Veritas Storage Foundation™ Installation Guide

HP-UX

5.0.1

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 5.0.1

Document Version 5.0.1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/business/support/assistance_care.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:

https://licensing.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Documentation feedback

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:

clustering_docs@symantec.com

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

About Storage Foundation and High-Availability Solutions

This chapter includes the following topics:

Veritas Storage Foundation product suites

The following table lists the Symantec products and optionally licensed features available with each Veritas Storage Foundation product suite.

Table 1-1 Contents of Veritas Storage Foundation products

Storage Foundation version	Products and features
Storage Foundation Standard	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Extension for Oracle Disk Manager option Optionally licensed features: Veritas Volume Replicator

Table 1-1 Contents of Veritas Storage Foundation products *(continued)*

Storage Foundation version	Products and features
Storage Foundation Standard HA	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Extension for Oracle Disk Manager option Veritas Cluster Server Optionally licensed features: Veritas Volume Replicator
Storage Foundation Enterprise	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Storage Checkpoint option Veritas Extension for Oracle Disk Manager option Optionally licensed features: Veritas Volume Replicator
Storage Foundation Enterprise HA	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Storage Checkpoint option Veritas Extension for Oracle Disk Manager option Veritas Cluster Server Optionally licensed features: Veritas Volume Replicator
Storage Foundation for Oracle Standard	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Extension for Oracle Disk Manager option Optionally licensed features: Veritas Volume Replicator

Table 1-1 Contents of Veritas Storage Foundation products *(continued)*

Storage Foundation version	Products and features
Storage Foundation for Oracle Enterprise	Veritas File System Veritas Volume Manager Veritas Quick I/O option Veritas Extension for Oracle Disk Manager option Veritas Storage Checkpoint option Veritas Storage Mapping option Veritas Database Flashsnap Optionally licensed features: Veritas Volume Replicator
Storage Foundation for Oracle Enterprise HA	Veritas File System Veritas Volume Manager Veritas Cluster Server Veritas Quick I/O option Veritas Extension for Oracle Disk Manager option Veritas Storage Checkpoint option Veritas Storage Mapping option Veritas Database Flashsnap Optionally licensed features: Veritas Volume Replicator

About Veritas Enterprise Administrator (VEA)

The Veritas Enterprise Administrator (VEA) is the graphical administrative interface for configuring shared storage devices. VEA simplifies administrative tasks, such as mounting and unmounting file systems, creating and removing storage checkpoints, enabling and disabling change log, and many others. For basic information on running the VEA, refer to *Veritas Enterprise Administrator User's Guide*. For a complete list of administrative tasks and their instructions, see the online help that is available from within the VEA.

Chapter 2

Before you install

This chapter includes the following topics:

About planning for a Storage Foundation installation

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 Storage Foundation will be installed.

Follow the preinstallation instructions if you are installing one of the Veritas Storage Foundation products by Symantec.

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

- Veritas Storage Foundation (Standard and Enterprise Editions)
- Veritas Storage Foundation High Availability (HA) (Standard and Enterprise Editions)

Several component products are bundled with each of these Storage Foundation products.

See "Veritas Storage Foundation product suites" on page 13.

Veritas Installation Assessment Service

The Veritas Installation Assessment Service (VIAS) utility assists you in getting ready for a Veritas Storage Foundation and High Availability Solutions installation or upgrade. The VIAS utility allows the preinstallation evaluation of a configuration, to validate it prior to starting an installation or upgrade.

https://vias.symantec.com/

Release notes

Read the *Release Notes* for all products included with this product.

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

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

Symantec product licensing

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. A single key lets you install the product on the number and type of systems for which you purchased the license. A key may enable the operation of more products than are specified on the certificate; however, you are legally limited to the number of product licenses purchased.

The product installation procedure describes how to activate the key. If you encounter problems while licensing this product, visit the Symantec licensing support website.

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

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

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

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.

Additional variables may be needed to use a Veritas Storage Foundation product after installation.

If you install the Veritas manual pages, set the path of your `MANPATH` environment variable to include the relevant directories.

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

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

```
$ PATH=$PATH:/usr/sbin:/opt/VRTSvxfs/sbin:/opt/VRTSob/bin:\
/opt/VRTSvcs/bin:/opt/VRTS/bin
$ MANPATH=/usr/share/man:/opt/VRTS/man:$MANPATH
$ export PATH MANPATH
```

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

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

Creating the /opt directory

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

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

Ensure that the `/opt` directory exists and has write permissions for `root`.

Cluster environment requirements

If your configuration has a cluster, which is a set of hosts that share a set of disks, there are additional requirements.

To set up a cluster environment

1. If you plan to place the root disk group under VxVM control, decide into which disk group you want to configure it for each node in the cluster. The root disk group, usually aliased as `bootdg`, contains the volumes that are used to boot the system. VxVM sets `bootdg` to the appropriate disk group if it takes control of the root disk. Otherwise `bootdg` is set to `nodg`. To check the name of the disk group, enter the command:

   ```
   # vxdg bootdg
   ```

2. Decide on the layout of shared disk groups. There may be one or more shared disk groups. Determine how many you wish to use.
3. If you plan to use Dirty Region Logging (DRL) with VxVM in a cluster, leave a small amount of space on the disk for these logs. The log size is proportional to the volume size and the number of nodes. Refer to the *Veritas Volume Manager Administrator's Guide* and the *Veritas Storage Foundation Cross-Platform Data Sharing Administrator's Guide* for more information on DRL.
4. Install the license that supports the clustering feature on every node in the cluster.

Configuring secure shell (ssh) or remote shell before installing products

Establishing communication between nodes is required to install Veritas software from a remote system, or to install and configure a cluster. The node from which the installation utility is run must have permissions to run `remsh` (remote shell) or `ssh` (secure shell) utilities. These utilities must run as `root` on all cluster nodes or remote systems.

You can install products to remote systems using either secure shell (ssh) or remote shell (remsh).Using ssh is the default, and is recommended, to configure a secure shell environment before you install any Veritas product.

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.

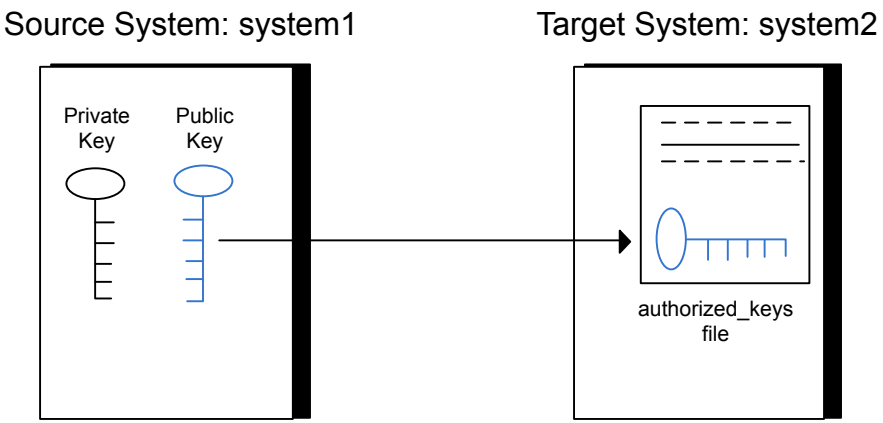
Configuring and enabling ssh

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 2-1 illustrates this procedure.

Figure 2-1 Creating the DSA key pair and appending it to target systems



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

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

To create the DSA key pair

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

   ```
   system1 # cd /
   ```

2. To generate a DSA key pair on the source system, type the following command:

   ```
   system1 # ssh-keygen -t dsa
   ```

   System output similar to the following is displayed:

   ```
   Generating public/private dsa key pair.
   Enter file in which to save the key (//.ssh/id_dsa):
   ```

3. Press Enter to accept the default location of `/.ssh/id_dsa`.
4. When the program asks you to enter the passphrase, press the Enter key twice.

   ```
   Enter passphrase (empty for no passphrase):
   ```

   Do not enter a passphrase. Press Enter.

   ```
   Enter same passphrase again:
   ```

   Press Enter again.

5. Make sure the `/.ssh` directory is on all the target installation systems (system2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

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

   Change the permissions of this directory, to secure it.

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

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

1 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (system2 in this example).

To enable SFTP, the `/opt/ssh/etc/sshd_config` file must contain the following two lines:

```
PermitRootLogin           yes
  Subsystem          sftp    /opt/ssh/libexec/sftp-server
```

2 If the lines are not there, add them and restart ssh:

```
system1 # /sbin/init.d/secsh start
```

3 From the source system (system1), move the public key to a temporary file on the target system (system2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
system1 # sftp system2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to system2 ...
The authenticity of host 'system2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

4 Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'system2,10.182.00.00'
(DSA) to the list of known hosts.
root@system2 password:
```

5 Enter the root password of system2.

6 At the `sftp` prompt, type the following command:

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

The following output is displayed:

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

7 To quit the SFTP session, type the following command:

```
sftp> quit
```

8 To begin the `ssh` session on the target system (system2 in this example), type the following command on system1:

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

9 After you log in to system2, enter the following command to append the `id_dsa.pub` file to the authorization key file:

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

10 After the `id_dsa.pub` public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, type the following command on system2:

```
system2 # rm /id_dsa.pub
```

11 To log out of the `ssh` session, type the following command:

```
system2 # exit
```

12 When you install from a source system that is also an installation target, also add the local system `id_dsa.pub` key to the local `authorized_keys` file. The installation can fail if the installation source system is not authenticated.

To add the local system `id_dsa.pub` key to the local `authorized_keys` file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

13 Run the following commands on the source installation system. If your ssh session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available for the user `root`:

```
system1 # exec /usr/bin/ssh-agent $SHELL
system1 # ssh-add

  Identity added: //.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

1 On the source system (system1), type 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.

Enabling remsh

Remote shell functionality is enabled automatically after installing an HP-UX system.

Typically, the only requirement to enable remote installations is to modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. You must modify this file for each user who remotely accesses the system using `remsh`. Each line of the `.rhosts` file must contain a fully qualified domain name or IP address for each remote system that has 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`.

```
# echo "system2.companyname.com" >> $HOME/.rhosts
```

After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

```
# rm -f $HOME/.rhosts
```

See the operating system documentation and the `remsh`(1M) manual page for more information on configuring remote shell.

Preinstallation or upgrade planning for Veritas Volume Replicator

Before installing or upgrading 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.

The following related documents are available:

Veritas Volume Replicator Planning and Tuning Guide	Provides detailed explanation of VVR tunables
Veritas Volume Replicator Administrator's Guide	Describes how to change tunable values

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

VEA installation planning

The Veritas Enterprise Administrator (VEA) GUI consists of several depots. Follow these planning guidelines to install VEA for use with VVR.

- The VEA server packages must be installed on the hosts on which VVR is installed, not the client. If you install using the product installer, these depots are installed when you install Storage Foundation products.

  The VEA server packages include the following:

  - The Veritas Volume Replicator Management Services Provider depot, `VRTSvrpro`, must be installed on all hosts in the Replicated Data Set (RDS).
  - For `VRTSvrpro` to function, the Veritas Volume Manager Management Services Provider depot, `VRTSvmpro`, must be installed on each system.

- To use the functionality for receiving SNMP notifications and email notifications, the Veritas Action Agent depot, `VRTSaa` must be installed.

- The VEA client can be installed on a host on which VVR is installed, or a separate host that is used to administer the VVR hosts. To use the VEA client on a system, the `VRTSobgui` depot must be installed on that system.

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 nodes. We recommend that the Secondary hosts be upgraded before the Primary host in the RDS.

VVR supports replicating data between VVR 5.0.1 and VVR 4.1 or later.

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 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.

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.

Prerequisites for installing Veritas Volume Replicator

The following is a list of system prerequisites for installing VVR:

- To be able to use this release of the Veritas Volume Manager (VxVM) or Veritas Storage Foundation, you must upgrade the operating system to the latest version, that is, HP-UX 11i v3 0903 OEUR or later.
- After OS upgrade, the VxVM version 5.0 is available. Install VxVM from the product disc to overwrite the 5.0 version with version 5.0.1.
- After this release of Veritas Volume Manager (VxVM) or Veritas Storage Foundation is already installed on your system, you can start using VVR by installing the VVR license and configuring VVR.
  See "Configuring Veritas Volume Replicator" on page 76.

Database requirements

Table 2-1 identifies supported database and HP-UX combinations if you plan to use Veritas Storage Foundation for Oracle.

Table 2-1 Supported database and HP-UX combinations

Oracle Release	HP-UX 11iv3 0903 OEUR or later
9.2	Yes
10.1	Yes
10.2	Yes
11gr1	Yes

About centralized management

Storage Foundation Manager (SFM) is a free license add-on to Veritas Storage Foundation that provides centralized application, server and storage management capabilities across a heterogeneous infrastructure. SFM is not available on the Storage Foundation and High Availability Solutions release and must be obtained separately.

