33</b>
<b>Chapter 5</b>	<b>Preparing to install Storage Foundation .....</b>	<b>35</b>
	Installation preparation overview .....	35
	About using ssh or rsh with the Veritas installer .....	36
	Setting environment variables .....	36
	Mounting the product disc .....	37
	Assessing the system for installation readiness .....	38
	About Symantec Operations Readiness Tools .....	38
	Prechecking your systems using the Veritas installer .....	39
<b>Chapter 6</b>	<b>Installing Storage Foundation using the script-based installer .....</b>	<b>41</b>
	Installing Storage Foundation using the installer .....	41
<b>Chapter 7</b>	<b>Installing Storage Foundation using the web-based installer .....</b>	<b>45</b>
	About the Web-based installer .....	45
	Before using the Veritas Web-based installer .....	46
	Starting the Veritas Web-based installer .....	46
	Obtaining a security exception on Mozilla Firefox .....	47
	Performing a pre-installation check with the Veritas Web-based installer .....	48
	Installing SF with the Web-based installer .....	48
<b>Chapter 8</b>	<b>Performing an automated installation using response files .....</b>	<b>51</b>
	Installing SF using response files .....	51
	Response file variables to install Storage Foundation .....	52
	Sample response file for SF installation .....	54
	Configuring SF using response files .....	55
	Response file variables to configure Storage Foundation .....	55
<b>Chapter 9</b>	<b>Installing Storage Foundation using operating system-specific methods .....</b>	<b>59</b>
	Installing SF using Kickstart .....	59
	Sample Kickstart configuration file .....	61



	Installing Storage Foundation using yum .....	62
Chapter 10	Configuring Storage Foundation .....	69
	Configuring Storage Foundation using the installer .....	69
	Configuring Storage Foundation manually .....	69
	Configuring Veritas Volume Manager .....	70
	Configuring Veritas File System .....	70
	Configuring the SFDB repository database after installation .....	71
Section 3	Upgrade of SF .....	73
Chapter 11	Planning to upgrade SF .....	75
	Upgrade methods for SF .....	75
	Supported upgrade paths for SF 6.0.1 .....	76
	About using the installer to upgrade when the root disk is encapsulated .....	81
	Preparing to upgrade SF .....	81
	Getting ready for the upgrade .....	81
	Creating backups .....	82
	Tasks for upgrading the Storage Foundation for Databases (SFDB) .....	83
	Determining if the root disk is encapsulated .....	84
	Pre-upgrade tasks for migrating the SFDB repository database .....	84
	Pre-upgrade planning for Veritas Volume Replicator .....	84
	Upgrading the array support .....	87
Chapter 12	Upgrading Storage Foundation .....	89
	Upgrading Storage Foundation from previous versions to 6.0.1 .....	89
	Upgrading Storage Foundation using the script-based installer .....	89
	Upgrading Storage Foundation using the Veritas Web-based installer .....	93
	Upgrading Veritas Volume Replicator .....	94
	Upgrading VVR without disrupting replication .....	94
Chapter 13	Performing an automated SF upgrade using response files .....	97
	Upgrading SF using response files .....	97
	Response file variables to upgrade Storage Foundation .....	98

	Sample response file for SF upgrade .....	99
Chapter 14	Performing post-upgrade tasks .....	101
	Optional configuration steps .....	101
	Re-joining the backup boot disk group into the current disk group .....	102
	Reverting to the backup boot disk group after an unsuccessful upgrade .....	102
	Post upgrade tasks for migrating the SFDB repository database .....	103
	Migrating from a 5.0 repository database to 6.0.1 .....	103
	Migrating from a 5.1 or higher repository database to 6.0.1 .....	106
	After upgrading from 5.0.x and before migrating SFDB .....	108
	Recovering VVR if automatic upgrade fails .....	108
	Upgrading disk layout versions .....	109
	Upgrading VxVM disk group versions .....	109
	Updating variables .....	110
	Setting the default disk group .....	110
	Verifying the Storage Foundation upgrade .....	110
Section 4	Post-installation tasks .....	111
Chapter 15	Verifying the SF installation .....	113
	Verifying that the products were installed .....	113
	Installation log files .....	113
	Using the installation log file .....	114
	Using the summary file .....	114
	Starting and stopping processes for the Veritas products .....	114
	Checking Veritas Volume Manager processes .....	115
Section 5	Uninstallation of SF .....	117
Chapter 16	Uninstalling Storage Foundation .....	119
	Removing VxFS file systems .....	119
	Removing rootability .....	120
	Moving volumes to disk partitions .....	121
	Moving volumes onto disk partitions using VxVM .....	122
	Removing the Replicated Data Set .....	123
	Uninstalling SF RPMs using the script-based installer .....	125
	Uninstalling SF with the Veritas Web-based installer .....	126
	Removing license files (Optional) .....	127

	Removing the Storage Foundation for Databases (SFDB) repository after removing the product .....	127
Chapter 17	Uninstalling SF using response files .....	129
	Uninstalling SF using response files .....	129
	Response file variables to uninstall Storage Foundation .....	130
	Sample response file for SF uninstallation .....	131
Section 6	Installation reference .....	133
Appendix A	Installation scripts .....	135
	Installation script options .....	135
Appendix B	Tunable files for installation .....	141
	About setting tunable parameters using the installer or a response file .....	141
	Setting tunables for an installation, configuration, or upgrade .....	142
	Setting tunables with no other installer-related operations .....	143
	Setting tunables with an un-integrated response file .....	144
	Preparing the tunables file .....	145
	Setting parameters for the tunables file .....	145
	Tunables value parameter definitions .....	146
Appendix C	Configuring the secure shell or the remote shell for communications .....	153
	About configuring secure shell or remote shell communication modes before installing products .....	153
	Manually configuring and passwordless ssh .....	154
	Restarting the ssh session .....	158
	Enabling rsh for Linux .....	158
Appendix D	Storage Foundation components .....	161
	Storage Foundation installation RPMs .....	161
	Veritas Storage Foundation obsolete and reorganized installation RPMs .....	164
Appendix E	Troubleshooting installation issues .....	169
	Restarting the installer after a failed connection .....	169
	What to do if you see a licensing reminder .....	169

	About the VRTSspt RPM troubleshooting tools .....	170
	Incorrect permissions for root on remote system .....	170
	Inaccessible system .....	172
	Troubleshooting the webinstaller .....	172
Appendix F	Compatibility issues when installing Storage Foundation with other products .....	173
	Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present .....	173
	Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present .....	174
	Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present .....	174
Index .....		175

# Installation overview and planning

- [Chapter 1. Introducing Storage Foundation](#)
- [Chapter 2. System requirements](#)
- [Chapter 3. Planning to install SF](#)
- [Chapter 4. Licensing SF](#)



# Introducing Storage Foundation

This chapter includes the following topics:

- [About Veritas products](#)
- [About Veritas graphical user interfaces](#)

## About Veritas products

The following products are available for this release.

### About Storage Foundation

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

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

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

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

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

## About Veritas Storage Foundation Basic

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

## About Veritas Replicator Option

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

Veritas File Replicator enables replication at the file level over IP networks. File Replicator leverages data duplication, provided by Veritas File System, to reduce the impact of replication on network resources.

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

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

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

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

## About Veritas graphical user interfaces

The following are descriptions of Veritas GUIs.

### About Veritas Operations Manager

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

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

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

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

The Veritas Enterprise Administrator (VEA) console is no longer packaged with Storage Foundation products. If you want to continue using VEA, a software



version is available for download from [http://go.symantec.com/vcsm\\_download](http://go.symantec.com/vcsm_download).  
Veritas Storage Foundation Management Server is deprecated.



# System requirements

This chapter includes the following topics:

- [Release notes](#)
- [Hardware compatibility list \(HCL\)](#)
- [Supported operating systems](#)
- [Storage Foundation memory requirements](#)
- [Disk space requirements](#)
- [Discovering product versions and various requirement information](#)
- [Database requirements](#)
- [VxVM licenses](#)
- [Cross-Platform Data Sharing licensing](#)

## 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*.

## Storage Foundation memory requirements

A minimum of 1 GB of memory is strongly recommended.

## Disk space requirements

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

Use the "Perform a Pre-installation Check" (P) menu for the Web-based installer or the `-precheck` option of the script-based installer to determine whether there is sufficient space.

Go to the installation directory and run the installer with the `-precheck` option.

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

If you have downloaded SF, you must use the following command:

```
# ./installsf -precheck<version>
```

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

See ["About the Veritas installer"](#) on page 25.

# Discovering product versions and various requirement information

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

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

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 RPMs or patches (if applicable) that are missing
- The available updates (including patches or hotfixes) from Symantec Operations Readiness Tools (SORT) for the installed products

## To run the version checker

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

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

## Database requirements

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

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

---

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

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

---

## VxVM licenses

The following table shows the levels of licensing in Veritas Volume Manager and the features supported at each level.

**Table 2-1** describes the levels of licensing in Veritas Volume Manager and supported features.

**Table 2-1** Levels of licensing in Veritas Volume Manager and supported features

VxVM License	Description of Supported Features
Full	Concatenation, spanning, rootability, volume resizing, multiple disk groups, co-existence with native volume manager, striping, mirroring, DRL logging for mirrors, striping plus mirroring, mirroring plus striping, RAID-5, RAID-5 logging, Smartsync, hot sparing, hot-relocation, online data migration, online relayout, volume snapshots, volume sets, Intelligent Storage Provisioning, FastResync with Instant Snapshots, Storage Expert, Device Discovery Layer (DDL), Dynamic Multipathing (DMP), and Veritas Operations Manager (VOM).
Add-on Licenses	Features that augment the Full VxVM license such as clustering functionality (cluster-shareable disk groups and shared volumes) and Veritas Volume Replicator.

---

**Note:** You need a Full VxVM license to make effective use of add-on licenses to VxVM.

---

To see the license features that are enabled in VxVM

- ◆ Enter the following command:

```
# vxctl license
```

## Cross-Platform Data Sharing licensing

The Cross-Platform Data Sharing (CDS) feature is also referred to as Portable Data Containers.

The ability to import a CDS disk group on a platform that is different from the platform on which the disk group was last imported is controlled by a CDS license. CDS licenses are included as part of the Veritas Storage Foundation license.

# Planning to install SF

This chapter includes the following topics:

- [About planning for SF installation](#)
- [About installation and configuration methods for SF](#)
- [About the Veritas installer](#)
- [Downloading the Storage Foundation software](#)

## About planning for SF installation

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

<https://sort.symantec.com/documents>

Document version: 6.0.1 Rev 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 for SF

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

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

- The Veritas product installer  
The installer displays a menu that simplifies the selection of installation options.
- The product-specific installation scripts  
The installation scripts provide a command-line interface to install a specific product. The product-specific scripts enable you to specify some additional command-line options. Installing with the installation script is also the same as specifying SF from the installer menu.
- The Web-based Veritas installer  
The installer provides an interface to manage the installation from a remote site using a standard Web browser.  
See [“About the Web-based installer”](#) on page 45.
- Silent installation with response files  
You can use any of the above options to generate a response file. You can then customize the response file for another system. Run the product installation script with the response file to install silently on one or more systems.  
See [“About response files”](#) on page 24.
- KickStart  
You can use the Veritas product installer or the product-specific installation script to generate a Kickstart script file. Use the generated script to install Veritas RPMs from your Kickstart server.

## About response files

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

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

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



See [“Installation script options”](#) on page 135.

## Syntax in the response file

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

For example, in the case of a string value:

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

or, in the case of an integer value:

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

or, in the case of a list:

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

# About the Veritas installer

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

- The general product installer. The general product installer enables you to install and configure the product, verify preinstallation requirements, and view the product’s description. You perform the installation from a disc, and you are prompted to choose a product to install.  
See [“Installing Storage Foundation using the installer”](#) on page 41.
- Product-specific installation scripts. If you obtained a standalone Veritas product from an electronic download site, the single product download files do not contain the general product installer. Use the product installation script to install the individual products. You can find these scripts at the root of the product media in the scripts directory. These scripts are also installed with the product.

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

---

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

---

**Table 3-1** Product installation scripts

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

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

For example, for the 6.0.1 version:

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

---

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

---

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

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

See “[Installation script options](#)” on page 135.

## Downloading the Storage Foundation software

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

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

### To download the trialware version of the software

- 1 Open the following link in your browser:  
<http://www.symantec.com/index.jsp>
- 2 In Products and Solutions section, click the **Trialware & Downloads** link.
- 3 On the next page near the bottom of the page, click **Business Continuity**.
- 4 Under Cluster Server, click **Download Now**.
- 5 In the new window, click **Download Now**.
- 6 Review the terms and conditions, and click **I agree**.
- 7 You can use existing credentials to log in or create new credentials.
- 8 Find the product that you want to download and select it. Continue with the installation.

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

---

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

---

See [“About the Veritas installer”](#) on page 25.

#### To download the software

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

The estimated space for download, gunzip, and tar extract is 1 GB.

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 20.

- 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.

```
# df -k filesystem
```

---

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

---

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

# Licensing SF

This chapter includes the following topics:

- [About Veritas product licensing](#)
- [Setting or changing the product level for keyless licensing](#)
- [Installing Veritas product license keys](#)

## 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/](http://www.symantec.com/techsupp/)

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

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

Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled. If you do not comply with the above terms, continuing to use the Symantec product is a violation of your end user license agreement, and results in warning messages.

For more information about keyless licensing, see the following URL:

<http://go.symantec.com/sfhakeyless>

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

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

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

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

---

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

---

## Setting or changing the product level for keyless licensing

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

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

<http://go.symantec.com/vom>

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

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

### To set or change the product level

- 1 Change your current working directory:

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

- 2 View the current setting for the product level.

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

- 3 View the possible settings for the product level.

```
# ./vxkeyless displayall
```

- 4 Set the desired product level.

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

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

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

---

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

---

### To clear the product license level

- 1 View the current setting for the product license level.