See "Downloading Storage Foundation Manager" on page 30.

If you plan to use Storage Foundation Manager, configure the Storage Foundation products to use centralized management. Several prerequisites are necessary before you configure the system as a Storage Foundation Manager managed host. You must install and configure Storage Foundation Manager and the Authentication Broker from the SFM server.

For information about configuring and using Storage Foundation Manager, see the *Storage Foundation Manager Installation Guide* and the *Storage Foundation Manager Administrator's Guide*.

Veritas File System requirements

Complete the tasks in this section before installing Veritas File System.

Before installing Veritas File System, perform the following tasks:

- Review the *Veritas Storage Foundation Release Notes*.
- Ensure that the `/opt` directory exists and has write permissions for `root`.
- The Veritas File System does not support OmniStorage. Do not install VxFS without first retrieving any files archived using OmniStorage.
- Install all the latest required HP-UX patches.
  See "Required HP-UX patches" on page 32.

Downloading the Storage Foundation and High Availability software

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

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

See "About installation scripts" on page 155.

To download the software

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

   The estimated space that is needed for download, gunzip, and tar extract is 5 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 33.

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 -b 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. You must download the Veritas 5.0 software and the Veritas 5.0.1 software into separate directories.

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

Downloading Storage Foundation Manager

SF Manager is a free license add-on to Veritas Storage Foundation. You can download SF Manager packages from the following URL:

http://www.go.symantec.com/vom

Chapter 3

System requirements

This chapter includes the following topics:

Hardware and software requirements

For information on hardware requirements, see the hardware compatibility list. The hardware compatibility list (HCL) is available at:

http://entsupport.symantec.com/docs/283161

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

Supported HP-UX operating systems

This release of Veritas products can only be installed on a system running the HP-UX 11i v3 0903 OEUR release or later on the PA-RISC or Itanium platforms.

To verify the operating system version

Use the `swlist` command as follows:

```
# swlist | grep HPUX11i
HPUX11i-DC-OE     B.11.31.0903   HP-UX Data Center Operating Environment
```

JFS must be installed on your system prior to installing any Veritas software.

To verify that JFS is installed

Use the `swlist` command as follows:

```
# swlist -l product JFS
JFS              B.11.31        Base VxFS File System 4.1 for HP-UX
```

Required HP-UX patches

The 5.0.1 releases of Veritas Storage Foundation and Veritas Storage Foundation for Oracle require the following HP-UX patches.

Table 3-1 lists the required HP-UX patches.

Table 3-1 Required HP-UX patches

HP-UX Patch ID	Description
PHSS_36311	This patch fixes a security vulnerability in HP-UX IA-64 platforms. The Veritas Enterprise Administrator Service Core and VRTSobc33 depots require this OS patch on IA-64 platform.
PHKL_40022	This patch distributes vxiod threads to processors other than the moncarch CPU.

Table 3-2 lists the recommended HP-UX patches.

Table 3-2 Recommended HP-UX patches

HP-UX Patch ID	Description
PHKL_39401	This patch fixes a Virtual-Memory defect. This patch should be installed for Veritas File System (VxFS) to respond to memory pressure situations.

Warning: Install all the latest required HP-UX patches before you install the Veritas products. You can use the `swlist` command to determine whether the correct update and patches are installed. The installation procedure terminates if the correct patches are not found.

HP may release patches that supersede the ones in this list. To verify that you have the latest HP-UX patches, go to the Symantec support website to view the relevant TechNote.

http://www.symantec.com/techsupp

Also, you can get the patches from Hewlett-Packard's Patch Database offered under the Maintenance and Support section of the HP Services & Support - IT Resource Center. HP's Patch Database provides fast, accurate searches for the latest recommended and superseded patches available for Veritas File System or Veritas Volume Manager.

Mandatory patch required for Oracle Bug 4130116

If you are running Oracle versions 9.2.0.6 or 9.2.0.7, you must apply the Oracle patch for Oracle Bug 4130116. Contact Oracle to obtain this patch, and for details on how to apply it.

Other required HP-UX software

If you plan to install Storage Foundation from an NFS mounted directory, you must install the software `ONCplus - HP-UX 11i v3 version B.11.31.07.01`. The `ONCplus B.11.31.06` software bundled with HP-UX 11i v3 March 2009 OEUR release reports issues with long path names. This causes the installation to fail as the installer can not copy files from the mounted directory to the systems on which you want to install Storage Foundation.

To download the software:

- Go to http://software.hp.com.
- Search for the software depot `ONCplus`.
- Download ONCplus for HP-UX 11i v3 version B.11.31.07.01.

Disk space requirements

Before installing any of the Veritas Storage Foundation products, confirm that your system has enough free disk space.

Use the "Perform a Preinstallation Check" (P) menu or the `-precheck` option of the product installer to determine whether there is sufficient space.

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

Disk space

Table 3-3 shows the approximate disk space used by the Storage Foundation products for all (both the required and optional) packages.

Table 3-3 Disk space requirements

Product Name	Minimum Space Required (Without Optional Packages)	Maximum Space Required (Including All Packages)
Storage Foundation Standard	698 MB	850 MB
Storage Foundation Enterprise	699 MB	851 MB
Storage Foundation Enterprise HA	1131 MB	1311 MB

Disk space requirements for Veritas Volume Replicator

Table 3-4 shows the approximate disk space used by VVR for the required and optional packages.

Table 3-4 Approximate disk space use for VVR

English	/root	/opt	/usr	/var
Required Packages	170 MB	60 MB	85 MB	0.5 MB
Optional Packages	240 MB	256 MB	85 MB	0.5 MB
All Packages	410 MB	316 MB	170 MB	1 MB

Chapter 4

Installing Storage Foundation and High Availability products

This chapter includes the following topics:

About installing Veritas Storage Foundation on HP-UX

This release of Veritas Storage Foundation requires the HP-UX 11i v3 0903 OEUR release. If you are not running this release of HP-UX, upgrade HP-UX on your system before you install the new Veritas software.

For an initial installation on a new system, you can use one of the installation procedures described in this section. If you have an existing installation of Storage Foundation that you are upgrading, you must perform an upgrade to move to the 5.0.1 versions of the Veritas products.

See "Upgrading Storage Foundation products or the operating system" on page 87.

Summary of Veritas Storage Foundation installation tasks

Installation of Veritas Storage Foundation products consists of the following tasks:

- Obtain a license key, if required.
- If the operating system is not at the required OS fusion level, upgrade the operating system to the latest release.
  See "Upgrading Storage Foundation products or the operating system" on page 87.
  The operating system is bundled with Veritas Volume Manager and Veritas File System. If the Veritas Volume Manager or Veritas File System is in use, follow the steps in the upgrade chapter to upgrade the Storage Foundation and the operating system.
  See "Upgrading Storage Foundation products or the operating system" on page 87.
- If patches for the operating system are required, install the patches before upgrading the product.
  See "Required HP-UX patches" on page 32.
- Mount the disk.
  See "Mounting a software disc" on page 36.
- Install the 5.0.1 Veritas Storage Foundation product.
  Start the installer and select 'I' for install, or run the appropriate installation script.
  See "Performing the installation" on page 37.
- Reboot the system.

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

- Configure the Veritas software.
  Start the installer and select 'C' for configure, or run the appropriate installation script with the `-configure` option.
  See "Configuring the products using the common product installer" on page 49.

Mounting a software disc

Veritas software is provided on a DVD format disc. If you have the media kit, then get the software disc from the media kit.

To mount the software disc

1. Place the Veritas software disc into a DVD drive connected to your system and log in as superuser.
2. Determine the block device file for the DVD drive:

   ```
   # ioscan -fnC disk
   ```

   Make a note of the device file as it applies to your system.
3. Create a directory in which to mount the software disc and mount the disc using the appropriate drive name. For example:

   ```
   # mkdir -p /mnt/dvdrom
   # /usr/sbin/mount -F cdfs /dev/dsk/c3t2d0 /mnt/dvdrom
   ```

4. Verify that the disc is mounted:

   ```
   # mount
   ```

5. Change to the appropriate directory and product subdirectory to view the product release notes and installation guides, or install the products.

Performing the installation

The Veritas product installer is the recommended method to license and install Storage Foundation. Select the procedure for the Storage Foundation product you are installing:

- Storage Foundation
- Storage Foundation for Oracle
- Storage Foundation HA
- Veritas Volume Replicator

About the common product installer

The product installer is the recommended method to license and install the Veritas products. The installer also enables you to configure the product, verify preinstallation requirements, and view the product's description.

If you obtained a standalone Veritas product from an electronic download site, the single product download files do not contain the general product installer. Use the product installation script to install the product.

See "About installation scripts" on page 155.

At most points during an installation, you can type `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. If an installation procedure hangs, use `Control-c` to stop and exit the program. After a short delay, the script exits. You can also enter `q` to quit the installer or `?` to display help information.

Default responses are in parentheses. Press Return to accept the defaults.

Additional options are available for the common product installer.

See "Installation script options" on page 156.

Installing Storage Foundation or Storage Foundation for Oracle using the common product installer

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

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

To install Storage Foundation

1. To install on multiple systems, set up the systems so that commands between systems execute without prompting for passwords or confirmations.

   See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

2. Load and mount the software disc.

   See "Mounting a software disc" on page 36.

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

4. From this directory, type the following command to install on the local system only. Also use this command to install on remote systems using the secure shell (ssh) utilities:

   ```
   # ./installer
   ```

   If you use the remote shell utilities to install on remote systems, additionally specify the `-rsh` option:

   ```
   # ./installer -rsh
   ```

   The sample installation assumes that ssh is used.

5 Enter I to install and press Return.

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

Veritas Storage Foundation for Oracle can also be installed using this procedure. Select the number corresponding to this product, if desired.

7 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 system names separated by spaces on which to
install SF:  host1

Do you want to continue with the system names? (y,n,q) y
```

8 Enter the product license information.

Each system requires a product license before installation. License keys for additional product features should also be added at this time.

```
Enter a SF license key for host1:
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X

XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X successfully registered on
host1
SF license registered on host1
```

9 You are prompted to enter additional license information, until all licenses for all systems have been entered. Then reply that you have no additional licenses to enter.

```
Do you want to enter another license key for host1?
[y,n,q] (n) n
```

10 You can choose to install required depots or all depots. Optional depots include man pages, for example.

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

For example, you should see output similar to the following:

```
SF can be installed without optional depots to conserve
disk space.

1) Install required Veritas Storage Foundation depots -
   1779 MB required
2) Install all Veritas Storage Foundation depots -
   1780 MB required

Select the depots to be installed on all systems?
[1-2,q,?] (2) 2
```

11 Reboot the system.

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

12 After rebooting, you must configure the system.

Start the installer and select 'C' for configure, or run the appropriate installation script with the `-configure` option.

the section called “Configuring the products using the common product installer”

Installing Storage Foundation High Availability or Storage Foundation for Oracle High Availability using the common product installer

The following sample procedure is based on the installation of a Storage Foundation Enterprise High Availability (SF/HA) clusterwith two nodes: "host1" and "host2.". Use the same procedure to install Storage Foundation for Oracle High Availability.

To install Storage Foundation and High Availability products

1. To install on multiple systems, set up the systems so that commands between systems execute without prompting for passwords or confirmations.

   See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

2. Load and mount the software disc.

   See "Mounting a software disc" on page 36.

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

4. From this directory, type the following command to install on the systems, if you use the ssh utilities:

   ```
   # ./installer
   ```

   If you use the remote shell utilities to install on remote systems, additionally specify the `-rsh` option:

   ```
   # ./installer -rsh
   ```

   The sample installation assumes that ssh is used.

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

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

   Veritas Storage Foundation for Oracle can also be installed using this procedure. Select the number corresponding to this product, if desired.

   With a Veritas Storage Foundation HA license, the high availability cluster components are also installed for this menu selection.

7. You are prompted to enter the system names (in the following example, "host1" and "host2") on which the software is to be installed. Enter the system name or names and then press Return.

   ```
   Enter the system names separated by spaces on which to
   install SF:  host1 host2

   Do you want to continue with the system names? (y,n,q) y
   ```

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

If the installer hangs or asks for a login password, stop the installer and set up ssh or rsh. Then run the installer again.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

9 Enter the product license information.

```
Enter a SF license key for
host1: [?] XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X successfully registered
   on host1
Do you want to enter another license key for host1?
   [y,n,q,?]  (n) n

Enter a SF license key for
host2:  [?] XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X successfully registered
   on host2
Do you want to enter another license key for host2? [y,n,q,?]
   (n) n
```

Enter `n` if you have no further license keys to add for a system. You are then prompted to enter the keys for the next system.

Each system requires a product license before installation. License keys for additional product features should also be added at this time.

10 You can choose to either install only required depots or all depots. Optional depots include man pages, for example.

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

For example, you should see output similar to the following:

```
SF can be installed without optional depots to conserve disk space.

 1) Required Veritas Storage Foundation depots - 929 MB required
 2) All Veritas Storage Foundation depots - 930 MB required

Select the depots to be installed on all systems? [1-2,q,?] (2) 2
```

The list of optional depots may differ depending on the license key that you entered.

11 Reboot the system.

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

12 After rebooting, you must configure the system.

Start the installer and select 'C' for configure, or run the appropriate installation script with the `-configure` option.

Installing Veritas Volume Replicator using the common product installer

The Veritas software disc provides a product installer, which is the recommended method to license and install Veritas Volume Replicator (VVR).

To install VVR using the product installer

1 To install on multiple systems, set up the systems so that commands between systems execute without prompting for passwords or confirmations.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

2 Load and mount the software disc.

See "Mounting a software disc" on page 36.

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

4 From this directory, type the following command to install on the systems, if you use the ssh utilities:

```
# ./installer
```

If you use the remote shell utilities to install on remote systems, additionally specify the `-rsh` option:

```
# ./installer -rsh
```

The sample installation assumes that ssh is used.

5 Enter `I` to install and press Return.

6 When the list of available products is displayed, select Veritas Volume Replicator, enter the corresponding number, and press Return.

7 You are prompted to enter the system names (in the following example, "host1" and "host2") on which the software is to be installed. Enter the system name or names and then press Return.

```
Enter the system names separated by spaces on which to
install VVR:  host1 host2

Do you want to continue with the system names? (y,n,q) y
```

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

If the installer hangs or asks for a login password, stop the installer and run it again after setting up ssh or rsh.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

9 Enter the product license information.

```
Enter a VVR license key for
   system01: [?] XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
   XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X successfully registered
   on system01
Do you want to enter another license key for system01?
   [y,n,q,?]  (n) n
Enter a VVR license key for
   system02:  [?] XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
   XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X successfully registered
   on system02
Do you want to enter another license key for system02? [y,n,q,?]
    (n) n
```

Enter `n` if you have no further license keys to add for a system. You are then prompted to enter the keys for the next system.

Each system requires a product license before installation. License keys for additional product features should also be added at this time.

10 If you have multiple Veritas products, we recommend using the option to install Storage Foundation Enterprise (which includes VVR) rather than installing each product individually. This option ensures that installation steps are done in the proper order and interdependencies are met.

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

For example, you should see output similar to the following:

```
Additional depots are typically installed to simplify
future upgrades.

   1)  Required Veritas Volume Replicator depots - 855 MB required
   2)  All Veritas Volume Replicator depots - 861 MB required
   3)  Storage Foundation Enterprise depots - 911 MB required

Select the depots to be installed on all systems? [1-3,q] (3) 3
```

The list of optional packages may differ depending on the license key that you entered.

11 Reboot the system.

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

12 After rebooting, you must configure the system.

Start the installer and select 'C' for configure, or run the appropriate installation script with the `-configure` option.

the section called “Configuring the products using the common product installer”

Installing VVR when VxVM is already installed

If this release of Veritas Volume Manager (VxVM) is already installed on your system, you can start using VVR by installing the VVR license.

After the VVR license is installed, install VVR-specific components and configure VVR.

If a previous version of Veritas Volume Manager (VxVM) is already installed on your system, you must upgrade to this release of VxVM. In some cases, this requires upgrading the operating system (OS) version to the latest version.

After VxVM is upgraded, install VVR-specific components and configure VVR.

To use the new features of VVR 5.0.1, upgrade the version of each disk group.

See "Upgrading VxVM disk group versions" on page 127.

Installing Veritas Enterprise Administrator

Veritas Enterprise Administrator (VEA) is required to access the graphical user interface (GUI) for Veritas Storage Foundation. You can use the GUI to administer disks, volumes, file systems, and database functionality on local or remote machines. This section describes the installation of VEA components.

The VEA server depot, `VRTSob`, is installed when you install Veritas Storage Foundation products using the installation script. The VEA server package must be installed on all nodes that are to be administered.

The VEA client depot contains the Graphical User Interface (GUI) program to administer Veritas Storage Foundation products. The VEA client may be installed on one or more of the nodes to be administered. The VEA client may also be installed on a separate system that can be used to administer Veritas Storage Foundation.

Installing the Veritas Enterprise Administrator client

Veritas Enterprise Administrator (VEA) is required to access the graphical user interface (GUI) for Veritas Storage Foundation. You can use the GUI to administer disks, volumes, file systems, and database functionality on local or remote machines.

The Veritas Enterprise Administrator (VEA) client can be installed and run on any HP-UX, Windows XP, Windows NT, Windows ME, Windows 2000, or Windows 98 machine that supports the Java Runtime Environment.

The VEA client requires one of the following depots:

- Veritas Enterprise Administrator client depot (`VRTSobgui`)
  This is the client package for UNIX.
- Veritas Enterprise Administrator for Windows (`windows\VRTSobgui.msi`)
  This is the client package for Windows.

Minimum system requirements for VEA clients

Table 4-1 shows the system minimum requirements for the GUI.

Table 4-1 VEA system minimum requirements

Operating System	System minimum requirements
HP-UX	Minimum of 512MB of memory

Table 4-1 VEA system minimum requirements *(continued)*

Operating System	System minimum requirements
Windows XP, NT, Me, 2000, 98, 2k3, Vista, 2k8	300MHz Pentium with at least 256MB of memory

Installing the Veritas Enterprise Administrator client on HP-UX

If you plan to run the VEA client, you must install the VEA client packages on the machine you are planning to use.

To install the VEA client on an HP-UX machine using swinstall

1. Log in as `root`.
2. Determine whether the VEA client package is already installed.

   ```
   # swlist | grep VRTSobgui
   ```

   This command will return `VRTSobgui` if `VRTSobgui` is already installed. It will return nothing if the package has not been installed.
3. To install the VEA client package for HP-UX, insert the appropriate media disc into your system's DVD-ROM drive and mount it.

   See "Mounting a software disc" on page 36.
4. Run the `swinstall` command.

   ```
   # swinstall -s /dvdrom/depot
   ```

5. Select the software bundles `VRTSobgui` for installation.

   The VEA client package for HP-UX is installed.

Installing the VEA client on Microsoft Windows

This package can be installed on Windows NT, Windows XP, Windows 2000, Windows 2003, Windows ME, Windows 98, Windows 95, Vista, and Windows 2k3 and 2k8 machines.

To install and run the VEA client, your system must conform to the following specifications:

- Windows Installer 2.0 or later must be present. For information about upgrading Windows Installer, visit: http://www.microsoft.com

For Windows NT 4.0, it is also recommended that you use Windows NT 4.0 Service Pack 6.

- 100MHz Pentium with 256MB memory or higher specification.
- 100MB available disk space.
- Microsoft Installer is required to install the `VRTSobgui.msi` package. You can get this product from the Microsoft website if it is not already installed on your system.

If you plan to install the GUI client on Windows NT 4.0, Windows Installer must be upgraded to version 2.0. For more information about upgrading Windows Installer, visit:

http://www.microsoft.com

If you are using Windows NT 4.0, it is also recommended that you use Windows NT 4.0 Service Pack 6.

To install the VEA client on a Windows machine

1. Insert the appropriate media disc into your system's DVD-ROM drive.
2. Using Windows Explorer or a DOS Command window, go to the `windows` directory and execute the `vrtsobgui.msi` program with Windows Installer.
3. Follow the instructions presented by the `vrtsobgui.msi` program.
4. After installation is complete, ensure environment changes made during installation take effect by performing one of the following procedures:
   - For Windows NT, Windows 2000, Windows 2003 or Windows XP, log out and then log back in.
   - For Windows ME, Windows 98 or Windows 95, restart the computer.

Chapter 5

Configuring Storage Foundation and High Availability products

This chapter includes the following topics:

Configuring the products using the common product installer

After installation, you must configure the product. To configure, run the Veritas product installer or the appropriate installation script using the `-configure` option.

To configure Storage Foundations and High Availability Solutions or cluster configurations, refer to that section.

See "Configuring Storage Foundation and High Availability Solutions" on page 53.

Configuring Storage Foundation

This section describes how to configure Storage Foundation with the common product installer.

To configure Storage Foundation

1. To configure Storage Foundation, enter the following command:

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

2. When the list of available products is displayed, select Veritas Storage Foundation (SF), enter the corresponding number, and press Return.

   ```
   Select a product to configure:
   ```

3. Enter the names of the systems on which you want to configure the software.

   ```
   Enter the system names separated by spaces on which to
   configure SF: host1
   ```

4. The procedure checks system licensing, and you can enter additional licenses, if needed.

   ```
   Checking system licensing

   SF license registered on host1

   Do you want to enter another license key for host1? [y,n,q] (n) n
   ```

5. The enclosure-based naming scheme (rather than disk device naming) is a feature of Veritas Volume Manager. You can reference disks using a symbolic name that is more meaningful than the operating system's normal device access name.

   See the *Veritas Volume Manager Administrator's Guide*.

   ```
   Do you want to set up the enclosure-based naming
   scheme? [y,n,q,?] (n) n
   ```

6 You have the option of specifying the default name of a disk group. If you specify a name, it is used for Veritas Volume Manager commands when a disk group is not specified.

Enter **n** if you do not want to specify the name of the default disk group at this time. You can set the name of the default disk group after installation.

See "Setting the default disk group" on page 128.

If you specify the name of a default disk group, this step does not create the disk group. After installation, you can use the `vxdiskadm` command to create the disk group.

```
Do you want to set up a default disk group for each
system? [y,n,q,?] (y) y
```

7 If you responded `y`, then enter the information for the default disk group name.

```
Will you specify one disk group name for all eligible
systems? [y,n,q,?] (y) y

Specify a default disk group name for all systems. [?] dg001
```

8 You are prompted to confirm the default disk group.

Note: If `nodg` is displayed, then the host will be configured to have no default disk group.

```
Is this correct? [y,n,q] (y) y
```

9 If a valid license for VVR is installed, the installer prompts you for the VVR configuration. If a license for VVR is not present, skip to step 14.

The script displays the default ports for VVR. Follow the instructions on the screen if you want to change the VVR ports.

The port settings should be identical for the systems that are part of the same Replicated Data Set. They should also be identical for all the systems in a cluster.

```
Do you want to change any of the VVR ports on system01?
[y,n,q] (n) n
```

10 The VVR Statistics Collection Tool collects and maintains the statistics which are helpful in solving VVR performance issues.

Options can be set, such as the frequency for gathering the statistics, and the number of days for which the collected statistics should be preserved.

Change the frequency of online statistics collection, if needed.

```
The frequency of online stats collection on system01
is set to per 10 seconds.
Do you want to change the frequency
of online stats collection on system01 ? [y,n,q] (n) n
```

11 Change the maximum number of days that online statistics are retained, if needed.

```
The maximum number of days for which VVR statistics
can be retained is set to 3 on system01

Do you want to change the maximum number of days
for retaining VVR statistics on system01? [y,n,q] (n) n
```

12 The VVR Statistics Collection Tool collects and maintains the statistics which are helpful in solving VVR performance issues.

Options can be set, such as the frequency for gathering the statistics, and the number of days for which the collected statistics should be preserved.

Change the frequency of online statistics collection, if needed.

```
The frequency of online stats collection on system01
is set to per 10 seconds.
Do you want to change the frequency
of online stats collection on system01 ? [y,n,q] (n) n
```

13 Repeat steps 9 to 12 for all other systems.

14 Verify the fully qualified hostname of the systems.

```
Is the fully qualified hostname of system
 "host1" = "host1.domain_name"? [y,n,q] (y) y
```

15 The Veritas Storage Foundation software is verified and configured.

Start the Veritas Storage Foundation processes.