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

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

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

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

## Installing Veritas product license keys

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

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

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

### To install a new license

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

```
# cd /opt/VRTS/bin  
  
# ./vxlicinst -k license key
```

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

```
# ./vxkeyless display
```

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



# Installation of Storage Foundation

- [Chapter 5. Preparing to install Storage Foundation](#)
- [Chapter 6. Installing Storage Foundation using the script-based installer](#)
- [Chapter 7. Installing Storage Foundation using the web-based installer](#)
- [Chapter 8. Performing an automated installation using response files](#)
- [Chapter 9. Installing Storage Foundation using operating system-specific methods](#)
- [Chapter 10. Configuring Storage Foundation](#)



# Preparing to install Storage Foundation

This chapter includes the following topics:

- [Installation preparation overview](#)
- [About using ssh or rsh with the Veritas installer](#)
- [Setting environment variables](#)
- [Mounting the product disc](#)
- [Assessing the system for installation readiness](#)

## 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 <a href="#">“About Veritas product licensing”</a> on page 29.
Download the software, or insert the product DVD.	See <a href="#">“Downloading the Storage Foundation software”</a> on page 27. See <a href="#">“Mounting the product disc”</a> on page 37.
Set environment variables.	See <a href="#">“Setting environment variables”</a> on page 36.

**Table 5-1** Installation overview (*continued*)

Installation task	Section
Configure the secure shell (ssh) or remote shell (rsh) on all nodes.	See <a href="#">“About configuring secure shell or remote shell communication modes before installing products”</a> on page 153.
Verify that hardware, software, and operating system requirements are met.	See <a href="#">“Release notes”</a> on page 19.
Check that sufficient disk space is available.	See <a href="#">“Disk space requirements”</a> on page 20.
Use the installer to install the products.	See <a href="#">“About the Veritas installer”</a> on page 25.

## About using ssh or rsh with the Veritas installer

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

See [“Installation script options”](#) on page 135.

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

- When you perform installer sessions using a response file.

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 153.

## 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`.

Specify `/opt/VRTS/bin` in your `PATH` after the path to the standard Linux commands.

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.

To invoke the VxFS-specific `df`, `fsdb`, `ncheck`, or `umount` commands, type the full path name: `/opt/VRTS/bin/command`.

To set your `MANPATH` environment variable to include `/opt/VRTS/man` do the following:

- If you are using a shell such as `sh` or `bash`, enter the following:

```
$ MANPATH=$MANPATH:/opt/VRTS/man; export MANPATH
```

- If you are using a shell such as `csh` or `tcsh`, enter the following:

```
% setenv MANPATH $(MANPATH) :/opt/VRTS/man
```

On a Red Hat system, also include the `1m` manual page section in the list defined by your `MANSECT` environment variable.

- If you are using a shell such as `sh` or `bash`, enter the following:

```
$ MANSECT=$MANSECT:1m; export MANSECT
```

- If you are using a shell such as `csh` or `tcsh`, enter the following:

```
% setenv MANSECT $(MANSECT) :1m
```

If you use the `man(1)` command to access manual pages, set `LC_ALL=C` in your shell to ensure that they display correctly.

## 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 with the SF software into a drive that is connected to the system.  
The disc is automatically mounted.

- 3 If the disc does not automatically mount, then enter:

```
# mkdir /mnt/cdrom  
  
# mount -o ro /dev/cdrom /mnt/cdrom
```

- 4 Navigate to the location of the RPMs.

```
# cd /mnt/cdrom/dist_arch/rpms
```

Where *dist* is rhel5, rhel6, sles10, or sles11, and *arch* is x86\_64 for RHEL and SLES.

## Assessing the system for installation readiness

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

### Symantec Operations Readiness Tools

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

See [“About Symantec Operations Readiness Tools”](#) on page 38.

### Prechecking your systems using the installer

Performs a pre-installation check on the specified systems. The Veritas product installer reports whether the specified systems meet the minimum requirements for installing Veritas Storage Foundation 6.0.1.

See [“Prechecking your systems using the Veritas installer”](#) on page 39.

## About Symantec Operations Readiness Tools

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

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

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

To access SORT, go to:

<https://sort.symantec.com>

## Prechecking your systems using the Veritas installer

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

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

### To use the precheck option

- 1 Start the script-based or Web-based installer.  
 See “[Installing Storage Foundation using the installer](#)” on page 41.  
 See “[Installing SF with the Web-based installer](#)” on page 48.
- 2 Select the precheck option:
  - From the Web-based installer, select the **Perform a Pre-Installation Check** from the Task pull-down menu.
  - In the script-based installer, from root on the system where you want to perform the check, start the installer.

```
# ./installer
```

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

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





# Installing Storage Foundation using the script-based installer

This chapter includes the following topics:

- [Installing Storage Foundation using the installer](#)

## 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 153.

- 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 37.

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

```
# cd /mnt/cdrom/dist_arch
```

Where *dist* is rhel5, rhel6, sles10, or sles11, and *arch* is x86\_64 for RHEL and SLES.

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

```
# ./installer
```

- 5 Enter `I` to install and press Return.

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

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

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

- 8 Select from one of the following installation options:

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

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

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

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

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

- 11 The installer can configure remote shell or secure shell communications for you among systems, however each system needs to have RSH or SSH servers installed. You also need to provide the superuser passwords for the systems. Note that for security reasons, the installation program neither stores nor caches these passwords.
- 12 The installer may prompt to restore previous Veritas Volume Manager configurations.
- 13 Choose the licensing method. Answer the licensing questions and follow the prompts.

---

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

---

See [“About Veritas product licensing”](#) on page 29.

- 14 The installer prompts you to configure SFHA. You can continue with configuration if you answer **y**.
- 15 You are prompted to enter the Standard or Enterprise product mode.

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

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

- 16 At the prompt, specify whether you want to send your installation information to Symantec.

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

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



# Installing Storage Foundation using the web-based installer

This chapter includes the following topics:

- [About the Web-based installer](#)
- [Before using the Veritas Web-based installer](#)
- [Starting the Veritas Web-based installer](#)
- [Obtaining a security exception on Mozilla Firefox](#)
- [Performing a pre-installation check with the Veritas Web-based installer](#)
- [Installing SF with the Web-based installer](#)

## About the Web-based installer

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

You use the `webinstaller` script to start and stop the Veritas XPortal Server `xprt1wid` process. The `webinstaller` script can also be used to check the status of the XPortal Server.

When the `webinstaller` script starts the `xprt1wid` process, the script displays a URL. Use this URL to access the Web-based installer from a Web browser such as Internet Explorer or FireFox.

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

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

See [“Before using the Veritas Web-based installer”](#) on page 46.

See [“Starting the Veritas Web-based installer”](#) on page 46.

## Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

**Table 7-1** Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Veritas products.	Must be a supported platform for Veritas Storage Foundation 6.0.1.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: <ul style="list-style-type: none"><li>■ Internet Explorer 6, 7, and 8</li><li>■ Firefox 3.x and later</li></ul>

## Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

### To start the Web-based installer

- 1 Mount the installation media.
- 2 Change directory to the top level on the media, for example:

```
# cd /mnt/cdrom/dist_arch
```

- 3 Start the Veritas XPortal Server process `xprt1wid`, on the installation server:

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

---

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

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

---

- 4 On the administrative server, start the Web browser.
- 5 Navigate to the URL that the script displayed.
- 6 Certain browsers may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

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

- 7 Log in as superuser.

## Obtaining a security exception on Mozilla Firefox

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

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

### To obtain a security exception

- 1 Click **Or you can add an exception** link.
- 2 Click **I Understand the Risks**, or **You can add an exception**.
- 3 Click **Get Certificate** button.
- 4 Uncheck **Permanently Store this exception checkbox (recommended)**.

- 5 Click **Confirm Security Exception** button.
- 6 Enter root in User Name field and root password of the web server in the Password field.

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

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

### To perform a pre-installation check

- 1 Start the Web-based installer.  
See [“Starting the Veritas Web-based installer”](#) on page 46.
- 2 On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list. Select **Veritas Storage Foundation and High Availability** from the **Product** drop-down list and click **Next**.
- 3 Select the Storage Foundation from the **Product** drop-down list, and click **Next**.
- 4 Indicate the systems on which to perform the precheck. Enter one or more system names, separated by spaces. Click **Next**.
- 5 The installer performs the precheck and displays the results.
- 6 If the validation completes successfully, click **Next**. The installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.
- 7 Click **Finish**. The installer prompts you for another task.

## Installing SF with the Web-based installer

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

### To install SF using the Web-based installer

- 1 Perform preliminary steps.  
See [“Performing a pre-installation check with the Veritas Web-based installer”](#) on page 48.
- 2 Start the Web-based installer.  
See [“Starting the Veritas Web-based installer”](#) on page 46.
- 3 Select **Install a Product** from the **Task** drop-down list.



- 4 Select **Storage Foundation** from the Product drop-down list, and click **Next**.
- 5 On the License agreement page, read the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
- 6 Choose minimal, recommended, or all RPMs. Click **Next**.
- 7 Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Next**.
- 8 If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or rsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.
- 9 After the validation completes successfully, click **Next** to install SF on the selected system.
- 10 After the installation completes, you must choose your licensing method. On the license page, select one of the following tabs:
  - Keyless licensing

---

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

For more information, go to the following website:

<http://go.symantec.com/sfhakeyless>

---

Complete the following information:

- Choose whether you want to install Standard or Enterprise mode.
  - Choose whether you want to enable Veritas Replicator.
  - Choose whether you want to enable Veritas File Replicator.
- Click **Register**.
- Enter license key  
If you have a valid license key, select this tab. Enter the license key for each system. Click **Register**.

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

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

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

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

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

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

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

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

- 13 If prompted, select the checkbox to specify whether you want to send your installation information to Symantec.

```
Would you like to send the information about this installation  
to Symantec to help improve installation in the future?
```

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

# Performing an automated installation using response files

This chapter includes the following topics:

- [Installing SF using response files](#)
- [Response file variables to install Storage Foundation](#)
- [Sample response file for SF installation](#)
- [Configuring SF using response files](#)
- [Response file variables to configure Storage Foundation](#)

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

Where <version> is the specific release version and /tmp/response\_file is the response file’s full path name.

See “[About the Veritas installer](#)” on page 25.

## Response file variables to install Storage Foundation

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

**Table 8-1** Response file variables for installing SF

Variable	Description
CFG{opt}{install}	<p>Installs SF RPMs. Configuration can be performed at a later time using the <code>-configure</code> option.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{installallpkgs} or CFG{opt}{installrecpkgs} or CFG{opt}{installminpkgs}	<p>Instructs the installer to install SF RPMs based on the variable that has the value set to 1:</p> <ul style="list-style-type: none"> <li>■ <code>installallpkgs</code>: Installs all RPMs</li> <li>■ <code>installrecpkgs</code>: Installs recommended RPMs</li> <li>■ <code>installminpkgs</code>: Installs minimum RPMs</li> </ul> <p><b>Note:</b> Set only one of these variable values to 1. In addition to setting the value of one of these variables, you must set the variable <code>\$CFG{opt}{install}</code> to 1.</p> <p>List or scalar: scalar</p> <p>Optional or required: required</p>
CFG{accepteula}	<p>Specifies whether you agree with the EULA.pdf file on the media.</p> <p>List or scalar: scalar</p> <p>Optional or required: required</p>

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

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

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

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

## Sample response file for SF installation

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

```
our %CFG;

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

1;
```

## Configuring SF using response files

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

### To configure SF using response files

- 1 Make sure the SF RPMs 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 55.

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

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

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

See [“About the Veritas installer”](#) on page 25.

## Response file variables to configure Storage Foundation

[Table 8-2](#) lists the response file variables that you can define to configure SF.

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

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

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

Variable	List or Scalar	Description
CFG{opt}{configure}	Scalar	Performs the configuration if the RPMs are already installed.  (Required)  Set the value to 1 to configure SF.
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media.  (Required)
CFG{systems}	List	List of systems on which the product is to be configured.  (Required)
CFG{prod}	Scalar	Defines the product to be configured.  The value is VCS60 for VCS.  (Required)
CFG{opt}{keyfile}	Scalar	Defines the location of an ssh keyfile that is used to communicate with all remote systems.  (Optional)
CFG{opt}{rsh}	Scalar	Defines that <i>rsh</i> 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.  <b>Note:</b> The installer copies the response files and summary files also to the specified <i>logpath</i> location.  (Optional)



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

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

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



# Installing Storage Foundation using operating system-specific methods

This chapter includes the following topics:

- [Installing SF using Kickstart](#)
- [Sample Kickstart configuration file](#)
- [Installing Storage Foundation using yum](#)

## Installing SF using Kickstart

You can install SF using Kickstart. Kickstart is supported for Red Hat Enterprise Linux 5 (RHEL5) and Red Hat Enterprise Linux 6 (RHEL6).

To install SF using Kickstart

- 1 Create a directory for the Kickstart configuration files.

```
# mkdir /kickstart_files/
```

- 2 Generate the Kickstart configuration files. The configuration files have the extension `.ks`. Do one of the following:

- To generate configuration files, enter the following command:

```
# ./installer -kickstart /kickstart_files/
```

The system lists the files.

- If you only need to install Storage Foundation RPMs during the Kickstart operating system installation, that is, you do not need to generate the `.ks` configuration file for Veritas Cluster Server RPMs, run the `installsf` script. Enter the following:

```
# ./installsf -kickstart /kickstart_files/
```

The output includes the following:

```
The kickstart script for SF is generated at  
/kickstart_files/kickstart_sf601.ks
```

- 3 Setup an NFS exported location which the Kickstart client can access. For example, if `/nfs_mount_kickstart` is the directory which has been NFS exported, the NFS exported location may look similar to the following:

```
# cat /etc/exports  
/nfs_mount_kickstart * (rw, sync, no_root_squash)
```

- 4 Copy the `rpms` directory from the installation media to the NFS location.
- 5 Verify the contents of the directory.

```
# ls /nfs_mount_kickstart/
```

- 6 In the SF Kickstart configuration file, modify the `BUILDSRC` variable to point to the actual NFS location. The variable has the following format:

```
BUILDSRC="hostname_or_ip:/nfs_mount_kickstart"
```

- 7 Append the entire modified contents of the Kickstart configuration file to the operating system `ks.cfg` file.
- 8 Launch the Kickstart installation for the operating system.
- 9 After the operating system installation is complete, check the file `/var/tmp/kickstart.log` for any errors related to the installation of Veritas RPMs and Veritas product installer scripts.