```
Do you want to start Veritas Storage Foundation processes
now? [y,n,q] (y) y
```

16 The configuration completes automatically.

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

```
Configuration log files, summary file, and response file are saved at:

        /opt/VRTS/install/logs/installer-****
```

17 After the configuration completes, restart the Storage Agent

```
# /opt/VRTSobc/pal33/bin/vxpalctrl -a StorageAgent -c restart
```

Configuring Storage Foundation and High Availability Solutions

After installation, you must configure the product. To do this, run the Veritas product installer or the appropriate installation script using the `-configure` option.

Use the following procedures to configure Storage Foundation High Availability and clusters using the common product installer. Use the same procedures to configure Storage Foundation for Oracle High Availability.

Required information for configuring Storage Foundation and High Availability Solutions

To configure Storage Foundation High Availability or Storage Foundation for Oracle High Availability, the following information is required:

- A unique Cluster name
- A unique Cluster ID number between 0-65535
- Two or more NIC cards per system used for heartbeat links
  One or more heartbeat links are configured as private links One heartbeat link may be configured as a low priority link

Veritas Storage Foundation can be configured to use Symantec Security Services.

Running Storage Foundation in Secure Mode guarantees that all inter-system communication is encrypted and that users are verified with security credentials. When running Storage Foundation in Secure Mode, NIS and system usernames and passwords are used to verify identity. Storage Foundation usernames and passwords are no longer used when a cluster is running in Secure Mode.

Before configuring a cluster to operate using Symantec Security Services, another system must already have Symantec Security Services installed and be operating as a Root Broker.

The following information is required to configure SMTP notification:

- The domain-based hostname of the SMTP server
- The email address of each SMTP recipient
- A minimum severity level of messages to be sent to each recipient

The following information is required to configure SNMP notification:

- System names of SNMP consoles to receive VCS trap messages
- SNMP trap daemon port numbers for each console
- A minimum severity level of messages to be sent to each console

Configuring Veritas Storage Foundation and High Availability Solutions

After installation, you must configure the product.

Use the procedure in this section if you installed an HA version of the Storage Foundation software.

To configure Storage Foundation product on a cluster

1. To invoke the common installer, run the `installer` command with the `configure` option, as shown in this example:

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

2. When the list of available products is displayed, select Veritas Storage Foundation (SF) or Veritas Storage Foundation for Oracle (SFORA). Enter the corresponding number, and press Return.

   ```
   Select a product to configure:
   ```

3. You are prompted to enter the system names (in the following example, "host1" and "host2") on which the software is to be installed. Enter the system name or names and then press Return.

   ```
   Enter the system names separated by spaces on which to
   configure SF: host1 host2
   ```

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

The installer requires that ssh commands used between systems execute without prompting for passwords or confirmations. If the installer hangs or asks for a login password, stop the installer and run it again with the ssh configured for password free logins, or configure rsh and use the -rsh option.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

5 The procedure checks system licensing, and you can enter additional licenses, if needed.

```
Checking system licensing

SF license registered on host1

Do you want to enter another license key for host1? [y,n,q] (n) n
```

6 Enter the unique cluster name and Cluster ID number.

```
Enter the unique cluster name: [?]cluster2
Enter the unique Cluster ID number between 0-65535: [b,?] 76
```

7 The installer discovers the network interfaces (NICs) available on the first system and reports them:

```
  Discovering NICs on host1 ... discovered lan0 lan1 lan2 lan3 lan4 lan
```

8 Enter private heartbeat NIC information for each host.

```
Enter the NIC for the first private heartbeat
link on host1: [b,?] lan2
Would you like to configure a second private heartbeat
link? [y,n,q,b,?] (y) y
Enter the NIC for the second private heartbeat
link on host1: [b,?] lan3

Would you like to configure a third private heartbeat
link? [y,n,q,b,?] (n) n
Do you want to configure an additional low priority
heartbeat link? [y,n,q,b,?] (n) n
Are you using the same NICs for private heartbeat links
on all systems? [y,n,q,b,?] (y) y
```

Warning: When answering `y`, make sure that the same NICs are available on each system; the installer may not verify this. The NICs should also be the same speed on both systems for the heartbeat links to function properly.

Notice that in this example, `lan0` is not selected for use as a private heartbeat NIC because it already in use as the public network interface.

9 A summary of the information you entered is given. When prompted, confirm that the information is correct.

```
Is this information correct? [y,n,q]
```

If the information is correct, enter `y`. If the information is not correct, enter `n`. The installer prompts you to enter the information again.

10 When prompted to configure the product to use Veritas Security Services, enter `n`, unless a Root Broker has already been set up.

Warning: Before configuring a cluster to operate using Veritas Security Services, another system must already have Veritas Security Services installed and be operating as a Root Broker. Refer to the *Veritas Cluster Server Installation Guide* for more information on configuring a secure cluster.

```
Would you like to configure SF to use
Symantec Security Services? [y,n,q] (n) n
```

11 To add users, you will need the user name, password, and user privileges (Administrator, Operator, or Guest).

When prompted, set the user name and /or password for the Administrator.

Enter `n` if you want to decline. If you enter `y`, you are prompted to change the password.

```
Do you want to set the username and/or password for the Admin user
(default username = 'admin', password='password')?
  [y,n,q] (n) n
```

12 When prompted to configure SMTP notification, enter `n` or `y` to configure. To configure SNMP notification, enter the following information. You can then confirm that it is correct, or enter it again.

```
Do you want to configure SMTP notification? [y,n,q] (y) y
Active NIC devices discovered on host1: lan0
Enter the NIC for the SF Notifier to use on host1: [b,?] (lan0) lan0
Is lan0 to be the public NIC used by all systems [y,n,q,b,?] (y) y

Enter the domain-based hostname of the SMTP server
(example: smtp.yourcompany.com): [b,?] smtp.mycompany.com
Enter the full email address of the SMTP recipient
(example: user@yourcompany.com): [b,?] user@mycompany.com
Enter the minimum severity of events for which mail should be sent
to user@163.com  [I=Information, W=Warning, E=Error,
S=SevereError]: [b,?] E
```

13 When prompted to configure SNMP notification, enter `n` or `y` to configure. To configure SNMP notification enter the following information. You can then confirm that it is correct, or enter it again.

```
Do you want to configure SNMP notification? [y,n,q] (y)
Active NIC devices discovered on host1: lan0
Enter the NIC for the SF Notifier to use on host1: [b,?] (lan0) lan0
Is lan0 to be the public NIC used by all systems [y,n,q,b,?] (y) y

Enter the SNMP trap daemon port: [b,?] (162) 162
Enter the SNMP console system name: [b,?] host1
Enter the minimum severity of events for which SNMP traps should
be sent to host1  [I=Information, W=Warning, E=Error,
S=SevereError]: [b,?] E
Would you like to add another SNMP console? [y,n,q,b] (n) n
```

14 If you installed a valid HA/DR license, the installer prompts you to configure this cluster as a global cluster.

If you installed a HA/DR license to set up replicated data cluster or campus cluster, skip this installer option.

See *Veritas Cluster Server User's Guide* for instructions to set up VCS global clusters.

```
Do you want to configure the Global Cluster Option? [y,n,q] (y) y
```

15 If you select yes, the installer prompts you for a NIC and value for the netmask.

```
Enter the Virtual IP address for Global Cluster Option:
[b,?] (10.10.12.1)
```

16 Verify and confirm the configuration of the global cluster.

```
Global Cluster Option configuration verification:
NIC: eth0
IP: 10.10.12.1
Netmask: 255.255.240.0
Matching Cluster Management Console Virtual IP configuration
Is this information correct? [y,n,q] (y)
```

17 The enclosure-based naming scheme (rather than disk device naming) is a feature of Veritas Volume Manager. You can reference disks using a symbolic name that is more meaningful than the operating system's normal device access name.

See the *Veritas Volume Manager Administrator's Guide*

```
Do you want to set up the enclosure-based naming scheme?
   [y,n,q,?] (n) n
```

18 You are now given the option of specifying the default name of a disk group that is to be assumed by Veritas Volume Manager commands if a disk group is not otherwise specified.

Enter **n** if you do not want to specify the name of the default disk group at this time. You can set the name of the default disk group after installation.

See "Setting the default disk group" on page 128.

If you specify the name of a default disk group, this step does not create the disk group. After installation, you can use the `vxdiskadm` command to create the disk group.

```
Do you want to set up a default disk group for each system?
  [y,n,q,?] (y) y
```

19 If you responded `y`, then enter the information for the default disk group name.

```
Will you specify one disk group name for all eligible
systems? [y,n,q,?] (y) y

Specify a default disk group name for all systems. [?] dg001
```

20 Validate the default disk group information, and press Return.

21 You may be prompted to verify the fully qualified hostname of the systems. Press Return to continue.

22 The Veritas Storage Foundation or Veritas Storage Foundation for Oracle software is verified and configured.

Start the Veritas Storage Foundation processes.

```
Do you want to start Veritas Storage Foundation processes
now? [y,n,q] (y) y
```

23 The configuration and startup complete automatically.

View the log file, if needed, to confirm the configuration.

```
Configuration log files, summary file, and response file are saved at:

        /opt/VRTS/install/logs/installer-****
```

24 After the configuration completes, restart the Storage Agent

```
# /opt/VRTSobc/pal33/bin/vxpalctrl -a StorageAgent -c restart
```

About adding and removing nodes in a cluster

After you install Storage Foundation High Availability and create a cluster, you can add and remove nodes from the cluster. You can create a cluster of up to 32 nodes.

For information about adding and removing nodes, see the *Veritas Cluster Server Installation Guide*.

Configuring Storage Foundation for Databases

This section describes the procedure to configure Storage Foundation for Databases, using the common product installer.

You can use this procedure to configure Veritas Storage Foundation for Oracle (SFORA).

The example in this section shows a simple configuration on a single host. If you are installing Storage Foundation High Availability product or installing on multiple hosts, there are additional configuration prompts.

See "Configuring Storage Foundation and High Availability Solutions" on page 53.

Some databases may require additional configuration steps. See the following sections for details.

See "Creating and configuring the repository database for Oracle" on page 63.

To configure Storage Foundation for Oracle

1. To invoke the common installer, run the `installer` command with the `configure` option, as shown in this example:

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

2. When the list of available products is displayed, select the number correspnding to the product you want to configure, and press Return.

   You can use this procedure to configure Veritas Storage Foundation for Oracle (SFORA).

   ```
   Select a product to configure:
   ```

3. 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 system names separated by spaces on which to
   configure SF: host1
   ```

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

The installer requires that ssh commands used between systems execute without prompting for passwords or confirmations. If the installer hangs or asks for a login password, stop the installer and run it again with the ssh configured for password free logins, or configure rsh and use the -rsh option.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

5 The procedure checks system licensing, and you can enter additional licenses, if needed.

```
Checking system licensing

SF license registered on host1

Do you want to enter another license key for host1? [y,n,q] (n) n
```

6 If you are configuring Veritas Storage Foundation for Oracle, you are now prompted to configure permissions to allow database administrators (DBAs) access to the tools to support the Veritas Storage Foundation product. The default settings only allow access to the root user.

Respond **y** to change permission for a DBA or a group of DBAs to access the support tools. When prompted, enter the login account or group name.

For example, enter the following for a Veritas Storage Foundation for Oracle configuration:

```
Do you want to add single user access on host1? [y,n,q,?] (y) y
Enter login account name for DBA user: oracle
Do you want to add group access on host1? [y,n,q,?] (y) y
Enter group name for DBA users: oinstall
Are you using the same DBA user/group for all systems? [y,n,q,?] (y) y
```

7 The enclosure-based naming scheme (rather than disk device naming) is a feature of Veritas Volume Manager. You can reference disks using a symbolic name that is more meaningful than the operating system's normal device access name.

See the *Veritas Volume Manager Administrator's Guide*

```
Do you want to set up the enclosure-based naming scheme?
   [y,n,q,?] (n) n
```

8 You are now given the option of specifying the default name of a disk group that is to be assumed by Veritas Volume Manager commands if a disk group is not otherwise specified.

Enter **n** if you do not want to specify the name of the default disk group at this time. You can set the name of the default disk group after installation.

See "Setting the default disk group" on page 128.

If you specify the name of a default disk group, this step does not create the disk group. After installation, you can use the `vxdiskadm` command to create the disk group.

```
Do you want to set up a default disk group for each system?
  [y,n,q,?] (y) y
```

9 If you responded `y`, then enter the information for the default disk group name.

```
Will you specify one disk group name for all eligible
systems? [y,n,q,?] (y) y

Specify a default disk group name for all systems. [?] dg001
```

10 Validate the default disk group information, and press Return.

11 You may be prompted to verify the fully qualified hostname of the systems. Press Return to continue.

12 The Veritas Storage Foundation for databases software is verified and configured.

You are prompted to start the Veritas Storage Foundation product processes.

For example, when you configure Veritas Storage Foundation for Oracle, the following prompt displays:

```
Do you want to start Veritas Storage Foundation for Oracle processes
now? [y,n,q] (y) y
```

13 The configuration and startup complete automatically.

View the log file, if needed, to confirm the configuration.

```
Configuration log files, summary file, and response file are saved at:

        /opt/VRTS/install/logs/installer-****
```

14 After the configuration completes, restart the Storage Agent

```
# /opt/VRTSobc/pal33/bin/vxpalctrl -a StorageAgent -c restart
```

15 The installation script prompts for a reboot if there are one or more errors. Reboot the system (or systems) if the install script prompts you to do so.

16 If you installed Veritas Storage Foundation for Oracle, create a new repository database.

See "Creating and configuring the repository database for Oracle" on page 63.

Database configuration requirements

Most relational database management system (RDBMS) software requires operating system parameters to be set prior to operation. The Oracle database requires modifications to kernel settings before the databases will run correctly. The most critical settings are normally located in the Shared Memory and Semaphore settings on HP-UX. For precise settings, consult your current database installation and configuration documentation.

Creating and configuring the repository database for Oracle

After installing Veritas Storage Foundation for Oracle, and configuration of VCS is complete, you can create and configure the repository database using the `sfua_db_config` script.

The script detects whether your system is running in a stand-alone or HA configuration and then automatically configures the repository database.

Before running the script, review the following requirements for a stand-alone configuration:

- You must have a mount point mounted on a VxVM volume with a VxFS file system. The mount point is used to store the repository database.

Before running the script, review the following requirements for an HA configuration:

- Create a separate, non-shared disk group on shared storage. Create a VxVM volume and a VxFS file system and mount the volume.
- It is recommended that you have a separate disk group for the repository volume so that any failovers are independent of other service groups.
- The mount point is used to store the repository database.
- Obtain an unique virtual IP address for public NIC interface.

- Obtain the device names for the public NIC interface for all systems in the cluster.
  For example, use these names.
  lan0
- Obtain a subnet mask for the public NIC interface.
- Make sure VCS is not in read-write (-rw) mode. To make sure VCS is in read-only mode, use the following command:

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

Table 5-1 indicates the options available for the `sfua_db_config` script.

Table 5-1 sfua_db_config options

Option	Description
-ssh	Use this option in a high availability (HA) configuration. The option indicates that ssh and scp are to be used for communication between systems. Either ssh or rsh should be preconfigured so that you can execute the commands without being prompted for passwords or confirmations.
-o dropdb	Drops the repository database.
-o unconfig_cluster	Use this option in a high availability (HA) configuration. Unconfigures the repository database from the VCS cluster.
-o dbstatus	Verifies the status of the database and database server.
-o stopserver	Stops the database server.
-o startserver	Starts the database server.
-o serverstatus	Reports the database server status.
-o stopdb	Detaches the repository database from the database server.
-o startdb	Attaches the repository database to the database server.

To create and configure the repository database

1 Run the `sfua_db_config` script as follows:

```
# /opt/VRTSdbcom/bin/sfua_db_config
```

2 Confirm that you are ready to configure the Veritas Storage Foundation for Oracle repository:

```
Are you ready to configure SFORA repository (y/n/q) [y]?
```

3 The mount point is displayed.

```
filesystem mount point for SFORA repository: /sfua_rep
```

4 The network interfaces (NICs) are discovered, and you are prompted to enter the NIC for the repository configuration on each host:

```
Enter the NIC for system host1 for HA Repository configuration:

[lan0]

Enter the NIC for system host2 for HA Repository  configuration:

[lan0]
```

5 Enter the Virtual IP address for repository failover.

```
Enter the Virtual IP address for repository failover: 10.209.87.240

Enter the netmask for public NIC interface: [255.255.252.0]

Following information will be used for SFORA HA configuration:

        Public IP address:              10.209.87.240
        Subnet mask:                    255.255.252.0
        Public interface:               host1 -> lan0,host2 -> lan0
        Mount point:                    /sfua_rep
        Volume Name for mount point:    repvol
        Diskgroup for mount point:      repdg

Is this correct (y/n/q) [y]?
```

6 The mount point information is displayed, and the script asks for confirmation. Then the repository information is added.

7 Verify that the repository was configured.

If you are installing in a high availability configuration, enter the following command:

```
# /opt/VRTS/bin/hagrp -state
Group        Attribute             System     Value
Sfua_Base    State                 guan       |ONLINE|
Sfua_Base    State                 plover     |OFFLINE|

Note: Sfua_Base group should be online on one node in the
cluster.
```

8 If you are installing in a stand-alone configuration, enter the following command to verify that the repository was configured:

```
# /opt/VRTSdbcom/bin/sfua_db_config -o dbstatus
Database 'dbed_db' is alive and well on server
'VERITAS_DBMS3_host'.
```

Setting administrative permissions for databases

To allow database administrators to administer a database using Veritas Storage Foundation, you are required to change some permission settings. During the installation process, you have the opportunity to configure the product. Answering "y" allows you to provide database administrators access to various functionality. If you did not make the permission changes during installation, you can do so at a later time.

The default settings at installation time for the `/opt/VRTSdbed` directory allow only the `root` login to access the directory.

To allow the user "oracle" access to the /opt/VRTSdbed directory

Use the `chown` and `chmod` commands, as follows:

```
# chown oracle /opt/VRTSdbed
# chmod 500 /opt/VRTSdbed
```

To allow users in the group "dba" access to the /opt/VRTSdbed directory

Use the `chgrp` and `chmod` commands, as follows:

```
# chgrp dba /opt/VRTSdbed
# chmod 550 /opt/VRTSdbed
```

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 Volume Manager Administrator's Guide*.

Configuring Veritas Volume Manager with the installvm script

If you deferred configuring VxVM during installation, you can configure it by running the `installvm` script with the `-configure` option.

To configure VxVM using the installvm script

1. Enter the following commands.

```
# cd /dvdrom/volume_manager
# ./installvm -configure
```

2. The script runs an initial system check, and will tell you that you cannot configure already configured features such as enclosure-based naming and default disk groups.
3. Decide whether you want to set up the enclosure-based naming scheme:

```
Do you want to set up the enclosure-based naming scheme? [y, n, q]
```

4. You are then asked if you want to set up a default disk group for each system:

```
Do you want to set up a default disk group for each system? [y, n, q]
```

5. If you have a VVR license installed, the next phase concerns configuration of VVR:

```
Do you want to change any of the VVR ports ... [y, n, q]
```

6. You are now asked questions regarding the frequency of VVR statistics collection.
7. The next phase of the configuration procedure consists of setting up a centrally managed host:

```
Enable Centralized Management? [y,n,q]
```

8 If you selected centralized management, you will be asked a series of questions relating to hostnames.

After configuration is complete, the following message displays:

```
Startup completed successfully on all systems
```

9 After the installation and configuration of VxVM is complete, you can use the `vxdiskadm` command and the VEA GUI to create disk groups, and to populate these with disks.

See the *Veritas Volume Manager Administrator's Guide* and the VEA online help for details.

Converting to a VxVM root disk

It is possible to select VxVM as a choice for your root disk when performing a new installation using Ignite-UX. Alternatively, you can use the following procedure to achieve VxVM rootability by cloning your LVM root disk using the `vxcp_lvmroot` command.

To convert to a VxVM root disk

1 Select the disk to be used as your new VxVM root disk. It is recommended that this disk is internal to the main computer cabinet. If this is currently an LVM disk, then it must be removed from LVM control as follows:

- Use the `lvremove` command to remove any LVM volumes that are using the disk.
- Use the `vgreduce` command to remove the disk from any LVM volume groups to which it belongs.
- Use the `pvremove` command to erase the LVM disk headers

If the disk to be removed is the last disk in the volume group, use the `vgremove` command to remove the volume group, and then use `pvremove` to erase the LVM disk headers.

If the disk is not currently in use by any volume or volume group, but has been initialized by `pvcreate`, you must still use the `pvremove` command to remove LVM disk headers.

If you want to mirror the root disk across multiple disks, make sure that all the disks are free from LVM control.

2 While booted on the newly upgraded LVM root disk, invoke the `vxcp_lvmroot` command to clone the LVM root disk to the disk(s) you have designated to be the new VxVM root disks. In the following example, `c1t0d0` is used for the target VxVM root disk:

```
# /etc/vx/bin/vxcp_lvmroot -v c1t0d0
```

To additionally create a mirror of the root disk on `c2t0d0`:

```
# /etc/vx/bin/vxcp_lvmroot -v -m c2t0d0 c1t0d0
```

Use of the `-v` (verbose) option is highly recommended. The cloning of the root disk is a lengthy operation, and this option gives a time-stamped progress indication as each volume is copied, and other major events.

3 Use the `setboot` (1M) command to save the hardware path of the new VxVM root disk in the system NVRAM. The disk hardware paths can be found using this command:

```
# ioscan -kfnC disk
```

4 Reboot from the new VxVM root disk. If you created a mirrored root disk, then there is nothing more to do. The LVM root disk safely co-exists with your VxVM root disk, and provides a backup boot target.

5 If desired, you can convert the original LVM root disk into a mirror of your VxVM root disk by using the following commands:

```
# /etc/vx/bin/vxdestroy_lvmroot -v c2t0d0
# /etc/vx/bin/vxrootmir -v c2t0d0
```

Once this operation is complete, the system is running on a completely mirrored VxVM root disk.

6 If later required, you can use the `vxres_lvmroot` command to restore the LVM root disk.

Starting and enabling the configuration daemon

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

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

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

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

```
# vxdctl mode
```

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

```
mode: enabled
```

This message indicates that `vxconfigd` is not running:

```
mode: not-running
```

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

```
# vxconfigd
```

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

```
mode: disabled
```

To enable the volume daemon, enter the following command:

```
# vxdctl enable
```

Once started, `vxconfigd` automatically becomes a background process.

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

Starting the volume I/O daemon

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

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

```
# vxiod
```

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

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

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

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

```
# vxiod set 16
```

where 16 is the desired number of vxiod daemons. It is recommended that at least one vxiod daemon should be run for each CPU in the system.

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

Enabling the Intelligent Storage Provisioning (ISP) feature

If you load the allocator provider package (VRTSalloc), enter the following commands to restart the VEA service and enable the Intelligent Storage Provisioning (ISP) feature:

```
# /opt/VRTS/bin/vxsvcctrl restart
```

Enabling cluster support in VxVM (Optional)

This release includes an optional cluster feature that enables VxVM to be used in a cluster environment. The cluster functionality in VxVM allows multiple hosts to simultaneously access and manage a set of disks under VxVM control. A cluster is a set of hosts sharing a set of disks; each host is referred to as a node in the cluster.

The VxVM cluster feature requires a license, which can be obtained from your Customer Support channel.

To enable the cluster functionality in VxVM

1. Obtain a license for the VxVM cluster feature.
2. Install the software packages onto each system (node) to be included in the cluster.
3. Initialize VxVM.

   See "Configuring Veritas Volume Manager with the installvm script" on page 67.

4 Start VEA.

5 Configure shared disks.

See the *Veritas Volume Manager Administrator's Guide*.

Configuring shared disks

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

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

Make sure that the shared disks are not being accessed from another node while you are performing the configuration. If you start the cluster on the node where you perform the configuration only, you can prevent disk accesses from other nodes because the quorum control reserves the disks for the single node.

Configuring new disks

If you are installing and setting up VxVM for the first time, you must configure the shared disks.

To configure shared disks

1 Start the cluster on at least one node.

2 On one node, run the `vxdiskadm` program and choose option 1 to initialize new disks. When asked to add these disks to a disk group, choose `none` to leave the disks for future use.

3 On other nodes in the cluster, run `vxdctl enable` to see the newly initialized disks.

4 From the master node, create disk groups on the shared disks. To determine if a node is a master or slave, run `vxdctl -c mode`.

Use the `vxdg` program or VEA to create disk groups. In the `vxdg` program, use the `-s` option to create shared disk groups.

5 From the master node only, use `vxassist` or VEA to create volumes in the disk groups.

The volumes must be of type `gen`. Do not create RAID-5 volumes. Before creating any log subdisks, read the section on DRL in the *Veritas Volume Manager Adminstrator's Guide*.

6 If the cluster is only running with one node, bring up the other cluster nodes. Enter the `vxdg list` command on each node to display the shared disk groups.

Verifying existing shared disks

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

To verify that your shared disk groups exist

1 Start the cluster on all nodes.

2 Enter the following command on all nodes:

```
# vxdg -s list
```

This displays the existing shared disk groups.

Converting existing VxVM disk groups to shared disk groups

Use this procedure if you are upgrading from VxVM 3.x to VxVM 5.0.1 (or Storage Foundation 3.x to a Storage Foundation product at the 5.0.1 level) and you want to convert existing disk groups to shared disk groups.

To convert existing disk groups to shared disk groups

1 Ensure that all systems that are running are part of the same cluster.

2 Start the cluster on at least one node.

For a two-node cluster, start the cluster on one node; for a four-node cluster, start the cluster on three nodes.

3 Configure the disk groups using the following procedure.

To list all disk groups, use the following command:

```
# vxdg list
```

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

```
# vxdg deport disk_group_name
```

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

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

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

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

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

```
# vxdg list
```

The disk groups are now ready to be shared.

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

Upgrading in a clustered environment with FastResync set

Upgrading in a clustered environment with FastResync set requires additional steps.