- 10 Verify that all the product RPMs have been installed. Enter the following command:

```
# rpm -qa | grep -i vrts
```

- 11 If you do not find any installation issues or errors, configure the product stack. Enter the following command:

```
# /opt/VRTS/install/installsf<version> -configure node1 node2
```

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

See [“About the Veritas installer”](#) on page 25.

## Sample Kickstart configuration file

The following is a sample RedHat Enterprise Linux 5 (RHEL5) Kickstart configuration file.

```
# The packages below are required and will be installed from OS installation media
# automatically during the automated installation of products in the DVD, if they have not
# been installed yet.
```

```
%packages
libattr.i386
libacl.i386
```

```
%post --nochroot
# Add necessary scripts or commands here to your need
# This generated kickstart file is only for the automated installation of products in the
# DVD
```

```
PATH=$PATH:/sbin:/usr/sbin:/bin:/usr/bin
export PATH
```

```
#
# Notice:
# * Modify the BUILDSRC below according to your real environment
# * The location specified with BUILDSRC should be NFS accessible
#   to the Kickstart Server
# * Copy the whole directories of rpms from installation media
#   to the BUILDSRC
#
```

```
BUILDSRC="<hostname_or_ip>:/path/to/rpms"

#
# Notice:
# * You do not have to change the following scripts.
#

# Define path variables.
ROOT=/mnt/sysimage
BUILDDIR="${ROOT}/build"
RPMDIR="${BUILDDIR}/rpms"

# define log path
KSLOG="${ROOT}/var/tmp/kickstart.log"

echo "==== Executing kickstart post section: ====" >> ${KSLOG}

mkdir -p ${BUILDDIR}
mount -t nfs -o nolock,vers=3 ${BUILDSRC} ${BUILDDIR} >> ${KSLOG} 2>&1

# Install the RPMs in the following order.
for RPM in VRTSvlic VRTSperl VRTSspt VRTSvxvm VRTSaslapm VRTSob
VRTSslmconv VRTSsfmh VRTSvxfs VRTSfsadv VRTSfssdk VRTSdbed
VRTSodm VRTSsfcp1601

do
    echo "Installing package -- $RPM" >> ${KSLOG}
    rpm -U -v --root ${ROOT} ${RPMDIR}/${RPM}-* >> ${KSLOG} 2>&1
done

umount ${BUILDDIR}

CALLED_BY=KICKSTART ${ROOT}/opt/VRTS/install/bin/UXRT601/add_install_scripts >> ${KSLOG} 2>&1

exit 0
```

## Installing Storage Foundation using yum

You can install SF using yum. yum is supported for Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6.

## To install SF using yum

- 1 Run the `installsf -pkginfo` command to get SF RPMs.

```
# ./installsf -pkginfo
```

- 2 Add the SF RPMs into the yum repository. You can add SF RPMs into either a new repository or an existing repository with other RPMs. Use the `createrepo` command to create or update the repository. The operating system RPM `createrepo-ver-rel.noarch.rpm` provides the command.

### ■ To create the new repository */path/to/new/repository/* for SF RPMs

1. Create an empty directory, for example: */path/to/new/repository*. The yum client systems should be able to access the directory with the HTTP, FTP, or file protocols.

```
# rm -rf /path/to/new/repository  
# mkdir -p /path/to/new/repository
```

2. Copy all the SF RPMs into */path/to/new/repository/*.

```
# cp -f VRTSvlic-* VRTSperl-* ... VRTSsfcp601-*\  
/path/to/new/repository
```

3. Use the `createrepo` command to create the repository.

```
# /usr/bin/createrepo /path/to/new/repository
```

Output resembles:

```
27/27 - VRTSsfcp601-6.0.100.000-GA_GENERIC.noarch.rpm  
Saving Primary metadata  
Saving file lists metadata  
Saving other metadata
```

4. The metadata for this repository is created in */path/to/new/repository/repodata*.

### ■ To use an existing repository in */path/to/existing/repository/* for SF RPMs

1. Copy all the SF RPMs into */path/to/existing/repository/*. The yum client systems should be able to access the directory with the HTTP, FTP, or file protocols.

```
# cp -f VRTSvlic-* VRTSperl-* ... VRTSsfcp601-*\  
/path/to/existing/repository
```

2. Use the `createrepo` command with the `--update` option to update the repository's metadata.

```
# createrepo --update /path/to/existing/repository
```

Output resembles:

```
27/27 * VRTSsfcp601-6.0.100.000-GA_GENERIC.noarch.rpm  
Saving Primary metadata  
Saving file lists metadata  
Saving other metadata
```

3. The metadata in */path/to/existing/repository/repodata* is updated for the newly added RPMs.

■ **To create a package group for SF RPMs when the repository is created or updated (optional)**



1. Create an XML file, which you can name `SF_group.xml` in the repository directory. In the file specify the name, the id, the RPM list, and other information for the group. You can generate this XML file using the installer with the option `-yumgroupxml`. An example of this XML file for SF is:

```
# cat SF_group.xml
<comps>
  <group>
    <id>SF601</id>
    <name>SF601</name>
    <default>true</default>
    <description>RPMs of SF 6.01</description>
    <uservisible>true</uservisible>
    <packagelist>
      <packagereq type="default">VRTSvlic</packagereq>
      <packagereq type="default">VRTSperl</packagereq>
      ... [other RPMs for SF]
      <packagereq type="default">VRTSsfcp1601</packagereq>
    </packagelist>
  </group>
</comps>
```

2. Create the group when the repository is created or updated.

```
# createrepo -g SF_group.xml /path/to/new/repository/
```

Or

```
# createrepo -g SF_group.xml --update /path/to/existing\
/repository/
```

Refer to the *Red Hat Enterprise Linux Deployment Guide* for more information on yum repository configuration.

### 3 Configure a yum repository on a client system.

- Create a `.repo` file under `/etc/yum.repos.d/`. An example of this `.repo` file for SF is:

```
# cat /etc/yum.repos.d/SF.repo
[repo-SF]
name=Repository for SF
baseurl=file:///path/to/repository/
enabled=1
gpgcheck=0
```

The values for the `baseurl` attribute can start with `http://`, `ftp://`, or `file://`. The URL you choose needs to be able to access the `repodata` directory. It also needs to access all the SF RPMs in the repository that you create or update.

- Check the yum configuration. List SF RPMs.

```
# yum list 'VRTS*'
Available Packages
VRTSperl.x86_64          5.14.2.6-RHEL5.2      repo-SF
VRTSsfcp1601.noarch    6.0.100.000-GA_GENERIC repo-SF
VRTSvlic.x86_64        3.02.61.003-0         repo-SF
...
```

The SF RPMs may not be visible immediately if:

- the repository was visited before the SF RPMs were added, and
- the local cache of its metadata has not expired.

To eliminate the local cache of the repositories' metadata and get the latest information from the specified `baseurl`, run the following commands:

```
# yum clean expire-cache
# yum list 'VRTS*'
```

Refer to the *Red Hat Enterprise Linux Deployment Guide* for more information on yum repository configuration.

#### 4 Install the RPMs on the target systems.

- To install all the RPMs

1. Specify each RPM name as its yum equivalent. For example:

```
# yum install VRTSvlic VRTSperl ... VRTSsfcp1601
```

2. Specify all of the SF RPMs using its package glob. For example:

```
# yum install 'VRTS*'
```

3. Specify the group name if a group is configured for SF's RPMs. In this example, the group name is *SF601*:

```
# yum install @SF601
```

Or

```
# yum groupinstall SF601
```

## ■ To install one RPM at a time

1. Run the `installsf -pkginfo` command to determine package installation order.

```
# ./installsf -pkginfo
```

The following Veritas Storage Foundation RPMs must be installed in the specified order to achieve full functionality. The RPMs listed are all the RPMs offered by the Veritas Storage Foundation product.

```
RPMs: VRTSperl VRTSvlic VRTSspt VRTSvxvm VRTSaslapm VRTSob  
VRTSslmconv VRTSvxfs VRTSfsadv VRTSfssdk VRTSdbed VRTSodm  
VRTSsfmh VRTSsfcp1601
```

The following Veritas Storage Foundation RPMs must be installed in the specified order to achieve recommended functionality. The RPMs listed are the recommended s for Veritas Storage Foundation offering basic and some advanced functionality for the product.

```
RPMs: VRTSperl VRTSvlic VRTSspt VRTSvxvm VRTSaslapm VRTSob  
VRTSvxfs VRTSfsadv VRTSdbed VRTSodm VRTSsfmh VRTSsfcp1601
```

The following Veritas Storage Foundation RPMs must be installed in the specified order to achieve basic functionality. The RPMs listed provide minimum footprint of the Veritas Storage Foundation product.

```
RPMs: VRTSperl VRTSvlic VRTSvxvm VRTSaslapm VRTSvxfs  
VRTSfsadv VRTSsfcp1601
```

2. Use the same order as the output from the `installsf -pkginfo` command:

```
# yum install VRTSperl
# yum install VRTSvlic
...
# yum install VRTSsfcp601
```

- 5 After you install all the RPMs, use the `/opt/VRTS/install/installsf<version>` script to license, configure, and start the product.

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

See [“About the Veritas installer”](#) on page 25.

If the VRTSsfcp601 RPM is installed before you use yum to install SF, this RPM is not upgraded or uninstalled. If the `/opt/VRTS/install/installsf<release_version>` script is not created properly, use the `/opt/VRTS/install/bin/UXRT601/add_install_scripts` script to create the `installsf` or `uninstallsf` scripts after all the other SF RPMs are installed. For example, your output may be similar to the following, depending on the products you install:

```
# /opt/VRTS/install/bin/UXRT601/add_install_scripts
Creating install/uninstall scripts for installed products
Creating /opt/VRTS/install/installdmp601 for UXRT601
Creating /opt/VRTS/install/uninstalldmp601 for UXRT601
Creating /opt/VRTS/install/installfs601 for UXRT601
Creating /opt/VRTS/install/uninstallfs601 for UXRT601
Creating /opt/VRTS/install/installsf601 for UXRT601
Creating /opt/VRTS/install/uninstallsf601 for UXRT601
Creating /opt/VRTS/install/installvm601 for UXRT601
Creating /opt/VRTS/install/uninstallvm601 for UXRT601
```

# Configuring Storage Foundation

This chapter includes the following topics:

- [Configuring Storage Foundation using the installer](#)
- [Configuring Storage Foundation manually](#)
- [Configuring the SFDB repository database after installation](#)

## Configuring Storage Foundation using the installer

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

**To start Storage Foundation**

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

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

## Configuring Storage Foundation manually

You can manually configure different products within Storage Foundation.

## Configuring Veritas Volume Manager

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

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

## 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/fstab
```

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 file system.

In some instances, you may find it efficient to load the file system module manually. For example, some larger class systems can have many dual interface I/O cards with multiple disk chains attached. The device interrogation process when such a system is rebooted can be very time consuming, so to avoid doing a reboot, use the `modprobe` command to load the `vxfs` module:

```
# modprobe vxfs ; modprobe vxportal ; modprobe fdd
```

Do not use the `insmod` command to load the `vxfs` module as `insmod` does not examine the module configuration file `/etc/modprobe.conf`.

To determine if the modules successfully loaded, use the `lsmod` command as shown here:

```
# lsmod | grep vxportal
vxportal                2952          0
vxfs                    3427960       0    fdd vxportal
```

```
# lsmod | grep fdd
fdd                67212              0      (unused)
vxfs               3427960            0      [fdd vxportal]
# lsmod | grep vxfs
vxfs               3427960            0      [fdd vxportal]
```

The first field in the output is the module name. You can unload the modules by entering:

```
# rmmod fdd
# rmmod vxportal
# rmmod vxfs
```

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