This procedure applies to the following upgrade scenarios:

- Upgrading from VxVM 3.5 to VxVM 5.0.1
- Upgrading from VxVM 3.5 Maintenance Pack 4 to VxVM 5.0.1

If there are volumes in the shared disk groups with FastResync set (`fastresync=on`), before beginning the upgrade procedure, reattach each snapshot to its data volume, using this procedure:

To upgrade in a clustered environment when FastResync is set

1. You should run this procedure from the master node; to find out if you are on the master node, enter the command:

   ```
   # vxdctl -c mode
   ```

2. On the master node, list which disk groups are shared by entering:

   ```
   # vxdg -s list
   ```

3. Using the diskgroup names displayed by the previous command, list the disk groups that have volumes on which FastResync is set:

   ```
   # vxprint -g diskgroup -F "%name" -e "v_fastresync"
   ```

4. Reattach each snapshot:

   ```
   # vxassist -g diskgroup -o nofmr snapback snapshot_volume
   ```

5. If you are upgrading from VxVM 3.5 Maintenance Patch 3 or from VxVM 3.2 Maintenance Patch 5, set FastResync to off for each volume:

   ```
   # vxvol -g diskgroup set fastresync=off volume
   ```

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*.

vxtunefs command permissions and Cached Quick I/O

By default, you must have superuser (`root`) privileges to use the `/opt/VRTS/bin/vxtunefs` command. The `vxtunefs` command is a tool that lets

you change caching policies to enable Cached Quick I/O and change other file system options. Database administrators can be granted permission to change default file system behavior in order to enable and disable Cached Quick I/O. The system administrator must change the `vxtunefs` executable permissions as follows:

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

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

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

Configuring Veritas Volume Replicator

This section describes configuring Veritas Volume Replicator using the Veritas product installer. If you configured Veritas Volume Replicator during the installation process, you do not need to perform the procedure in this section.

To configure VVR, run the Veritas product installer or the appropriate installation script using the `-configure` option.

To configure VVR

1. To invoke the common installer, run the `installer` command with the `configure` option, as shown in this example:

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

2. When the list of available products is displayed, select Veritas Volume Replicator (VVR), enter the corresponding number, and press Return.

   ```
   Select a product to configure:
   ```

3. At the prompt, enter the name of the system or systems on which you want to configure VVR.

   ```
   Enter the system names separated by spaces on which to configure
   VVR: system01 system02
   ```

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

The installer requires that ssh commands used between systems execute without prompting for passwords or confirmations. If the installer hangs or asks for a login password, stop the installer and run it again after setting it up. Set up the system with ssh configured for password free logins, or configure remote shell and use the -rsh option.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

5 The script continues the initial system check. The script confirms success by displaying information, such as the OS version, communication with the remote hosts, and whether the required VVR packages are installed. Press Return to continue.

6 The script proceeds to verify whether the required licenses are installed. If a valid license for VVR is not present, the script prompts you to enter a license. The script validates whether the current license enables VVR.

See "Symantec product licensing" on page 18.

You cannot proceed until a valid VVR license has been entered. If a valid VVR license is present on the system, the script provides the option to add additional licenses. Press Return to continue.

7 The script enables you to choose whether you want to use enclosure-based naming. The enclosure-based naming scheme (rather than disk device naming) is a feature of Veritas Volume Manager. You can reference disks using a symbolic name that is more meaningful than the operating system's normal device access name.

If you enter `y` to the enclosure-based naming question, the script decides whether the system is eligible for enclosure-based naming. If it is eligible, confirm whether you want to set up enclosure-based naming.

See the *Veritas Volume Manager Administrator's Guide*

```
Do you want to set up the enclosure-based naming scheme?
[y,n,q,?] (n)
```

8 Specify the default name of a disk group for Veritas Volume Manager commands, if a disk group is not otherwise specified.

Enter **n** if you do not want to specify the name of the default disk group at this time. 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 `vxdctl (1M)` manual page and the *Veritas Volume Manager Administrator's Guide* for more information.

If you specify the name of a default disk group, this step does not create the disk group. After installation, you can use the `vxdiskadm` command to create the disk group.

```
Do you want to set up a default disk group for each system?
  [y,n,q,?] (y) y
```

9 If you responded `y`, then enter the information for the default disk group name.

```
Will you specify one disk group name for all eligible
systems? [y,n,q,?] (y) y

Specify a default disk group name for all systems. [?] dg001
```

10 Validate the default disk group information, and press Return.

11 The script displays the default ports for VVR. Follow the instructions on the screen if you want to change the VVR ports.

The port settings should be identical for the systems that are part of the same Replicated Data Set. They should also be identical for all the systems in a cluster.

```
Do you want to change any of the VVR ports on system01?
[y,n,q] (n) n
```

12 The VVR Statistics Collection Tool collects and maintains the statistics which are helpful in solving VVR performance issues.

Options can be set, such as the frequency for gathering the statistics, and the number of days for which the collected statistics should be preserved.

Change the frequency of online statistics collection, if needed.

```
The frequency of online stats collection on system01
is set to per 10 seconds.
Do you want to change the frequency
of online stats collection on system01 ? [y,n,q] (n) n
```

13 Change the maximum number of days that online statistics are retained, if needed.

```
The maximum number of days for which VVR statistics
can be retained is set to 3 on system01

Do you want to change the maximum number of days
for retaining VVR statistics on system01? [y,n,q] (n) n
```

14 Configure the VVR statistics options (tunables), if needed.

For more information about the VVR statistics options, refer to the *Veritas Volume Replicator Planning and Tuning Guide*.

```
Do you want to view or modify VVR tunables on
system01? [y,n,q,?] (n) n
```

15 Repeat steps 11 to 14 for all other systems.

16 Verify the fully qualified hostnames of the systems. Press Return to continue.

17 To start the VVR processes, press Return, or type `y`.

```
Do you want to start Veritas Volume Replicator
processes now? [y,n,q] (y) y
```

18 The configuration and startup completes automatically.

View the log file, if needed, to confirm the configuration.

```
Configuration log files, summary file, and response file are saved at:

        /opt/VRTS/install/logs/installer-****
```

19 After the configuration completes, restart the Storage Agent

```
# /opt/VRTSobc/pal33/bin/vxpalctrl -a StorageAgent -c restart
```

Configuring your system after the installation

Use the following procedure to configure your system after installation.

To configure your system after the software upgrade

1 Reinstate the mount points in the `/etc/fstab` file that you recorded in the preparation steps.

See "Preparing to upgrade the Veritas software" on page 91.

2 Reboot the upgraded systems.

3 Restart all the volumes by entering the following command for each disk group:

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

Optional configuration steps

Perform the following optional configuration steps:

- If you want to use features of Veritas Storage Foundation 5.0.1 or Veritas Storage Foundation 5.0.1 for Oracle 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.
- Stop the cluster, restore the VCS configuration files to the `/etc/VRTSvcs/conf/config` directory, and restart the cluster.
- To create root volumes that are under VxVM control after installation, use the `vxcp_lvmroot` command.
  See "Converting to a VxVM root disk" on page 68.
  See the *Veritas Volume Manager Administrator's Guide*.
- To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.

See "Upgrading VxFS disk layout versions" on page 125.
See "Upgrading VxVM disk group versions" on page 127.

4 After you complete the installation procedure, proceed to initializing (where required), setting up, and using Veritas Storage Foundation.

See "Configuring the products using the common product installer" on page 49.

Configuring and starting Veritas Enterprise Administrator

Before using the Veritas Enterprise Administrator server or client, start them both.

Optional configuration can also be completed at this time.

Stopping and starting the VEA server

After installing the VEA packages, the VEA server may need to be stopped and restarted. The VEA service is automatically started when you reboot your system.

To start up the VEA server

1 Check the state of the VEA server.

```
# /opt/VRTS/bin/vxsvcctrl status
```

2 Stop the VEA server.

```
# /opt/VRTS/bin/vxsvcctrl stop
```

You can also stop the VEA server manually by killing the `vxsvc` process.

3 Start the VEA server.

```
# /opt/VRTS/bin/vxsvcctrl start
```

The VEA server is automatically started on a reboot.

Starting the VEA client on Windows or HP-UX

Only users with appropriate privileges can run VEA. VEA can administer the local machine or a remote machine. However, VxVM and the VEA server must be installed on the machine to be administered. The VxVM `vxconfigd` daemon and the VEA server must be running on the machine to be administered.

After installing VxVM and VEA and starting the server, start the VEA client in one of the following ways.

HP-UX operating system

To administer the HP-UX machine, use the following command:

```
# /opt/VRTSob/bin/vea
```

Windows operating system

To administer a remote HP-UX machine from a Windows machine, select Start > Programs > Veritas > Veritas Enterprise Administrator.

Modifying optional connection access on HP-UX

To allow users other than root to access VEA, set up a group called vrtsadm in `/etc/group`, and add the users to this group. For example, adding the following entry:

vrtsadm::600:root,ed

will allow the two users, root and ed, to access VEA.

To specify a group other than vrtsadm, you should add the group to `/etc/group`, modify the Security key and restart the VEA server daemon, as in the following example.

To modify connection access

1. Add a new group:

   ```
   # groupadd -g gid veagrp
   ```

2. Edit `/etc/group` to add users to the group.
3. Modify the Security key in the registry:

   ```
   # /opt/VRTSob/bin/vxregctl /etc/vx/isis/Registry setvalue \
   Software/Veritas/VxSvc/Current/Version/Security AccessGroups \
   REG_SZ veagrp
   ```

4. Restart the VEA server.

   ```
   # /opt/VRTS/bin/vxsvcctrl restart
   ```

VMSA and VEA co-existence

If you do not plan to use VMSA to administer other (pre-VxVM 3.5) machines, then you should uninstall VMSA before installing VEA. You can later do a client-only install if you want to run the VMSA client on your machine.

Warning: The release of VEA that ships with VxVM 5.0 is not compatible with VMSA, the previous Veritas Volume Manager GUI. You cannot run VMSA with VxVM version 5.0.

If you do not remove VMSA, the following warning appears during a reboot:

```
Veritas VM Storage Administrator Server terminated.

Stopping Veritas VM Storage Administrator Server

### Terminated
```

Configuring Veritas Enterprise Administrator for Oracle

You may need to update Veritas Enterprise Administrator (VEA) so that users other than `root` can access features.

Adding users to the VEA Service Console Registry for Oracle

You may want to add users to the VEA service console registry to allow access to the interface to users other than `root`. You also have the option to give database administrators `root` privileges.

To add users other than root to the Veritas Enterprise Administrator Service console registry

1 Make sure that the optional GUI package was installed.

```
# swlist -l product | grep VRTSorgui
VRTSorgui    5.0.31.5.%20090323 Veritas Storage Foundation Graphical
User Interface for Oracle from Symantec
```

2 To give `root` privileges to the database administrator, use the `vxdbedusr` command as follows.

```
# /opt/VRTS/bin/vxdbedusr -a user [-A] [-f] -n user_name -h host_name
```

where:

`-a user` adds a user to the registry

`-A` grants the user root access

`-f` allows the user to be a user other than the `/opt/VRTSdbed` owner.

`-n` indicates the name of the user.

`-h` specifies the hostname.

For example, to add a database administrator with the name "oracle" as a user with `root` privileges on the host "host1", enter the following:

```
# /opt/VRTS/bin/vxdbedusr -a user -A -f -n oracle -h host1
```

3 To add a user without `root` privileges, use the `vxdbedusr` command as follows.

```
# /opt/VRTS/bin/vxdbedusr -a user -n user_name -h host_name
```

where `-a` adds a user to the registry.

For example, to add "oracle" as a user, enter the following:

```
# /opt/VRTS/bin/vxdbedusr -a user -n oracle -h host1
```

4 To add a group to the console registry, use the `vxdbedusr` command as follows:

```
# /opt/VRTS/bin/vxdbedusr -a group [-A] [-f] -n group_name -h hostname
```

where:

`-a user` adds a user group to the registry

`-A` grants the user group root access

`-f` allows the group access to the GUI.

`-h` specifies the hostname.

For example, to add "dba" as a group, enter the following:

```
# /opt/VRTS/bin/vxdbedusr -a group -A -f -n dba -h host1
```

Removing users from the VEA Service Console Registry for Oracle

You may need to restrict access to the VEA service console registry. You can remove users or user groups from the registry if they have been previously added.

You cannot remove `root` from the VEA console registry.

To remove users other than root from the Veritas Enterprise Administrator Service console registry

1 Make sure that the optional GUI package was installed.

```
# swlist -l product | grep VRTSorgui
VRTSorgui     5.0.31.5.%20090323 Veritas Storage Foundation Graphical User
Oracle from Symantec
```

2 Use the `vxdbedusr` command to remove a group or user.

```
# /opt/VRTS/bin/vxdbedusr -r {user | group} \
-n {user_name | group_name} -h host_name
```

where `-r` removes a user or user group from the registry.

For example, to remove the user "oracle," enter the following:

```
# /opt/VRTS/bin/vxdbedusr -r user -n oracle -h host1
```

Chapter 6

Upgrading Storage Foundation

This chapter includes the following topics:

Upgrading Storage Foundation products or the operating system

If your system is already running a previous release of a Storage Foundation (or Foundation Suite) product, this section describes how to upgrade it to Veritas Storage Foundation 5.0.1. The operating system must be at a supported level for this upgrade. Perform the procedures in the following sections to upgrade Storage Foundation or your operating system, or both. You can perform an upgrade to Storage Foundation using the Veritas product installer or product installation script if you already have Storage Foundation installed.