```
# df -T | grep vxfs
```

## 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 or DB2. For SFDB repository set up procedures:

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

See *Veritas Storage Foundation: Storage and Availability Management for DB2 Databases*





# Upgrade of SF

- [Chapter 11. Planning to upgrade SF](#)
- [Chapter 12. Upgrading Storage Foundation](#)
- [Chapter 13. Performing an automated SF upgrade using response files](#)
- [Chapter 14. Performing post-upgrade tasks](#)



# Planning to upgrade SF

This chapter includes the following topics:

- [Upgrade methods for SF](#)
- [Supported upgrade paths for SF 6.0.1](#)
- [About using the installer to upgrade when the root disk is encapsulated](#)
- [Preparing to upgrade SF](#)

## Upgrade methods for SF

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

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

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

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

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

## Supported upgrade paths for SF 6.0.1

The following tables describe upgrading to 6.0.1.

**Table 11-2** RHEL 5 x64 upgrades using the script- or Web-based installer

Veritas software versions	RHAS 2.1 or RHEL 3	RHEL 4	RHEL 5
3.4.x 4.0	No upgrade path exists. Uninstall the product. Upgrade to RHEL 5 U5. Use the installer to install 6.0.1.	N/A	N/A
4.1 4.1 MP1 4.1 MP2 4.1 MP3 4.1 MP4	N/A	No upgrade path exists. Uninstall the product. Upgrade to RHEL 5 U5. Use the installer to install 6.0.1.	No upgrade path exists. Uninstall the product. Upgrade to RHEL 5 U5. Use the installer to install 6.0.1.
5.0 5.0 MP1 5.0 MP2	N/A	No upgrade path exists. Uninstall the product. Upgrade to RHEL 5 U5. Use the installer to install 6.0.1.	N/A
5.0 MP3 5.0 MP4	N/A	No upgrade path exists. Uninstall the product. Upgrade to RHEL 5 U5. Use the installer to install 6.0.1.	Upgrade to RHEL5 U5. Use the installer to upgrade to 6.0.1.

**Table 11-2** RHEL 5 x64 upgrades using the script- or Web-based installer  
*(continued)*

Veritas software versions	RHAS 2.1 or RHEL 3	RHEL 4	RHEL 5
5.1 5.1 RPx 5.1 PR1 5.1 SP1 5.1 SP1 RPx	N/A	N/A	Upgrade to RHEL5 U5. Use the installer to upgrade to 6.0.1.
6.0 6.0 RP1	N/A	N/A	Upgrade to RHEL5 U5. Use the installer to upgrade to 6.0.1.

**Table 11-3** RHEL6 x64 upgrades using the script- or Web-based installer

Veritas software versions	RHEL 4	RHEL5	RHEL 6
4.1 4.1 MP1 4.1 MP2 4.1 MP3 4.1 MP4	No upgrade path exists. Uninstall the product. Upgrade to RHEL 6 U2. Use the installer to install to 6.0.1.	No upgrade path exists. Uninstall the product. Upgrade to RHEL 6 U2. Use the installer to install to &Version;.	N/A
5.0 5.0 MP1 5.0 MP2	No upgrade path exists. Uninstall the product. Upgrade to RHEL 6 U2. Use the installer to install to &Version;.	N/A	N/A
5.0 MP3 5.0 MP4	No upgrade path exists. Uninstall product. Upgrade to RHEL 6 U2. Use the installer to install to &Version;.	No upgrade path exists. Uninstall product. Upgrade to RHEL 6 U2. Use the installer to install to &Version;.	N/A

**Table 11-3** RHEL6 x64 upgrades using the script- or Web-based installer  
(continued)

Veritas software versions	RHEL 4	RHEL5	RHEL 6
5.1 5.1 RPx 5.1 PR1 5.1 SP1 5.1 SP1 RPx	N/A	No upgrade path exists. Uninstall product. Upgrade to RHEL 6 U2. Use the installer to install to &Version;.	Upgrade to RHEL 6 U2 or RHEL 6 U3 and then use the installer to upgrade to &Version;.
5.1 SP1 PR2 5.1 SP1PR3	N/A	N/A	Upgrade to RHEL 6 U2. Upgrade VM P-patch for RHEL 6 U2 if VRTSvxvm is installed. Use the installer to upgrade to &Version;.
6.0 6.0 RP1	N/A	No Upgrade Path exists. Uninstall product. Upgrade to RHEL 6 U2. Use the installer to install to &Version;.	Upgrade to RHEL6 U2 or later. Use the installer to upgrade to 6.0.1.

**Table 11-4** SLES 10 x64 upgrades using the script- or Web-based installer

Veritas software versions	SLES 8	SLES 9	SLES 10
3.4.x	No upgrade path exists. Uninstall the product. Upgrade to SLES10 SP4. Use the installer to install &Version;.	N/A	N/A
4.1 4.1 MP1 4.1 MP2	N/A	No upgrade path exists. Uninstall the product. Upgrade to SLES10 SP4. Use the installer to install &Version;.	N/A

**Table 11-4** SLES 10 x64 upgrades using the script- or Web-based installer  
*(continued)*

Veritas software versions	SLES 8	SLES 9	SLES 10
4.1 MP3 4.1 MP4	N/A	No upgrade path exists. Uninstall the product. Upgrade to SLES10 SP4. Use the installer to install &Version;.	No upgrade path exists. Uninstall the product. Upgrade to SLES10 SP4. Use the installer to install &Version;.
5.0 5.0 MP1 5.0 MP2	N/A	No upgrade path exists. Uninstall the product. Upgrade to SLES10 SP4. Use the installer to install &Version;.	N/A
5.0 MP3 5.0 MP4	N/A	No upgrade path exists. Uninstall the product. Upgrade to SLES10 SP4. Use the installer to install &Version;.	Upgrade to SLES10 SP4. Use the installer to upgrade to &Version;.
5.0 RU4 5.1 5.1 RPx 5.1 PR1 5.1 SP1 5.1 SP1 RPx	N/A	N/A	Upgrade to SLES10 SP4. Use the installer to upgrade to &Version;.
6.0 6.0 RP1	N/A	N/A	Upgrade directly to 6.0.1 using the installer script.

**Table 11-5** SLES 11 x64 upgrades using the script- or Web-based installer

Veritas software versions	SLES 9	SLES 10	SLES 11
4.1 4.1 MP1 4.1 MP2 5.0 5.0 MP1 5.0 MP2	No upgrade path exists. Uninstall the product. Upgrade to SLES11 SP1 or SP2. Use the installer to install &Version;.	N/A	N/A
4.1 MP3 4.1 MP4 5.0 MP3	No upgrade path exists. Uninstall the product. Upgrade to SLES11 SP1 or SP2 . Use the installer to install &Version;.	No upgrade path exists. Uninstall the product. Upgrade to SLES11 SP1 or SP2. Use the installer to install &Version;.	N/A
5.0 MP4	No upgrade path exists. Uninstall the product. Upgrade to SLES11 SP1 or SP2. Use the installer to install &Version;.	No upgrade path exists. Uninstall the product. Upgrade to SLES11 SP1 or SP2. Use the installer to install &Version;.	Upgrade to SLES11 SP1 or SP2. Use the installer to upgrade to &Version;.
5.0 RU1	N/A	N/A	Upgrade to SLES11 SP1 or SP2. Use the installer to upgrade to &Version;.
5.1 5.1 RPx 5.1 SP1 5.1 SP1 RPx	N/A	N/A	Upgrade to SLES11 SP1 or SP2. Use the installer to upgrade to &Version;.
6.0 6.0 RP1	N/A	N/A	No upgrade path exists. Uninstall product. Upgrade to SLES11 SP1 or SP2. Upgrade directly to 6.0.1 using the installer script.



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

When you use the installer to upgrade from a previous version of SF and the system where you plan to upgrade has an encapsulated root disk, you may have to unencapsulate it.

**Table 11-6** Upgrading using installer when the root disk is encapsulated

Starting version	Ending version	Action required
5.0 MP3	6.0.1	You need to unencapsulate the root disk. The installer exits.
5.1 or 5.1 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
5.1 SP1 or 5.1 SP1 RPx	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.
6.0 or 6.0 RP1	6.0.1	Do not unencapsulate. The installer runs normally. Reboot after upgrade.

## Preparing to upgrade SF

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

### Getting ready for the upgrade

Complete the following tasks before you perform the upgrade:

- Review the *Veritas Storage Foundation Release Notes* for any late-breaking information on upgrading your system.
- Review the Symantec Technical Support website for additional information: <http://www.symantec.com/techsupp/>
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.

- Make sure that all users are logged off and that all major user applications are properly shut down.
- Make sure that you have created a valid backup.  
See [“Creating backups”](#) on page 82.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the RPMs, for example `/packages/Veritas` when the root file system has enough space or `/var/tmp/packages` if the `/var` file system has enough space.  
Do not put the files under `/tmp`, which is erased during a system reboot. Do not put the files on a file system that is inaccessible prior to running the upgrade script.  
You can use a Veritas-supplied disc for the upgrade as long as modifications to the upgrade script are not required. If `/usr/local` was originally created as a slice, modifications are required.
- For any startup scripts in `/sbin/rcS.d`, comment out any application commands or processes that are known to hang if their file systems are not present.
- Make sure that the current operating system supports version 6.0.1 of the product. If the operating system does not support it, plan for a staged upgrade.
- Schedule sufficient outage time and downtime for the upgrade and any applications that use the Veritas products. Depending on the configuration, the outage can take several hours.
- Any swap partitions not in `rootdg` must be commented out of `/etc/fstab`. If possible, swap partitions other than those on the root disk should be commented out of `/etc/fstab` and not mounted during the upgrade. Active swap partitions that are not in `rootdg` cause `upgrade_start` to fail.
- Make sure the file systems are clean before upgrading.
- Upgrade arrays (if required).  
See [“Upgrading the array support”](#) on page 87.
- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a fallback point.
- Determine if the root disk is encapsulated.  
See [“Determining if the root disk is encapsulated”](#) on page 84.

## Creating backups

Save relevant system information before the upgrade.

### To create backups

- 1 Log in as superuser.
- 2 Before the upgrade, ensure that you have made backups of all data that you want to preserve.
- 3 Back up information in files such as `/boot/grub/menu.lst`, `/etc/grub.conf` or `/etc/lilo.conf`, and `/etc/fstab`.
- 4 Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

If not, a warning message is displayed.

---

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

---

- 5 Copy the `fstab` file to `fstab.orig`:
 

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

## Tasks for upgrading the Storage Foundation for Databases (SFDB)

Tasks for upgrading SFDB tools to version 6.0.1:

- Preparing to migrate the repository database before upgrading from 5.0x or earlier to 6.0.1  
See [“Pre-upgrade tasks for migrating the SFDB repository database”](#) on page 84.
- Migrating the repository database after upgrading from 5.0.x or earlier to 6.0.1  
See [“Post upgrade tasks for migrating the SFDB repository database”](#) on page 103.

---

**Caution:** If you are running Oracle version 11.1.0.6 and upgrading a Storage Foundation product to 6.0.1: upgrade the Oracle binaries and database to version 11.1.0.7 before moving to 6.0.1.

---

## Determining if the root disk is encapsulated

Check if the system's root disk is under VxVM control by running this command:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootdg/rootvol` is listed as being mounted as the root (`/`) file system.

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

See [“About using the installer to upgrade when the root disk is encapsulated”](#) on page 81.

## Pre-upgrade tasks for migrating the SFDB repository database

If you plan to continue using Database Storage Checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle, you must prepare to migrate the SFDB repository database to 6.0.1 before upgrading to Storage Foundation or Storage Foundation for Oracle RAC 6.0.1.

---

**Note:** The `Sfua_Base` repository resource group will be removed from the `main.cf` file. It is not required as a separate service group for SF 6.0.1.

---

Perform the following before upgrading SF.

**To prepare to migrate the repository database**

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

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

---

**Warning:** The Database Flashsnap clone database will not be able to be carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 6.0.1.

---

## Pre-upgrade planning for Veritas Volume Replicator

Before installing or upgrading Veritas Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.

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

```
# vxdg list diskgroup
```

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

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

---

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

---

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.

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

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

## Planning an upgrade from the previous VVR version

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

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

Replicating between versions is intended to remove the restriction of upgrading the Primary and Secondary at the same time. VVR can continue to replicate an existing RDS with Replicated Volume Groups (RVGs) on the systems that you

want to upgrade. When the Primary and Secondary are at different versions, VVR does not support changing the configuration with the `vradmin` command or creating a new RDS.

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in [Table 11-7](#), if either the Primary or Secondary are running a version of VVR prior to 6.0.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.0.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

**Table 11-7** VVR versions and checksum calculations

VVR prior to 6.0.1 (DG version <= 140)	VVR 6.0.1 (DG version >= 150)	VVR calculates checksum TCP connections?
Primary	Secondary	Yes
Secondary	Primary	Yes
Primary and Secondary		Yes
	Primary and Secondary	No

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

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

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

### Planning and upgrading VVR to use IPv6 as connection protocol

Storage Foundation supports using IPv6 as the connection protocol.

This release supports the following configurations for VVR:

- VVR continues to support replication between IPv4-only nodes with IPv4 as the internet protocol
- VVR supports replication between IPv4-only nodes and IPv4/IPv6 dual-stack nodes with IPv4 as the internet protocol

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

## Upgrading the array support

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

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

See “[Hardware compatibility list \(HCL\)](#)” on page 20.

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

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

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





# Upgrading Storage Foundation

This chapter includes the following topics:

- [Upgrading Storage Foundation from previous versions to 6.0.1](#)
- [Upgrading Storage Foundation using the Veritas Web-based installer](#)
- [Upgrading Veritas Volume Replicator](#)

## Upgrading Storage Foundation from previous versions to 6.0.1

If you are running an earlier release of Storage Foundation, you can upgrade to the latest version using the procedures described in this chapter.

See [“Upgrading Storage Foundation using the script-based installer”](#) on page 89.

If you need to upgrade your kernel with Veritas Storage Foundation 6.0.1 already installed, use the kernel upgrade procedure.

See the *Veritas Storage Foundation Administrator's Guide* for information about upgrading the kernel.

## Upgrading Storage Foundation using the script-based installer

Use this procedure to upgrade Storage Foundation (SF).

### To upgrade SF from previous versions to 6.0.1

- 1 Log in as superuser.
- 2 Use the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -F | grep vxfs
```

- 3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name  
# umount /filesystem
```

- 4 Verify that all file systems have been cleanly unmounted:

```
# echo "8192B.p S" | fsdb -t vxfs filesystem | grep clean  
flags 0 mod 0 clean clean_value
```

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

Perform the following steps in the order listed:

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

```
# fsck -t vxfs filesystem  
# mount -t vxfs filesystem mountpoint  
# umount mountpoint
```

This should complete any extended operations that were outstanding on the file system and unmount the file system cleanly.

There may be a pending large RPM clone removal extended operation if the `umount` command fails with the following error:

```
file system device busy
```

You know for certain that an extended operation is pending if the following message is generated on the console:

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

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

- Repeat this step to verify that the unclean file system is now clean.

- 5 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.
- 6 Stop all the volumes by entering the following command for each disk group:

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

To verify that no volumes remain open, use the following command:

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

- 7 Make a record of the mount points for VxFS file systems and VxVM volumes that are defined in the `/etc/fstab` file. You will need to recreate these entries in the `/etc/fstab` file on the freshly installed system.
- 8 Perform any necessary preinstallation checks.  
See [“About planning for SF installation”](#) on page 23.
- 9 To invoke the installer, run the `installer` command on the disc as shown in this example:

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

- 10 Enter `G` to upgrade and press Return.
- 11 You are prompted to enter the system names (in the following example, "host1") on which the software is to be installed. Enter the system name or names and then press Return.