This section describes how to upgrade Veritas Storage Foundation, Veritas Storage Foundation for Oracle, Veritas Storage Foundation High Availability, or Veritas Volume Replicator.

Caution: Make sure that supported combinations of Storage Foundation and the operating system are present on your system during the upgrades. Do not upgrade to a version of Storage Foundation that is not supported with the current operating system.

Upgrade requirements

This release of Veritas Storage Foundation requires the HP-UX 11i v 3.0 March 2009 OEUR release. If you are not running this release of HP-UX, upgrade HP-UX on your system before you install the new Veritas software.

Installing the 5.0.1 Veritas software will overwrite Veritas Volume Manager 5.0 software and Veritas File System 5.0 software if these were present on the system.

Disk group versions

The default disk group version for Veritas Volume Manager5.0.1 is version 140. Some new features for VxVM 5.0.1 require the latest disk group version. VxVM supports shared disk groups only on disk group version 140.

VxVM 5.0.1 supports disk groups with certain earlier versions. Table 6-1 shows the supported disk groups.

When you upgrade from a previous release, you can import the disk groups that were created with a supported disk group. For example, VxVM 5.0.1 supports all disk group versions that VxVM 4.1 supported (90 and 120). Consequently, all the disk groups that were created using VxVM 4.1 can be imported after upgrading to VxVM 5.0.1

Table 6-1 Disk group versions

Veritas Volume Manager version	Supported disk group versions
4.1	90, 120
5.0	90, 120, 140
5.0.1	90, 120, 140

After you upgrade from a previous release of VxVM, we recommend that you upgrade to the latest disk group version.

For more information about disk groups, see the *Veritas Volume Manager Administrator's Guide* .

Upgrading the operating system

If you are on an unsupported version of the operating system, you need to upgrade it to HP-UX 11i v3 March 2009 OEUR release or later.

If you are upgrading the operating system from HP-UX 11i v2, make sure that you choose the following depots along with the HP-UX 11i v3 March 2009 OEUR release depots:

- `Base-VxFS-50`
- `Base-VxTools-50`
- `Base-VxVM-50`

To upgrade the operating system from HP-UX 11i v2, run the `update-ux` command specifying the Veritas depots along with the HP-UX opearting system depots:

```
# update-ux -s os_path HPUX11i-DC-OE \
Base-VxFS-50 Base-VxTools-50 Base-VxVM-50
```

where `os_path` is the full path of the directory containing the operating system depots.

To upgrade the operating system from HP-UX 11i v3, run the `update-ux` command as follows:

```
# update-ux -s os_path HPUX11i-DC-OE
```

where `os_path` is the full path of the directory containing the operating system depots.

For detailed instructions on upgrading the operating system, see the operating system documentation.

Upgrading Storage Foundation or Storage Foundation for Oracle from older releases

If your system is already running a previous release of Storage Foundation (or Foundation Suite), this section describes how to upgrade it to Veritas Storage Foundation 5.0.1. The operating system must be at a supported level for this

upgrade. The procedure is the same if you are upgrading Storage Foundation for Oracle.

Upgrade paths for Storage Foundation or Storage Foundation for Oracle

Table 6-2 shows the recommended sequence of steps for installing any of the Veritas Storage Foundation products.

Table 6-2 Supported upgrade paths

Storage Foundation version	HP-UX version	Upgrade steps
Storage Foudation 5.0, including Maintenance Packs and Rolling Patches	HP-UX 11i v3	Upgrade to latest OS. Install SF See "Upgrading from Storage Foundation 5.0 or Storage Foundation for Oracle 5.0 on HP-UX 11i v3" on page 94.
Storage Foudation 5.0, including Maintenance Packs and Rolling Patches	HP-UX 11i v2	Upgrade to latest OS. Install SF See "Upgrading from previous versions of Storage Foundation or Storage Foundation for Oracle on HP-UX 11i v2" on page 95.
Storage Foundation 4.1, including Maintenance Packs and Rolling Patches	HP-UX 11i v3	Upgrade to latest OS. Install SF See "Upgrading from Storage Foundation 5.0 or Storage Foundation for Oracle 5.0 on HP-UX 11i v3" on page 94.
Storage Foundation 4.1, including Maintenance Packs and Rolling Patches	HP-UX 11i v2	Upgrade to latest OS. Install SF See "Upgrading from previous versions of Storage Foundation or Storage Foundation for Oracle on HP-UX 11i v2" on page 95.

Table 6-2 Supported upgrade paths *(continued)*

Storage Foundation version	HP-UX version	Upgrade steps
Storage Foundation 3.5, including Maintenance Packs and Rolling Patches	HP-UX 11i v1	Requires intermediate step to upgrade to HP-UX 11i v2. See "Upgrading from Storage Foundation 3.5 on 11i v1 to Storage Foundation 5.0.1 on HP-UX 11i v3 " on page 98.

Preparing to upgrade the Veritas software

Ensure that you have made backups of all data that you want to preserve. In particular, you will need the information in files such as `/etc/fstab`. You should also run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands, and record the output from these. You may need this information to reconfigure your system after the upgrade.

If you are upgrading an HA cluster, follow the guidelines given in the *Veritas Cluster Server (VCS) Installation Guide* for information on preserving your VCS configuration across the upgrade procedure. In particular, you should take care to make backups of configuration files, such as `main.cf` and `types.cf`, in the `/etc/VRTSvcs/conf/config` directory. Additional configuration files, such as `OracleTypes.cf`, may also be present in this directory if you have installed any VCS agents. You should also back up these files.

To prepare for the Veritas software upgrade

1. Log in as superuser.
2. Perform any necessary preinstallation checks and configuration.

   See "About planning for a Storage Foundation installation" on page 17.
3. If you are upgrading Veritas Storage Foundation for Oracle, resynchronize all existing snapshots before upgrading.

   ```
   # /opt/VRTS/bin/dbed_vmsnap -S $ORACLE_SID -f SNAPPLAN -o resync
   ```
4. Use the `vxlicrep` command to make a record of the currently installed Veritas licenses. Print the output or save it on a different system.
5. Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes.

6 If you are upgrading a high availability (HA) product, take all service groups offline.

List all service groups:

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

For each service group listed, take it offline:

```
# /opt/VRTSvcs/bin/hagrp -offline service_group -sys system_name
```

7 Use the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

```
# df -F vxfs
```

8 Unmount all Storage Checkpoints and non-system VxFS file systems:

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

9 Verify that all file systems have been cleanly unmounted:

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

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

10 (Optional) If a file system is not clean, enter the following commands for that file system:

```
# fsck -F vxfs filesystem
# mount -F 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 fileset clone removal extended operation if the `umount` command fails with the following error:

```
file system device busy
```

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.
```

11 (Optional) 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 fileset clone can take several hours.

12 (Optional) Repeat step 9 to verify that the unclean file system is now clean.

13 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
```

14 Comment out the non-system local VxFS mount points from the `/etc/fstab`. 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 uncomment these entries in the `/etc/fstab` file on the upgraded system.

15 If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:

- Verify that all of the Primary RLINKs are up to date:

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

- Detach the RLINKs.

- Disassociate the SRL.

Upgrading from Storage Foundation 5.0 or Storage Foundation for Oracle 5.0 on HP-UX 11i v3

This procedure describes upgrading from Storage Foundation 5.0 on HP-UX 11i v3 to Storage Foundation 5.0.1 on HP-UX 11i v3. Use the same procedure to upgrade from Storage Foundation for Oracle 5.0 on HP-UX 11i v3 to Storage Foundation for Oracle 5.0.1.

After successful completion of the upgrade, any disk groups that were created in Storage Foundation 5.0 are accessible by Storage Foundation 5.0.1.

The Veritas product installer does not support changing the product level and upgrading versions in a single operation. To upgrade from Storage Foundation 5.0 to Storage Foundation for Oracle 5.0.1, first upgrade to Storage Foundation 5.0.1. Then install Storage Foundation for Oracle 5.0.1.

To upgrade from Storage Foundation or Storage Foundation for Oracle on HP-UX 11i v3

1. Perform the necessary preupgrade tasks such as resynchronizing existing database snapshots.

   See "Preparing to upgrade the Veritas software" on page 91.

2. Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release.

   See "Upgrading the operating system" on page 89.

3. If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.

4. Install Storage Foundation 5.0.1 for HP-UX 11i v3 using the installer script.

   ```
   # ./installer [-rsh]
   ```

5. From the Installation menu, choose the `I` option for Install and enter the number for for Veritas Storage Foundation or for Veritas Storage Foundation for Oracle. Press **Return**.

6. Enter `y` to upgrade to version 5.0.1 on these systems using the current configuration.

   ```
   Do you want to upgrade to version 5.0.31.5 on these systems using
   the current configuration? [y,n,q,?] (y)
   ```

7 Uncomment the entries in the `/etc/fstab` file which were commented as part of the pre-upgrade steps.

8 Reboot all the nodes.

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

9 Configure Veritas Storage Foundation or Veritas Storage Foundation for Oracle.

To configure Storage Foundation 5.0.1 for HP-UX 11i v3 use the following command:

```
# ./ installsf [-rsh] -configure
```

To configure Storage Foundation for Oracle. 5.0.1 for HP-UX 11i v3 use the following command:

```
# ./ installsfora [-rsh] -configure
```

10 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

11 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

12 If you upgraded from Storage Foundation 4.1, we recommend that you upgrade the VxVM disk groups to the latest version. Storage Foundation 5.0.1 supports importing disk groups that were created using VxVM 4.1. However, new functionality may require the latest disk group version.

See "Upgrading VxVM disk group versions" on page 127.

13 If you upgraded SF for Oracle, perform the required post-upgrade tasks:

See "Post-upgrade tasks" on page 118.

Upgrading from previous versions of Storage Foundation or Storage Foundation for Oracle on HP-UX 11i v2

This procedure describes upgrading Storage Foundation or Storage Foundation for Oracle from a previous version on HP-UX 11i v2. You can upgrade to Storage Foundation 5.0.1 from Storage Foundation 4.1 or 5.0 on HP-UX 11i v2. You can upgrade to Storage Foundation for Oracle 5.0.1 from Storage Foundation for Oracle 4.1 or 5.0 on HP-UX 11i v2.

Both Storage Foundation and Storage Foundation for Oracle 5.0.1 require that you upgrade the operating system to the latest supported version of HP-UX 11i v3.

After successful completion of the upgrade, any disk groups that were created in Storage Foundation 4.1 or 5.0 are accessible by Storage Foundation 5.0.1.

The Veritas product installer does not support changing the product level and upgrading versions in a single operation. To upgrade from Storage Foundation 4.1MP2 to Storage Foundation for Oracle 5.0.1, first upgrade to Storage Foundation 5.0.1. Then install Storage Foundation for Oracle 5.0.1.

To upgrade from Storage Foundation or Storage Foundation for Oracle on HP-UX 11i v2

1. Perform the necessary preupgrade tasks such as resynchronizing existing database snapshots.

   See "Preparing to upgrade the Veritas software" on page 91.

2. If you have any external Array Policy Modules (APMs) installed, uninstall the APMs. The following warning message displays during the OS upgrade and also when you issue an administrative command for HP-UX kernel modules after the upgrade, until SF 5.0 on HP-UX 11i v3 is installed:

   ```
   WARNING: The file '/usr/conf/mod/dmpXXX.1' does not
   contain valid kernel code. It will be ignored.
   ```

   This message can be ignored and does not affect the functionality of SF.

3. Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release.

   See "Upgrading the operating system" on page 89.

4. If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.

5. Install Storage Foundation 5.0.1 for HP-UX 11i v3 using the installer script.

   ```
   # ./installer [-rsh]
   ```

6. From the Installation menu, choose the `I` option for Install and enter the number for Veritas Storage Foundation or for Veritas Storage Foundation for Oracle. Press **Return**.

7 Enter `y` to upgrade to version 5.0.1 on these systems using the current configuration.