```
Enter the 64 bit <platform> system names separated
by spaces : [q, ?] host1 host2
```

where `<platform>` is the platform on which the system runs, such as RHEL5.

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

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

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

- 13 The installer lists the RPMs to install or upgrade. You are prompted to confirm that you are ready to upgrade.
- 14 The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's boot disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer **y**.
- 15 The installer then prompts you to name the backup boot disk group. Enter the name for it or press **Enter** to accept the default.
- 16 You are prompted to start the split operation. Press **y** to continue.

---

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

---

- 17 Stop the product's processes.

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

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

- 18 The installer stops, uninstalls, reinstalls, and starts specified RPMs.
- 19 If necessary, reinstate any missing mount points in the `/etc/fstab` file on each node that you recorded in step 7.
- 20 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

- 21 Remount all VxFS file systems and Storage Checkpoints on all nodes:

```
# mount /filesystem  
# mount /checkpoint_name
```

- 22 You can perform the following optional configuration steps:
  - If you want to use features of Veritas Storage Foundation 6.0.1 for which you do not currently have an appropriate license installed, obtain the license and run the `vxlicinst` command to add it to your system.
  - To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.

See [“Upgrading VxVM disk group versions”](#) on page 109.

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

See [“Re-joining the backup boot disk group into the current disk group”](#) on page 102.

See [“Reverting to the backup boot disk group after an unsuccessful upgrade”](#) on page 102.

## Upgrading Storage Foundation using the Veritas Web-based installer

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

### To upgrade SF

- 1** Perform the required steps to save any data that you wish to preserve. For example, make configuration file backups.
- 2** Start the Web-based installer.  
See [“Starting the Veritas Web-based installer”](#) on page 46.
- 3** On the Select a task and a product page, select **Upgrade a Product** from the Task drop-down menu.  
The installer detects the product that is installed on the specified system. Click **Next**.
- 4** Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click **Next**.
- 5** On the License agreement page, select whether you accept the terms of the End User License Agreement (EULA). To continue, select **Yes I agree** and click **Next**.
- 6** The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the boot disk group. To create the backup, check the **Split mirrors on all the systems** box. Check the appropriate box to use the same name for the backup disk group on all systems--you can use the default name or choose a new one. Check the systems where you want to create the backup. When you are ready, click the **Next** button.

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

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

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

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

- 9 After the upgrade, if the product is not configured, the Web-based installer asks: "Do you want to configure this product?" If the product is already configured, it will not ask any questions.
- 10 Click **Finish**. The installer prompts you for another task.
- 11 Only perform this step if you have split the mirrored root disk to back it up. After a successful reboot, verify the upgrade and re-join the backup disk group into the upgraded boot disk group. If the upgrade fails, revert the upgrade boot disk group to the backup disk group.

See ["Re-joining the backup boot disk group into the current disk group"](#) on page 102.

See ["Reverting to the backup boot disk group after an unsuccessful upgrade"](#) on page 102.

## Upgrading Veritas Volume Replicator

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

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

See ["Upgrading VVR without disrupting replication"](#) on page 94.

## Upgrading VVR without disrupting replication

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

You may also need to set up replication between versions.

See ["Planning an upgrade from the previous VVR version"](#) on page 85.

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

---

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

---

## Upgrading VVR on the Secondary

Follow these instructions to upgrade the Secondary hosts.

### To upgrade the Secondary

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

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

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

- 3 Do one of the following:

- Upgrade the disk group now. Enter the following:

```
# vxdg upgrade dgname
```

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

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

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

## Upgrading VVR on the Primary

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

### To upgrade the Primary

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

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

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

- 3 Do one of the following:

- Upgrade the disk group now. Enter the following:

```
# vxdg upgrade dgname
```

- Upgrade the disk group later.

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

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

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

See [“Planning an upgrade from the previous VVR version”](#) on page 85.



# Performing an automated SF upgrade using response files

This chapter includes the following topics:

- [Upgrading SF using response files](#)
- [Response file variables to upgrade Storage Foundation](#)
- [Sample response file for SF upgrade](#)

## Upgrading SF using response files

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

### To perform automated SF upgrade

- 1 Make sure the systems where you want to upgrade SF meet the upgrade requirements.
- 2 Make sure the pre-upgrade tasks are completed.
- 3 Copy the response file to one of the systems where you want to upgrade SF.
- 4 Edit the values of the response file variables as necessary.

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

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

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

See [“About the Veritas installer”](#) on page 25.

## Response file variables to upgrade Storage Foundation

[Table 13-1](#) lists the response file variables that you can define to configure SF.

**Table 13-1** Response file variables for upgrading SF

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

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

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

## Sample response file for SF upgrade

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

```
our %CFG;

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

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

# Performing post-upgrade tasks

This chapter includes the following topics:

- [Optional configuration steps](#)
- [Re-joining the backup boot disk group into the current disk group](#)
- [Reverting to the backup boot disk group after an unsuccessful upgrade](#)
- [Post upgrade tasks for migrating the SFDB repository database](#)
- [Recovering VVR if automatic upgrade fails](#)
- [Upgrading disk layout versions](#)
- [Upgrading VxVM disk group versions](#)
- [Updating variables](#)
- [Setting the default disk group](#)
- [Verifying the Storage Foundation upgrade](#)

## Optional configuration steps

After the upgrade is complete, additional tasks may need to be performed.

You can perform the following optional configuration steps:

- If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:
  - Reattach the RLINKs.
  - Associate the SRL.

**Re-joining the backup boot disk group into the current disk group**

- To encapsulate and mirror the boot disk, follow the procedures in the "Administering Disks" chapter of the *Veritas Storage Foundation Administrator's Guide*.
- To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.  
See ["Upgrading VxVM disk group versions"](#) on page 109.

## Re-joining the backup boot disk group into the current disk group

Perform this procedure to rejoin the backup boot disk if you split the mirrored boot disk during upgrade. After a successful upgrade and reboot, you no longer need to keep the boot disk group backup.

### To re-join the backup boot disk group

- ◆ Re-join the *backup\_bootdg* disk group to the boot disk group.

```
# /etc/vx/bin/vxrootadm -Y join backup_bootdg
```

where the `-Y` option indicates a silent operation, and *backup\_bootdg* is the name of the backup boot disk group that you created during the upgrade.

## Reverting to the backup boot disk group after an unsuccessful upgrade

Perform this procedure if your upgrade was unsuccessful and you split the mirrored boot disk to back it up during upgrade. You can revert to the backup that you created when you upgraded.

### To revert the backup boot disk group after an unsuccessful upgrade

- 1 To determine the boot disk groups, look for the *rootvol* volume in the output of the `vxprint` command.

```
# vxprint
```

- 2 Use the `vxpdg` command to find the boot disk group where you are currently booted.

```
# vxpdg bootdg
```

- 3 Boot the operating system from the backup boot disk group.
- 4 Join the original boot disk group to the backup disk group.

```
# /etc/vx/bin/vxrootadm -Y join original_bootdg
```

where the `-Y` option indicates a silent operation, and `original_bootdg` is the boot disk group that you no longer need.

## Post upgrade tasks for migrating the SFDB repository database

Database Storage Checkpoints that have been created by using the SFDB tools before upgrade are visible using the `vxsfadm` CLI, and you can mount these Database Storage Checkpoints and roll back to them, if required. However, creating clones by using migrated Database Storage Checkpoints is not supported.

If you want to continue using previously created FlashSnap snapplans to take snapshots, you must validate them by using the `-o validate` option of the `vxsfadm` command.

To continue using the Database Storage Checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle, you must perform one of the following procedures after upgrading SF to 6.0.1:

- Rename startup script after upgrading from 5.0x and before migrating the SFDB repository  
 See [“After upgrading from 5.0.x and before migrating SFDB”](#) on page 108.
- Migrate from a 5.0x SFDB repository database to 6.0.1  
 See [“Migrating from a 5.0 repository database to 6.0.1”](#) on page 103.
- Migrate from a 5.1 or 5.1SP1 repository database to 6.0.1  
 See [“Migrating from a 5.1 or higher repository database to 6.0.1”](#) on page 106.

### Migrating from a 5.0 repository database to 6.0.1

To migrate from a 5.0 repository database to 6.0.1

- 1 Rename the startup script `NO_S*vxdbms3` to `S*vxdbms3`.  
 See [“After upgrading from 5.0.x and before migrating SFDB”](#) on page 108.
- 2 As root, dump out the old Sybase ASA repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

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

- 3 On the same node that you ran `sfua_rept_migrate` run the following command as Oracle user. For each Oracle instance, migrate the old repository data to the SQLite repository.

```
$ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

- 4 By default, the repository is created on the file system which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- Repository path has to be a directory writable by Oracle user.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

Create an alternate repository path.

```
$ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \  
Alternate_path
```

- 5 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform the previous steps on the secondary host.



- 6 On the primary host, edit your snapplans to remove the "SNAPSHOT\_DG=SNAP\_\*" parameter and add "SNAPSHOT\_DG\_PREFIX=SNAP\_\*". The parameter can be any PREFIX value and not necessarily "SNAP\_\*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=system1_data
SNAPSHOT_DG=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=judge_data
SNAPSHOT_DG_PREFIX=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

- 7 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/vxsfadm -s flashsnap \  
-a oracle -c SNAPPLAN -o validate
```

This completes the migration of the repository for Database Storage Checkpoints and Database Tiered Storage parameters.

To begin using the Storage Foundation for Databases (SFDB) tools:

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

## Migrating from a 5.1 or higher repository database to 6.0.1

### To migrate from a 5.0 repository database to 6.0.1

- 1 Run the following command as Oracle user. For each Oracle instance, migrate the old repository data to the SQLite repository.

```
$ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME
```

- 2 By default, the repository is created on the file system which contains the Oracle SYSTEM tablespace. If you need an alternative repository path, first verify the following requirements:

- Repository path has to be a directory writable by Oracle user.
- The update commands will not be able to verify accessibility of the repository path and will fail if you have not set up the path correctly.

Create an alternate repository path.

```
$ /opt/VRTS/bin/dbed_update -S $ORACLE_SID -H $ORACLE_HOME -R \  
Alternate_path
```

- 3 If you are using Database Flashsnap for off-host processing, and if you have a repository on the secondary host that you need to migrate: perform the previous steps on the secondary host.

- 4 On the primary host, edit your snapplans to remove the "SNAPSHOT\_DG=SNAP\_\*" parameter and add "SNAPSHOT\_DG\_PREFIX=SNAP\_\*. The parameter can be any PREFIX value and not necessarily "SNAP\_\*".

For example:

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=system1_data
SNAPSHOT_DG=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

```
$ /usr/oracle> more SNAPPLAN1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=system1
SECONDARY_HOST=system1.example.com
PRIMARY_DG=judge_data
SNAPSHOT_DG_PREFIX=SNAP_system1_data
ORACLE_SID=HN1
ARCHIVELOG_DEST=/oracle/orahome/dbs/arch
SNAPSHOT_ARCHIVE_LOG=yes
SNAPSHOT_MODE=online
SNAPSHOT_PLAN_FOR=database
SNAPSHOT_PLEX_TAG=dbed_flashsnap
SNAPSHOT_VOL_PREFIX=SNAP_
ALLOW_REVERSE_RESYNC=no
SNAPSHOT_MIRROR=1
```

- 5 On the primary host, revalidate your snapshots using the following command:

```
$ /opt/VRTS/bin/vxsfadm -s flashsnap \  
-a oracle -c SNAPPLAN -o validate
```

This completes the migration of the repository for Database Storage Checkpoints and Database Tiered Storage parameters.

To begin using the Storage Foundation for Databases (SFDB) tools:

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

## After upgrading from 5.0.x and before migrating SFDB

When upgrading from SF version 5.0 to SF 6.0.1 the S\*vxdbms3 startup script is renamed to NO\_S\*vxdbms3. The S\*vxdbms3 startup script is required by sfua\_rept\_migrate. Thus when sfua\_rept\_migrate is run, it is unable to find the S\*vxdbms3 startup script and gives the error message:

```
/sbin/rc3.d/S*vxdbms3 not found  
SFORA sfua_rept_migrate ERROR V-81-3558 File: is missing.  
SFORA sfua_rept_migrate ERROR V-81-9160 Failed to mount repository.
```

To prevent S\*vxdbms3 startup script error

- ◆ Rename the startup script NO\_S\*vxdbms3 to S\*vxdbms3.

## Recovering VVR if automatic upgrade fails

If the upgrade fails during the configuration phase, after displaying the VVR upgrade directory, the configuration needs to be restored before the next attempt. Run the scripts in the upgrade directory in the following order to restore the configuration:

```
# restoresrl  
# addcm  
# srlprot  
# attrlink  
# start.rvg
```

After the configuration is restored, the current step can be retried.

## Upgrading disk layout versions

In this release, you can create and mount only file systems with disk layout Version 7, 8, and 9. You can only local mount disk layout Version 6 only to upgrade to a later disk layout version.

Disk layout Version 6 has been deprecated and you cannot cluster mount an existing file system that has disk layout Version 6. To upgrade a cluster file system with disk layout Version 6, you must local mount the file system and then upgrade the file system using the `vxupgrade` utility to a later version.

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

Support for disk layout Version 4 has been removed. You must upgrade any existing file systems with disk layout Version 4 to disk layout Version 7 or later using the `vxfsconvert` command.

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

---

**Note:** Symantec recommends that you upgrade existing file systems to the highest supported disk layout version prior to upgrading to this release.

---

You can check which disk layout version your file system has by using the following command:

```
# fstyp -v /dev/vx/dsk/dg1/vol1 | grep -i version
```

For more information about disk layout versions, see the *Veritas Storage Foundation Administrator's Guide*.

## Upgrading VxVM disk group versions

All Veritas Volume Manager disk groups have an associated version number. Each VxVM release supports a specific set of disk group versions. VxVM can import and perform tasks on disk groups with those versions. Some new features and tasks work only on disk groups with the current disk group version. Before you can perform the tasks or use the features, upgrade the existing disk groups.

For 6.0.1, the Veritas Volume Manager disk group version is different than in previous VxVM releases. Symantec recommends that you upgrade the disk group version if you upgraded from a previous VxVM release.

After upgrading to SF 6.0.1, you must upgrade any existing disk groups that are organized by ISP. Without the version upgrade, configuration query operations continue to work fine. However, configuration change operations will not function correctly.

For more information about ISP disk groups, refer to the *Veritas Storage Foundation Administrator's Guide*.

Use the following command to find the version of a disk group:

```
# vxdg list diskgroup
```

To upgrade a disk group to the current disk group version, use the following command:

```
# vxdg upgrade diskgroup
```

For more information about disk group versions, see the *Veritas Storage Foundation Administrator's Guide*.

## Updating variables

In `/etc/profile`, update the `PATH` and `MANPATH` variables as needed.

`MANPATH` could include `/opt/VRTS/man` and `PATH /opt/VRTS/bin`.

## Setting the default disk group

You may find it convenient to create a system-wide default disk group. The main benefit of creating a default disk group is that VxVM commands default to the default disk group. You do not need to use the `-g` option.

You can set the name of the default disk group after installation by running the following command on a system:

```
# vxdctl defaultdg diskgroup
```

See the *Veritas Storage Foundation Administrator's Guide*.

## Verifying the Storage Foundation upgrade

Refer to the section about verifying the installation to verify the upgrade.

See [“Verifying that the products were installed”](#) on page 113.

# Post-installation tasks

- [Chapter 15. Verifying the SF installation](#)





# Verifying the SF installation

This chapter includes the following topics:

- [Verifying that the products were installed](#)
- [Installation log files](#)
- [Starting and stopping processes for the Veritas products](#)
- [Checking Veritas Volume Manager processes](#)

## Verifying that the products were installed

Verify that the SF products are installed.

Use the command to check which RPMs have been installed.

```
# rpm -qa | grep VRTS
```

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

```
# /opt/VRTS/install/installsf<version>
```

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

See [“About the Veritas installer”](#) on page 25.

Use the following sections to further verify the product installation.

## Installation log files

After every product installation, the installer creates three text files:

- Installation log file
- Response file

### ■ Summary file

The name and location of each file is displayed at the end of a product installation, and are always located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep the files for auditing, debugging, and future use.

## Using the installation log file

The installation log file contains all commands executed during the procedure, their output, and errors generated by the commands. This file is for debugging installation problems and can be used for analysis by Veritas Support.

## Using the summary file

The summary file contains the results of the installation by the installer or product installation scripts. The summary includes the list of the RPMs, and the status (success or failure) of each RPM. The summary also indicates which processes were stopped or restarted during the installation. After installation, refer to the summary file to determine whether any processes need to be started.

# Starting and stopping processes for the Veritas products

After the installation and configuration is complete, the Veritas product installer starts the processes that are used by the installed products. You can use the product installer to stop or start the processes, if required.

### To stop the processes

- ◆ Use the `-stop` option to stop the product installation script.

For example, to stop the product's processes, enter the following command:

```
# ./installer -stop
```

or

```
# /opt/VRTS/install/installsf<version> -stop
```

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

See [“About the Veritas installer”](#) on page 25.

### To start the processes

- ◆ Use the `-start` option to start the product installation script.

For example, to start the product's processes, enter the following command:

```
# ./installer -start
```

or

```
# /opt/VRTS/install/installsf<version> -start
```

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

See [“About the Veritas installer”](#) on page 25.

## Checking Veritas Volume Manager processes

Use the following procedure to verify that Volume Manager processes are running.

### To confirm that key Volume Manager processes are running

- ◆ Type the following command:

```
# ps -ef | grep vx
```

Entries for the `vxiod`, `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.



# Uninstallation of SF

- [Chapter 16. Uninstalling Storage Foundation](#)
- [Chapter 17. Uninstalling SF using response files](#)



# Uninstalling Storage Foundation

This chapter includes the following topics:

- [Removing VxFS file systems](#)
- [Removing rootability](#)
- [Moving volumes to disk partitions](#)
- [Removing the Replicated Data Set](#)
- [Uninstalling SF RPMs using the script-based installer](#)
- [Uninstalling SF with the Veritas Web-based installer](#)
- [Removing license files \(Optional\)](#)
- [Removing the Storage Foundation for Databases \(SFDB\) repository after removing the product](#)

## Removing VxFS file systems

The VxFS RPM cannot be removed if there are any mounted VxFS file systems. Unmount all VxFS file systems before removing the RPM. After you remove the VxFS RPM, VxFS file systems are not mountable or accessible until another VxFS RPM is installed. It is advisable to back up VxFS file systems before installing a new VxFS RPM. If VxFS will not be installed again, all VxFS file systems must be converted to a new file system type.

### To remove VxFS file systems

- 1 Check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -T | grep vxfs
```

- 2 Make backups of all data on the file systems that you wish to preserve, or recreate them as non-VxFS file systems on non-VxVM volumes or partitions.

- 3 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
```

```
# umount /filesystem
```

- 4 Comment out or remove any VxFS file system entries from the `/etc/fstab` file.

## Removing rootability

Perform this procedure if you configured rootability by encapsulating the root disk.



### To remove rootability

- 1 Check if the system's root disk is under VxVM control by running this command:

```
# df -v /
```

The root disk is under VxVM control if `/dev/vx/dsk/rootdg/rootvol` is listed as being mounted as the root (`/`) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:

- 2 Use the `vxplex` command to remove all the plexes of the volumes `rootvol`, `swapvol`, `usr`, `var`, `opt` and `home` that are on disks other than the root disk.

For example, the following command removes the plexes `mirrootvol-01`, and `mirswapvol-01` that are configured on a disk other than the root disk:

```
# vxplex -o rm dis mirrootvol-01 mirswapvol-01
```

---

**Warning:** Do not remove the plexes that correspond to the original root disk partitions.

---

- 3 Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices:

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

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

## Moving volumes to disk partitions

All volumes must be moved to disk partitions.

This can be done using one of the following procedures:

- Back up the system fully onto tape and then recover from it.
- Back up each file system individually and then recover them all after creating new file systems on disk partitions.
- Use VxVM to move volumes incrementally onto disk partitions as described in the following section.

## Moving volumes onto disk partitions using VxVM

Use the following procedure to move volumes onto disk partitions.

### To move volumes onto disk partitions

- 1 Evacuate disks using the `vxdiskadm` program, VEA, or the `vxevac` script. You should consider the amount of target disk space required for this before you begin.

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 using the following commands:

```
# vxdg -g diskgroup rmdisk disk _media_name  
# vxdisk rm disk_access_name
```

- 3 Decide which volume to move first. If the volume to be moved 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 data on the volume is synced.
- 5 Create a partition on free disk space of the same size as the volume. If there is not enough free space for the partition, a new disk must be added to the system for the first volume removed. Subsequent volumes can use the free space generated by the removal of this volume.
- 6 Copy the data on the volume onto the newly created disk partition using a command similar to the following:

```
# dd if=/dev/vx/dsk/diskgroup/volume-name of=/dev/sdb2
```

where `sdb` is the disk outside of VxVM and `2` is the newly created partition on that disk.

- 7 Replace the entry for that volume (if present) in `/etc/fstab` with an entry for the newly created partition.
- 8 Mount the disk partition if the corresponding volume was previously mounted.
- 9 Stop the volume and remove it from VxVM using the following commands:

```
# vxvol -g diskgroup -f stop volume_name  
# vxedit -g diskgroup -rf rm volume_name
```

- 10 Remove any disks that have become free (have no subdisks defined on them) by removing volumes from VxVM control. To check if there are still some subdisks remaining on a particular disk, use the following command:

```
# vxprint -F "%snum" disk_media_name
```

- 11 If the output is not 0, there are still some subdisks on this disk that must be subsequently removed. If the output is 0, remove the disk from VxVM control using the following commands:

```
# vxdg -g diskgroup rmdisk disk_media_name  
# vxdisk rm disk_access_name
```

- 12 The free space now created can be used for adding the data in the next volume to be removed.
- 13 After all volumes have been converted into disk partitions successfully, reboot the system. After the reboot, none of the volumes should be open. To verify that none of the volumes are open, use the following command:

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

- 14 If any volumes remain open, repeat the steps listed above.

## 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 RPMs using the script-based installer

Use the following procedure to remove SF products.

Not all RPMs may be installed on your system depending on the choices that you made when you installed the software.

---

**Note:** After you uninstall the product, you cannot access any file systems you created using the default disk layout version in SF 6.0.1 with a previous version of SF.

---

## To shut down and remove the installed SF RPMs

- 1 Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/fstab`. 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 RPM (`VRTSvxvm`) is installed, read and follow the uninstallation procedures for VxVM.

- 4 Make sure you have performed all of the prerequisite steps.

- 5 Move to the `/opt/VRTS/install` directory and run the uninstall script.

```
# cd /opt/VRTS/install
```

```
# ./uninstallsf<version>
```

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

Or, if you are using `ssh` or `rsh`, use one of the following:

```
■ # ./uninstallsf<version> -rsh
```

```
■ # ./uninstallsf<version> -ssh
```

See [“About the Veritas installer”](#) on page 25.

- 6 The uninstall script prompts for the system name. Enter one or more system names, separated by a space, from which to uninstall SF, for example, `sys1`:

```
Enter the system names separated by spaces: [q?] sys1 sys2
```

- 7 The uninstall script prompts you to stop the product processes. If you respond yes, the processes are stopped and the RPMs are uninstalled.  
The uninstall script creates log files and displays the location of the log files.
- 8 Most RPMs have kernel components. In order to ensure complete removal, a system reboot is recommended after all RPMs have been removed.

## Uninstalling SF with the Veritas Web-based installer

This section describes how to uninstall using the Veritas Web-based installer.

---

**Note:** After you uninstall the product, you cannot access any file systems you created using the default disk layout Version in SF 6.0.1 with a previous version of SF.

---

### To uninstall SF

- 1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.
- 2 Start the Web-based installer.  
See [“Starting the Veritas Web-based installer”](#) on page 46.
- 3 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.
- 4 Select **Storage Foundation** from the Product drop-down list, and click **Next**.
- 5 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Next**.
- 6 After the validation completes successfully, click **Next** to uninstall SF on the selected system.
- 7 If there are any processes running on the target system, the installer stops the processes. Click **Next**.
- 8 After the installer stops the processes, the installer removes the products from the specified system.  
Click **Next**.

- 9 After the uninstall completes, the installer displays the location of the summary, response, and log files. If required, view the files to confirm the status of the removal.

- 10 Click **Finish**.

Most RPMs have kernel components. In order to ensure their complete removal, a system reboot is recommended after all the RPMs have been removed.

## Removing license files (Optional)

Optionally, you can remove the license files.

### To remove the VERITAS license files

- 1 To see what license key files you have installed on a system, enter:

```
# /sbin/vxlicrep
```

The output lists the license keys and information about their respective products.

- 2 Go to the directory containing the license key files and list them:

```
# cd /etc/vx/licenses/lic  
# ls -a
```

- 3 Using the output from step 1, identify and delete unwanted key files listed in step 2. Unwanted keys may be deleted by removing the license key file.

## Removing the Storage Foundation for Databases (SFDB) repository after removing the product

After removing the product, you can remove the SFDB repository file and any backups.

Removing the SFDB repository file disables the SFDB tools.

**To remove the SFDB repository**

- 1** Identify the SFDB repositories created on the host.

```
# cat /var/vx/vxdba/rep_loc
```

- 2** Remove the directory identified by the `location` key.
- 3** Remove the repository location file.

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

This completes the removal of the SFDB repository.



# Uninstalling SF using response files

This chapter includes the following topics:

- [Uninstalling SF using response files](#)
- [Response file variables to uninstall Storage Foundation](#)
- [Sample response file for SF uninstallation](#)

## Uninstalling SF using response files

Typically, you can use the response file that the installer generates after you perform SF uninstallation on one system to uninstall SF on other systems.

### To perform an automated uninstallation

- 1 Make sure that you meet the prerequisites to uninstall SF.
- 2 Copy the response file to one of the cluster systems where you want to uninstall SF.
- 3 Edit the values of the response file variables as necessary.
- 4 Start the uninstallation from the system to which you copied the response file. For example:

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

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

See [“About the Veritas installer”](#) on page 25.

# Response file variables to uninstall Storage Foundation

Table 17-1 lists the response file variables that you can define to configure SF.

**Table 17-1** Response file variables for uninstalling SF

Variable	Description
CFG{systems}	List of systems on which the product is to be installed or uninstalled. List or scalar: list Optional or required: required
CFG{prod}	Defines the product to be installed or uninstalled. List or scalar: scalar Optional or required: required
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the RPMs that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional
CFG{opt}{uninstall}	Uninstalls SF RPMs. List or scalar: scalar Optional or required: optional

## Sample response file for SF uninstallation

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

```
our %CFG;  
  
$CFG{opt}{redirect}=1;  
$CFG{opt}{uninstall}=1;  
$CFG{prod}="SF601";  
$CFG{systems}=[ qw(thoropt89 thoropt90) ];  
  
1;
```



## Installation reference

- [Appendix A. Installation scripts](#)
- [Appendix B. Tunable files for installation](#)
- [Appendix C. Configuring the secure shell or the remote shell for communications](#)
- [Appendix D. Storage Foundation components](#)
- [Appendix E. Troubleshooting installation issues](#)
- [Appendix F. Compatibility issues when installing Storage Foundation with other products](#)



# Installation scripts

This appendix includes the following topics:

- [Installation script options](#)

## Installation script options

[Table A-1](#) shows command line options for the installation script. For an initial install or upgrade, options are not usually required. The installation script options apply to all Veritas Storage Foundation product scripts, except where otherwise noted.

See [“About the Veritas installer”](#) on page 25.

**Table A-1** Available command line options

Commandline Option	Function
-allpkgs	Displays all RPMs required for the specified product. The RPMs 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 <code>-comcleanup</code> 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 <i>full_path_to_file</i>	Specifies the location of a file that contains a list of hostnames on which to install.

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

Commandline Option	Function
-installallpkgs	The <code>-installallpkgs</code> option is used to select all RPMs.
-installrecpkgs	The <code>-installrecpkgs</code> option is used to select the recommended RPMs set.
-installminpkgs	The <code>-installminpkgs</code> option is used to select the minimum RPMs set.
-ignorepatchreqs	The <code>-ignorepatchreqs</code> option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
-keyfile <i>ssh_key_file</i>	Specifies a key file for secure shell (SSH) installs. This option passes <code>-i ssh_key_file</code> to every SSH invocation.
-kickstart <i>dir_path</i>	Produces a kickstart configuration file for installing with Linux RHEL Kickstart. The file contains the list of Symantec RPMs in the correct order for installing, in a format that can be used for Kickstart installations. The <i>dir_path</i> indicates the path to the directory in which to create the file.
-license	Registers or updates product licenses on the specified systems.
-logpath <i>log_path</i>	Specifies a directory other than <code>/opt/VRTS/install/logs</code> as the location where installer log files, summary files, and response files are saved.
-makeresponsefile	Use the <code>-makeresponsefile</code> option only to generate response files. No actual software installation occurs when you use this option.
-minpkgs	Displays the minimal RPMs required for the specified product. The RPMs are listed in correct installation order. Optional RPMs are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option.



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

Commandline Option	Function
-nolic	Allows installation of product RPMs without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
-pkginfo	Displays a list of RPMs and the order of installation in a human-readable format. This option only applies to the individual product installation scripts. For example, use the -pkginfo option with the installvcs script to display VCS RPMs.
-pkgpath <i>package_path</i>	Designates the path of a directory that contains all RPMs to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
-pkgset	Discovers and displays the RPM group (minimum, recommended, all) and RPMs that are installed on the specified systems.
-pkgtable	Displays product's RPMs 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 RPMs required for the specified product. The RPMs are listed in correct installation order. Optional RPMs are not listed. The output can be used to create scripts for command line installs, or for installations over a network. See <code>allpkgs</code> option.
-redirect	Displays progress details without showing the progress bar.

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

Commandline Option	Function
-requirements	The <code>-requirements</code> option displays required OS version, required RPMs and patches, file system space, and other system requirements in order to install the product.
-responsefile <i>response_file</i>	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The <i>response_file</i> 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.
-rsh	Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.  See <a href="#">“About configuring secure shell or remote shell communication modes before installing products”</a> on page 153.
-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.
-settnables	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 <code>-tunablesfile</code> option.
-start	Starts the daemons and processes for the specified product.
-stop	Stops the daemons and processes for the specified product.

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

Commandline Option	Function
-timeout	The <code>-timeout</code> option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the <code>-timeout</code> option overrides the default value of 1200 seconds. Setting the <code>-timeout</code> option to 0 prevents the script from timing out. The <code>-timeout</code> option does not work with the <code>-serial</code> option
-tmppath <i>tmp_path</i>	Specifies a directory other than <code>/var/tmp</code> as the working directory for the installation scripts. This destination is where initial logging is performed and where RPMs are copied on remote systems before installation.
-tunables	Lists all supported tunables and create a tunables file template.
-tunables_file <i>tunables_file</i>	Specify this option when you specify a tunables file. The tunables file should include tunable parameters.
-upgrade	Specifies that an existing version of the product exists and you plan to upgrade it.
-version	Checks and reports the installed products and their versions. Identifies the installed and missing RPMs and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing RPMs and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.
-yumgroupxml	The <code>-yumgroupxml</code> option is used to generate a yum group definition XML file. The <code>createrepo</code> command can use the file on Redhat Linux to create a yum group for automated installation of all RPMs for a product. An available location to store the XML file should be specified as a complete path. The <code>-yumgroupxml</code> option is supported on Redhat Linux only.



# Tunable files for installation

This appendix includes the following topics:

- [About setting tunable parameters using the installer or a response file](#)
- [Setting tunables for an installation, configuration, or upgrade](#)
- [Setting tunables with no other installer-related operations](#)
- [Setting tunables with an un-integrated response file](#)
- [Preparing the tunables file](#)
- [Setting parameters for the tunables file](#)
- [Tunables value parameter definitions](#)

## 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 142.

- When you apply the tunables file with no other installer-related operations.

```
# ./installer -tunablesfile tunables_file_name -setttunables [  
system1 system2 ...]
```

See [“Setting tunables with no other installer-related operations”](#) on page 143.

- 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 144.

See [“About response files”](#) on page 24.

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

See [“Tunables value parameter definitions”](#) on page 146.

## 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 146.

---

**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 145.
- 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 146.

---

**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 145.
- 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 `-setttunables` option.

```
# ./installer -tunablesfile tunables_file_name -setttunables [
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 146.

---

**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 145.
- 4 Copy the tunables file to one of the systems that you want to tune.
- 5 Mount the product disc and navigate to the directory that contains the installation program.
- 6 Start the installer with the `-responsefile` and `-tunablesfile` options.

```
# ./installer -responsefile response_file_name -tunablesfile
tunables_file_name
```

Where *response\_file\_name* is the full path name for the response file and *tunables\_file\_name* is the full path name for the tunables file.

- 7 Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.
- 8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.



## Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

You can use the installer to create a tunables file template, or manually format tunables files you create.

### To create a tunables file template

- ◆ Start the installer with the `-tunables` option. Enter the following:

```
# ./installer -tunables
```

You see a list of all supported tunables, and the location of the tunables file template.

### To manually format tunables files

- ◆ Format the tunable parameter as follows:

```
$TUN{"tunable_name"}{"system_name"|"*"}=value_of_tunable;
```

For the *system\_name*, use the name of the system, its IP address, or a wildcard symbol. The *value\_of\_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```
#  
# Tunable Parameter Values:  
#  
our %TUN;  
  
$TUN{"tunable1"}{"*"}=1024;  
$TUN{"tunable3"}{"sys123"}="SHA256";  
  
1;
```

## Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See [“Tunables value parameter definitions”](#) on page 146.

Each line for the parameter value starts with \$TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{"dmp_daemon_count"}{"node123"}=16;
```

In this example, you are changing the dmp\_daemon\_count value from its default of 10 to 16. You can use the wildcard symbol "\*" for all systems. For example:

```
$TUN{"dmp_daemon_count"}{"*"}=16;
```

## Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Veritas Storage Foundation and High Availability Solutions Tuning Guide* for detailed information on product tunable ranges and recommendations .

[Table B-1](#) describes the supported tunable parameters that can be specified in a tunables file.

**Table B-1** Supported tunable parameters

Tunable	Description
dmp_cache_open	(Veritas Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_daemon_count	(Veritas Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_delayq_interval	(Veritas Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

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

Tunable	Description
dmp_fast_recovery	(Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_health_time	(Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_log_level	(Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_low_impact_probe	(Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_lun_retry_timeout	(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_fabric	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_ownership	(Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_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.

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

Tunable	Description
dmp_path_age	(Veritas Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_pathswitch_blks_shift	(Veritas Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_idle_lun	(Veritas Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_threshold	(Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_cycles	(Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_interval	(Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_policy	(Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_state	(Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
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.

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

Tunable	Description
dmp_scsi_timeout	(Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_sfg_threshold	(Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_stat_interval	(Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
max_diskq	(Veritas File System) Specifies the maximum disk queue generated by a single file. The installer sets only the system default value of max_diskq. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_ahead	(Veritas File System) The 0 value disables read ahead functionality, the 1 value (default) retains traditional sequential read ahead behavior, and the 2 value enables enhanced read ahead for all reads. The installer sets only the system default value of read_ahead. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_nstream	(Veritas File System) The number of parallel read requests of size read_pref_io that can be outstanding at one time. The installer sets only the system default value of read_nstream. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
read_pref_io	(Veritas File System) The preferred read request size. The installer sets only the system default value of read_pref_io. Refer to the tunefstab(4) manual page for setting this tunable for a specified block device.
vol_checkpoint_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.

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

Tunable	Description
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 tunable requires system reboot to take effect.
vol_max_nmpool_sz	(Veritas Volume Manager) Maximum name pool size (bytes).
vol_max_rdback_sz	(Veritas Volume Manager) Storage Record readback pool maximum (bytes).
vol_max_wrspool_sz	(Veritas Volume Manager) Maximum memory used in clustered version of VERITAS Volume Replicator (bytes).
vol_maxio	(Veritas Volume Manager) Maximum size of logical VxVM I/O operations (sectors). This tunable requires system reboot to take effect.
vol_maxioctl	(Veritas Volume Manager) Maximum size of data passed into the VxVM ioctl calls (bytes). This tunable requires system reboot to take effect.
vol_maxparallelio	(Veritas Volume Manager) Number of I/O operations vxconfigd can request at one time. This tunable requires system reboot to take effect.
vol_maxspecialio	(Veritas Volume Manager) Maximum size of a VxVM I/O operation issued by an ioctl call (sectors). This tunable requires system reboot to take effect.
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).

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

Tunable	Description
vol_rvio_maxpool_sz	(Veritas Volume Manager) Maximum memory requested by VERITAS Volume Replicator (bytes).
vol_stats_enable	(Veritas Volume Manager) Enable VxVM I/O stat collection.
vol_subdisk_num	(Veritas Volume Manager) Maximum number of subdisks attached to a single VxVM plex. This tunable requires system reboot to take effect.
voldrl_max_drtregs	(Veritas Volume Manager) Maximum number of dirty VxVM regions that can exist on a non-sequential DRL. This tunable requires system reboot to take effect.
voldrl_max_seq_dirty	(Veritas Volume Manager) Maximum number of dirty regions in sequential mode. This tunable requires system reboot to take effect.
voldrl_min_regionsz	(Veritas Volume Manager) Minimum size of a VxVM Dirty Region Logging (DRL) region (sectors). This tunable requires system reboot to take effect.
voldrl_volumemax_drtregs	(Veritas Volume Manager) Max per volume dirty regions in log-plex DRL.
voldrl_volumemax_drtregs_20	(Veritas Volume Manager) Max per volume dirty regions in DCO version 20.
voldrl_dirty_regions	(Veritas Volume Manager) Number of regions cached for DCO version 30.
voliomem_chunk_size	(Veritas Volume Manager) Size of VxVM memory allocation requests (bytes). This tunable requires system reboot to take effect.
voliomem_maxpool_sz	(Veritas Volume Manager) Maximum amount of memory used by VxVM (bytes). This tunable requires system reboot to take effect.
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.

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

Tunable	Description
voliot_iobuf_limit	(Veritas Volume Manager) Maximum total size of all VxVM I/O trace buffers (bytes). This tunable requires system reboot to take effect.
voliot_iobuf_max	(Veritas Volume Manager) Maximum size of a VxVM I/O trace buffer (bytes). This tunable requires system reboot to take effect.
voliot_max_open	(Veritas Volume Manager) Maximum number of VxVM trace channels available for vxtrace commands. This tunable requires system reboot to take effect.
volpagemod_max_memsz	(Veritas Volume Manager) Maximum paging module memory used by Instant Snapshots (Kbytes).
volraid_rsrtransmax	(Veritas Volume Manager) Maximum number of VxVM RAID-5 transient reconstruct operations in parallel. This tunable requires system reboot to take effect.
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.



# 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](#)
- [Manually configuring and passwordless ssh](#)
- [Restarting the ssh session](#)
- [Enabling rsh for Linux](#)

## 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`.

---

**Note:** When installing on an RHEL5 / OEL5 system with SELinux enabled, only ssh is supported due to RedHat's SELinux policy restrictions.

---

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (system1) that contains the installation directories, and a target system (system2). This procedure also applies to multiple target systems.

---

**Note:** The script- and Web-based installers support establishing passwordless communication for you.

---

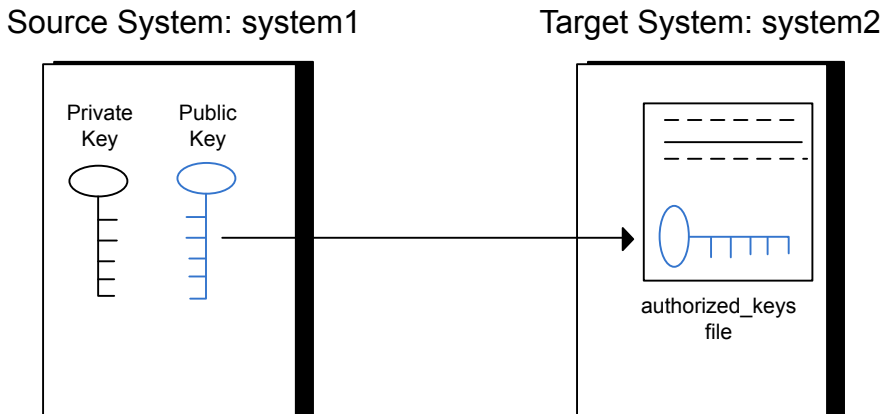
## Manually configuring and passwordless ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the `authorized_keys` file on the target systems.

Figure C-1 illustrates this procedure.

**Figure C-1** Creating the DSA key pair and appending it to target systems



Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: <http://openssh.org> to access online manuals and other resources.

### To create the DSA key pair

- 1 On the source system (system1), log in as root, and navigate to the root directory.

```
system1 # cd /root
```

- 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 (/root/.ssh/id_dsa):
```

- 3 Press Enter to accept the default location of `/root/.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 Output similar to the following lines appears.

```
Your identification has been saved in /root/.ssh/id_dsa.  
Your public key has been saved in /root/.ssh/id_dsa.pub.  
The key fingerprint is:  
1f:00:e0:c2:9b:4e:29:b4:0b:6e:08:f8:50:de:48:d2 root@system1
```

**To append the public key from the source system to the `authorized_keys` file on the target system, using secure file transfer**

- 1 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)?
```

- 2 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:
```

- 3 Enter the root password of system2.
- 4 At the `sftp` prompt, type the following command:

```
sftp> put /root/.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /root/.ssh/id_dsa.pub to /root/id_dsa.pub
```

- 5 To quit the SFTP session, type the following command:

```
sftp> quit
```

- 6 Add the `id_dsa.pub` keys to the `authorized_keys` file on the target system. 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:
```

Type the following commands on system2:

```
system2 # cat /root/id_dsa.pub >> /root/.ssh/authorized_keys
system2 # rm /root/id_dsa.pub
```

- 7 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 /root/.ssh/id_dsa.pub >> /root/.ssh/authorized_keys
```

- 8 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: /root/.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 rsh for Linux

The following section describes how to enable remote shell.

Veritas recommends configuring a secure shell environment for Veritas product installations.

See [“Manually configuring and passwordless ssh”](#) on page 154.

See the operating system documentation for more information on configuring remote shell.

### To enable rsh

- 1 To ensure that the `rsh` and `rsh-server` RPMs are installed, type the following command:

```
# rpm -qa | grep -i rsh
```

If it is not already in the file, type the following command to append the line `"rsh"` to the `/etc/securetty` file:

```
# echo "rsh" >> /etc/securetty
```

- 2 Modify the line `disable = no` in the `/etc/xinetd.d/rsh` file.

- 3 In the `/etc/pam.d/rsh` file, change the "auth" type from "required" to "sufficient":

```
auth    sufficient
```

- 4 Add the "promiscuous" flag into `/etc/pam.d/rsh` and `/etc/pam.d/rlogin` after item "pam\_rhosts\_auth.so".
- 5 To enable the rsh server, type the following command:

```
# chkconfig rsh on
```

- 6 Modify the `.rhosts` file. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system. This file also contains the name of a user having access to the local system. For example, if the root user must remotely access `system1` from `system2`, add an entry for `system2.companyname.com` to the `.rhosts` file on `system1` by typing the following command:

```
# echo "system2.companyname.com" >> $HOME/.rhosts
```

- 7 Install the Veritas product.

#### To disable rsh

- 1 Remove the "rsh" entry in the `/etc/securetty` file.
- 2 Disable the rsh server by typing the following command:

```
# chkconfig rsh off
```

- 3 After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

```
# rm -f $HOME/.rhosts
```





# Storage Foundation components

This appendix includes the following topics:

- [Storage Foundation installation RPMs](#)
- [Veritas Storage Foundation obsolete and reorganized installation RPMs](#)

## Storage Foundation installation RPMs

[Table D-1](#) shows the RPM name and contents for each English language RPM for Storage Foundation. The table also gives you guidelines for which RPMs to install based whether you want the minimum, recommended, or advanced configuration.

When you install all Storage Foundation and Veritas Cluster Server (VCS) RPMs, the combined functionality is called Storage Foundation and High Availability.

**Table D-1** Storage Foundation RPMs

RPMs	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 5.14.2 for Veritas	Minimum

**Table D-1** Storage Foundation RPMs (*continued*)

RPMs	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
VRTSob	Veritas Enterprise Administrator	Recommended
VRTSodm	Veritas ODM Driver for VxFS  Veritas Extension for Oracle Disk Manager is a custom storage interface designed specifically for Oracle9i and 10g. Oracle Disk Manager allows Oracle 9i and 10g to improve performance and manage system bandwidth.	Recommended

**Table D-1** Storage Foundation RPMs (*continued*)

RPMs	Contents	Configuration
VRTSsfpci601	<p>Veritas Storage Foundation Common Product Installer</p> <p>The Storage Foundation Common Product installer RPM contains the installer libraries and product scripts that perform the following:</p> <ul style="list-style-type: none"> <li>■ installation</li> <li>■ configuration</li> <li>■ upgrade</li> <li>■ uninstallation</li> <li>■ adding nodes</li> <li>■ removing nodes</li> <li>■ etc.</li> </ul> <p>You can use these script to simplify the native operating system installations, configurations, and upgrades.</p>	Minimum
VRTSsfmh	<p>Veritas Storage Foundation Managed Host</p> <p>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:</p>	Recommended
VRTSspt	Veritas Software Support Tools	Recommended
VRTSvcsdr	Contains the binaries for Veritas Cluster Server disk reservation.	Recommended
VRTSfssdk	<p>Veritas File System Software Developer Kit</p> <p>For VxFS APIs, the RPM contains the public Software Developer Kit (headers, libraries, and sample code). It is required if some user programs use VxFS APIs.</p>	All

**Table D-1** Storage Foundation RPMs (*continued*)

RPMs	Contents	Configuration
VRTSsvmconv	Symantec Logical Volume Manager (LVM) volume converter  Converts offline Linux LVM managed volumes to VxVM volumes by rearranging media contents.	All

## Veritas Storage Foundation obsolete and reorganized installation RPMs

[Table D-2](#) lists the RPMs that are obsolete or reorganized for Storage Foundation.

**Table D-2** Veritas Storage Foundation obsolete and reorganized RPMs

RPM	Description
Obsolete and reorganized for 6.0.1	
VRTSat	Obsolete
VRTSatClient	Obsolete
VRTSatServer	Obsolete
Obsolete and reorganized for 5.1	
Infrastructure	
SYMClma	Obsolete
VRTSaa	Included in VRTSsfmh
VRTSccg	Included in VRTSsfmh
VRTSdbms3	Obsolete
VRTSicsco	Obsolete
VRTSjre	Obsolete
VRTSjre15	Obsolete
VRTSmh	Included in VRTSsfmh
VRTSobc33	Obsolete

**Table D-2** Veritas Storage Foundation obsolete and reorganized RPMs  
*(continued)*

RPM	Description
VRTSobweb	Obsolete
VRTSobgui	Obsolete
VRTSpbx	Obsolete
VRTSsfm	Obsolete
VRTSweb	Obsolete
Product RPMs	
VRTSacclib	<p>Obsolete</p> <p>The following information is for installations, upgrades, and uninstalls using the script- or Web-based installer.</p> <ul style="list-style-type: none"> <li>■ For fresh installations VRTSacclib is not installed.</li> <li>■ For upgrades, VRTSacclib is not uninstalled.</li> <li>■ For uninstalls, VRTSacclib is not uninstalled.</li> </ul>
VRTSalloc	Obsolete
VRTScmccc	Obsolete
VRTScmcm	Obsolete
VRTScmcs	Obsolete
VRTScscm	Obsolete
VRTScscw	Obsolete
VRTScsocw	Obsolete
VRTScssim	Obsolete
VRTScutil	Obsolete
VRTSd2gui-common	Included in VRTSdbed
VRTSdb2ed-common	Included in VRTSdbed
VRTSdbcom-common	Included in VRTSdbed

**Table D-2** Veritas Storage Foundation obsolete and reorganized RPMs  
(continued)

RPM	Description
VRTSdbed-common	Included in VRTSdbed
VRTSdcli	Obsolete
VRTSddlpr	Obsolete
VRTSdsa	Obsolete
VRTSfsman	Included in the product's main RPM.
VRTSfsmnd	Included in the product's main RPM.
VRTSfspro	Included in VRTSsfmh
VRTSmapro-common	Included in VRTSsfmh
VRTSodm-common	Included in VRTSodm
VRTSodm-platform	Included in VRTSodm
VRTSorgui-common	Obsolete
VRTSvcscdb	Included in VRTSvcsea
VRTSvcsmn	Included in VRTSvcsc
VRTSvcscor	Included in VRTSvcsea
VRTSvcsvr	Included in VRTSvcsc
VRTSvdid	Obsolete
VRTSvmman	Included in the product's main RPM.
VRTSvmpro	Included in VRTSsfmh
VRTSvrpro	Included in VRTSob
VRTSvrw	Obsolete
VRTSvxfs-common	Included in VRTSvxfs
VRTSvxfs-platform	Included in VRTSvxfs
VRTSvxmsa	Obsolete
VRTSvxvm-common	Included in VRTSvxvm

**Table D-2** Veritas Storage Foundation obsolete and reorganized RPMs  
*(continued)*

<b>RPM</b>	<b>Description</b>
VRTSvxvm-platform	Included in VRTSvxvm
Documentation	All Documentation RPMs obsolete





# Troubleshooting installation issues

This appendix includes the following topics:

- [Restarting the installer after a failed connection](#)
- [What to do if you see a licensing reminder](#)
- [About the VRTSspt RPM troubleshooting tools](#)
- [Incorrect permissions for root on remote system](#)
- [Inaccessible system](#)
- [Troubleshooting the webinstaller](#)

## Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

## What to do if you see a licensing reminder

In this release, you can install without a license key. In order to comply with the End User License Agreement, you must either install a license key or make the host managed by a Management Server. If you do not comply with these terms within 60 days, the following warning messages result:

```
WARNING V-365-1-1 This host is not entitled to run Veritas Storage
Foundation/Veritas Cluster Server.As set forth in the End User
License Agreement (EULA) you must complete one of the two options
set forth below. To comply with this condition of the EULA and
stop logging of this message, you have <nn> days to either:
- make this host managed by a Management Server (see
  http://go.symantec.com/sfhakeyless for details and free download),
  or
- add a valid license key matching the functionality in use on this host
  using the command 'vxlicinst'
```

To comply with the terms of the EULA, and remove these messages, you must do one of the following within 60 days:

- Install a valid license key corresponding to the functionality in use on the host. See “[Installing Veritas product license keys](#)” on page 32. After you install the license key, you must validate the license key using the following command:

```
# /opt/VRTS/bin/vxlicrep
```

- Continue with keyless licensing by managing the server or cluster with a management server. For more information about keyless licensing, see the following URL: <http://go.symantec.com/sfhakeyless>

## About the VRTSspt RPM troubleshooting tools

The VRTSspt RPM provides a group of tools for troubleshooting a system and collecting information on its configuration. If you install and use the VRTSspt RPM, it will be easier for Symantec Support to diagnose any issues you may have.

The tools can gather Veritas File System and Veritas Volume Manager metadata information and establish various benchmarks to measure file system and volume manager performance. Although the tools are not required for the operation of any Veritas product, Symantec recommends installing them should a support case be needed to be opened with Symantec Support. Use caution when you use the VRTSspt RPM, and always use it in concert with Symantec Support.

## Incorrect permissions for root on remote system

The permissions are inappropriate. Make sure you have remote root access permission on each system to which you are installing.

```
Failed to setup rsh communication on 10.198.89.241:
'rsh 10.198.89.241 <command>' failed
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied
```

```
Failed to login to remote system(s) 10.198.89.241.
Please make sure the password(s) are correct and superuser(root)
can login to the remote system(s) with the password(s).
If you want to setup rsh on remote system(s), please make sure
rsh with command argument ('rsh <host> <command>') is not
denied by remote system(s).
```

```
Either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication
```

```
Would you like the installer to setup ssh/rsh communication
automatically between the nodes?
Superuser passwords for the systems will be asked. [y,n,q] (y) n
```

```
System verification did not complete successfully
```

```
The following errors were discovered on the systems:
```

```
The ssh permission denied on 10.198.89.241
rsh exited 1 on 10.198.89.241
either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication
```

**Suggested solution:** You need to set up the systems to allow remote access using ssh or rsh.

See [“About configuring secure shell or remote shell communication modes before installing products”](#) on page 153.

---

**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 Linux system names separated by spaces: q,? (host1)
```

Suggested solution: Verify that you entered the system name correctly; use the `ping(1M)` command to verify the accessibility of the host.

## Troubleshooting the webinstaller

This section provides possible solutions to problems that may occur when using the `webinstaller` script:

- Issue: The `webinstaller` script may report an error.

You may receive a similar error message when using the webinstaller:

```
Error: could not get hostname and IP address
```

Solution: Check whether `/etc/hosts` and `/etc/resolv.conf` file are correctly configured.

- Issue: The hostname is not a fully qualified domain name.

You must have a fully qualified domain name for the hostname in `https://<hostname>:<port>/`.

Solution: Check whether the `domain` section is defined in `/etc/resolv.conf` file.

- Issue: FireFox 3 may report an error.

You may receive a similar error message when using FireFox 3:

```
Certificate contains the same serial number as another certificate.
```

Solution: Visit FireFox knowledge base website:

<http://support.mozilla.com/en-US/kb/Certificate+contains+the+same+serial+number+as+another+certificate>

# Compatibility issues when installing Storage Foundation with other products

This appendix includes the following topics:

- [Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present](#)

## Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

## Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host RPMs 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 VRTSspb and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSspb, VRTSicsco, and VRTSat.

# Index

## B

backup boot disk group 102  
rejoining 102

## C

configuring  
rsh 36  
ssh 36

## D

disk groups  
rootdg 70

## I

Installing  
SF with the Web-based installer 48  
installing  
yum 62

## L

licensing 22  
add-on 21  
CDS 22  
full 21

## M

mounting  
software disc 37

## P

planning to upgrade VVR 84  
preinstallation 84

## R

rejoining  
backup boot disk group 102  
removing  
the Replicated Data Set 123

Replicated Data Set  
removing the 123  
root disk group 70  
rsh  
configuration 36

## S

ssh  
configuration 36

## T

tunables file  
about setting parameters 141  
parameter definitions 146  
preparing 145  
setting for configuration 142  
setting for installation 142  
setting for upgrade 142  
setting parameters 145  
setting with no other operations 143  
setting with un-integrated response file 144

## U

unsuccessful upgrade 102  
upgrading VVR  
from 4.1 85  
planning 84

## V

Veritas Operations Manager 16  
vradmin  
delpri 124  
stoprep 124  
VVR 4.1  
planning an upgrade from 85  
vxplex  
used to remove mirrors of root disk volumes 121

## **W**

Web-based installer 48

## **Y**

yum  
installing 62