```
Do you want to upgrade to version 5.0.1 on these systems using
the current configuration? [y,n,q,?] (y)
```

8 Reboot all the nodes.

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

9 Configure Veritas Storage Foundation or Veritas Storage Foundation for Oracle.

To configure Storage Foundation 5.0.1 for HP-UX 11i v3 use the following command:

```
# ./ installsf [-rsh] -configure
```

To configure Storage Foundation for Oracle. 5.0.1 for HP-UX 11i v3 use the following command:

```
# ./ installsfora [-rsh] -configure
```

10 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

11 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

12 If you upgraded from Storage Foundation 4.1, we recommend that you upgrade the VxVM disk groups to the latest version. Storage Foundation 5.0.1 supports importing disk groups that were created using VxVM 4.1. However, new functionality may require the latest disk group version.

See "Upgrading VxVM disk group versions" on page 127.

13 If you upgraded SF for Oracle, perform the necessary post-upgrade tasks.

See "Post-upgrade tasks" on page 118.

14 If you upgraded SF for Oracle, upgrade to the new repository database.

Upgrading from Storage Foundation 3.5 on 11i v1 to Storage Foundation 5.0.1 on HP-UX 11i v3

This procedure describes upgrading Storage Foundation 3.5 on HP-UX 11i v1 to Storage Foundation 5.0.1 on HP-UX 11i v3. Upgrading from HP-UX 11i v1 requires an intermediate upgrade to HP-UX 11i v2.

Veritas Volume Manager 3.5 and Veritas Volume Manager 5.0.1 both support disk group version 90. Therefore, any disk groups with version 90 are accessible by Storage Foundation 5.0.1 after the upgrade. However, certain features in Storage Foundation 5.0.1 may require the latest disk group version. Therefore, we recommend upgrading the disk group.

To upgrade from Storage Foundation 3.5 on HP-UX 11i v1 to Storage Foundation 5.0.1 on HP-UX 11i v3

1. Stop activity to all Storage Foundation 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.
2. Upgrade from HP-UX 11i v1 to HP-UX 11i v2 using practices recommended by HP. HP-UX 11i v2 includes VxVM 4.1 by default. All disk groups created using Storage Foundation 3.5 on HP-UX 11i v1 would be accessible.
3. Upgrade from HP-UX 11i v2 to the latest available HP-UX 11i v3 fusion release, using practices recommended by HP. The HP-UX 11i v3 fusion release includes VxVM 5.0 by default.
4. If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.
5. Install Storage Foundation 5.0.1 for HP-UX 11i v3.

   See “Performing the installation” on page 37.
6. Configure Storage Foundation 5.0.1 HP-UX 11i v3 using the `installsf -configure` option.

   See “Configuring the products using the common product installer” on page 49.
7. Disk groups created using VxVM 4.1 can be imported after upgrading to VxVM 5.0. However, we recommend upgrading the VxVM disk groups to the latest version.

   See “Upgrading VxVM disk group versions” on page 127.

Upgrading from VxVM 5.0 on HP-UX 11i v3 to VxVM 5.0.1 using integrated VxVM 5.0.1 package for HP-UX 11i v3

You can upgrade from VxVM 5.0 on HP-UX 11i v3 to VxVM 5.0.1 on HP-UX 11i v3. Use the integrated VxVM 5.0.1 package for HP-UX 11i v3 from the ignite depot.

To upgrade using the integrated VxVM 5.0.1 package from the ignite depot

1. Use HP recommended steps to integrate VxVM 5.0.1 package with the latest 11i v3 fusion.
2. Stop activity to all Storage Foundation 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.
3. Upgrade the HP-UX 11i v3 operating system to the latest fusion using the integrated VxVM 5.0.1 package. This process installs VxVM 5.0.1 package with the operating system. All disk groups that were created using VxVM 5.0 11i v3 are accessible.
4. The package VRTSvmdoc is obsolete in VxVM 5.0.1. After the upgrade, you can safely remove the package using the following command:

   ```
   # swremove VRTSvmdoc
   ```

Upgrading Storage Foundation High Availability (SFHA) or Storage Foundation for Oracle HA (SFORA HA) from older releases

If your system is already running a previous release of Storage Foundation High Availability or Storage Foundation for Oracle High Availability, this section describes how to upgrade it to 5.0.1. The operating system must be at a supported level for this upgrade.

Overview of procedures

Note: If VVR is configured, phased upgrade is not supported. We recommend that the secondary cluster be upgraded before the primary cluster in the RDS.

The upgrade procedures apply to both the phased and full upgrade procedures unless otherwise noted. Occasionally, steps differ between the two procedures. Screen output is also common between both procedures unless otherwise noted.

Note: Both procedures automatically uninstall the previous version of the software.

Phased upgrade

A phased upgrade minimizes downtime by upgrading portions of the cluster, one portion at a time. Although the entire cluster is offline for a shorter period than a full upgrade, this method requires command-line interaction and some manual configuration. Each phase of the phased upgrade should be performed on more than one node of the cluster.

Note: A phased upgrade should not be performed from one of the nodes in the cluster.

Full upgrade

A full upgrade upgrades the product on the entire cluster and the cluster remains offline for the duration of the procedure. Minimal command-line interaction and some manual configuration are required.

Upgrading from Storage Foundation HA or Storage Foundation for Oracle HA from 5.0 on HP-UX 11i v3 to 5.0.1 on HP-UX 11i v3

Storage Foundation HA or Storage Foundation for Oracle HA can be upgraded from 5.0 on HP-UX 11i v3 to 5.0.1 on HP-UX 11i v3 using phased or full upgrade procedure.

Performing a phased upgrade from version 5.0 on HP-UX 11i v3 to Storage Foundation 5.0.1

Perform the following procedures to upgrade Storage Foundation clusters from version 5.0 on HP-UX 11i v3 to Storage Foundation 5.0.1.

The phased upgrade involves the following steps:

- Upgrading the first half of the cluster, system01 and system02.

  Note: Your downtime starts after you complete the upgrade of the first half of the cluster.

- Stopping the second half of the cluster, system03 and system04.
- Bringing online the first half of the cluster, system01 and system02.

Note: Your downtime ends after you bring the first half of the cluster online.

- Upgrading the second half of the cluster, system03 and system04.

Note: Do not disable fencing as the high availability daemon must be up and running for the upgrade.

Perform the following steps on the first half of the cluster, system01 and system02.

To upgrade the first half of the cluster

1. Stop all the applications on the nodes that are not under VCS control. Use native application commands to stop the applications.
2. Switch the failover groups from the first half of the cluster to one of the nodes in the second half of the cluster.

   ```
   # hagrp -switch failover_group -to system03
   ```

3. Stop all VCS service groups.

   ```
   # hagrp -offline group_name -sys system01
   # hagrp -offline group_name -sys system02
   ```

4. Freeze the nodes in the first half of the cluster

   ```
   # haconf makerw
   # hasys -freeze -persistent system01
   # hasys -freeze -persistent system02
   # haconf -dump -makero
   ```

5. Stop VCS on the first half of the cluster:

   ```
   # hastop -local -force
   ```

6. If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.
7. Set the LLT_START attribute to 0 in the `/etc/rc.config.d/lltconf` file:

   ```
   LLT_START=0
   ```

8 On each node of the first half of the cluster, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

9 If the cluster-wide attribute `UseFence` is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file.

10 Stop all the modules on the first half of the cluster.

The first and fifth steps regarding odm apply only if you are upgrading SF Oracle HA.

```
# /sbin/init.d/odm stop
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule odm=unused
# kcmodule gab=unused
# lltconfig -U
# kcmodule llt=unused
```

11 On each node of the first half of the cluster, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
```

12 Upgrade the HP-UX operating system to HP-UX 11iv3 Mar 09 fusion.

See "Upgrading the operating system" on page 89.

13 Upgrade the Veritas product:.

To upgrade Storage Foundation HA:

```
# ./installsf [-rsh]  system01 system02
```

To upgrade Storage Foundation Oracle HA:

```
# ./installsfora [-rsh]  system01 system02
```

Note: DO NOT reboot the cluster.

After the installation completes, perform the following steps on the second half of the cluster.

Note: Your downtime starts now.

To stop the second half of the cluster

1. Stop all the applications on the node that are not under VCS control. Use native application commands to stop the applications.
2. Stop all VCS service groups.

```
# hagrp -offline group_name -sys system03
# hagrp -offline group_name -sys system04
```

3. Freeze the nodes in the second half of the cluster

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

4. Stop VCS on the second half of the cluster:

```
# hastop -local -force
```

5. If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.
6. Set the LLT_START attribute to 0 in the `/etc/rc.config.d/lltconf` file:

```
LLT_START=0
```

7. On each node of the second half of the cluster, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

8. If the cluster-wide attribute `UseFence` is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file.

9 Stop all the modules on the second half of the cluster:

The first and fifth steps regarding odm apply only if you are upgrading SF Oracle HA.

```
# /sbin/init.d/odm stop
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule odm=unused
# kcmodule gab=unused
# lltconfig -U
# kcmodule llt=unused
```

10 On each node of the second half of the cluster, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
```

Perform the following steps on the first half of the cluster, system01 and system02, to bring the first half of the cluster online.

To bring the first half of the cluster online

1 Uncomment the VxFS mount point entries in the /etc/fstab file.

2 Mount the VxFS file systems that were commented in step 6

3 Enable fencing:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

4 Remove the following line from `/etc/VRTSvcs/conf/config/main.cf`:

```
Frozen=1
```

5 Set the clusterwide attribute `UseFence` to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

```
UseFence=SCSI3
```

6 Remove the following file located in the directory `/opt/VRTS/install`:

For SF HA upgrade, remove the file: `.SF.upgrade`

For SF Oracle HA upgrade, remove the file: `.SFORA.upgrade`

7 Reboot the first half of the cluster:

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

8 After the nodes come up, seed the cluster membership:

```
# gabconfig -x
```

The first half of the cluster is now up and running.

Note: The downtime ends here.

Perform the following steps on the second half of the cluster, system03 and system04, to upgrade the second half of the cluster.

To upgrade the second half of the cluster

1 Upgrade the HP-UX operating system to HP-UX 11iv3 Mar 09 fusion.

See "Upgrading the operating system" on page 89.

2 Upgrade the Veritas product:.

To upgrade Storage Foundation HA:

```
# ./installsf [-rsh]  system03 system04
```

To upgrade Storage Foundation Oracle HA:

```
# ./installsfora [-rsh]  system03 system04
```

Note: DO NOT reboot the cluster.

3 Uncomment the VxFS mount point entries in the /etc/fstab file on the second half of the cluster.

4 Mount the VxFS file systems that were commented in step 5

5 Enable fencing:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

6 Remove the following file located in the directory `/opt/VRTS/install`:

For SF HA upgrade, remove the file: `.SF.upgrade`

For SF Oracle HA upgrade, remove the file: `.SFORA.upgrade`

7 Reboot the second half of the cluster:

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

The nodes system03 and system04 now join the first half of the cluster.

8 Start the applications that are not configured under VCS. Use native application commands to start the applications.

9 Perform the post-upgrade tasks.

See "Post-upgrade tasks" on page 118.

Performing a full upgrade from Storage Foundation HA or Storage Foundation for Oracle HA from 5.0 on HP-UX 11i v3 to 5.0.1 on HP-UX 11i v3

If your systems are already running Storage Foundation High Availability 5.0 on HP-UX 11i v3, this section describes how to upgrade to Veritas Storage Foundation 5.0.1. The operating system must be at a supported level for this upgrade.

This procedure describes upgrading from Storage Foundation 5.0 on HP-UX 11i v3 to Storage Foundation 5.0.1 on HP-UX 11i v3. Use the same procedure to upgrade from Storage Foundation for Oracle 5.0 on HP-UX 11i v3 to Storage Foundation for Oracle 5.0.1.

After successful completion of the upgrade, any disk groups that were created in Storage Foundation 5.0 are accessible by Storage Foundation 5.0.1.

The Veritas product installer does not support changing the product level and upgrading versions in a single operation. To upgrade from Storage Foundation 5.0 to Storage Foundation for Oracle 5.0.1, first upgrade to Storage Foundation 5.0.1. Then install Storage Foundation for Oracle 5.0.1.

To upgrade from SFHA or SFORA HA 5.0 on 11.31 to 5.0.1 on 11.31

1 Stop activity to all SFHA 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.

2 Offline all the VCS service groups.

```
# hagrp -offline servicegroup -sys node_name
```

3 Stop VCS if it is already running. On any node, run the following command:

```
# /opt/VRTS/bin/hastop -all
```

4 If fencing is configured with VCS, you must disable fencing before proceeding to upgrade.

To disable fencing, perform the following steps:

- If the cluster-wide attribute "UseFence" is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf`file
- On each node, edit the `etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

- Stop I/O fencing on each node:

```
# /sbin/init.d/vxfen stop
```

```
# /sbin/vxfenconfig -U
```

5 Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release.

6 If patches to HP-UX 11i v3 are required, apply the patches before upgrading the product.

7 Install Storage Foundation 5.0.1 for HP-UX 11i v3 using the installer script.

```
# ./installer [-rsh]
```

8 From the Installation menu, choose the `I` option for Install and enter the number for Veritas Storage Foundation High Availability. Press **Return**.

9 Enter `y` to upgrade to version 5.0 on these systems using the current configuration.

```
Do you want to upgrade to version 5.0 on these systems using
the current configuration? [y,n,q,?] (y)
```

10 Reboot all the nodes.

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

11 Configure Storage Foundation 5.0.1 for HP-UX 11i v3 using the following command:

```
# ./ installsf [-rsh] -configure
```

12 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

13 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

14 Disk groups that were created using VxVM 4.1 can be imported after upgrading to VxVM 5.0. However, we recommend upgrading the VxVM disk groups to the latest version.

See "Upgrading VxVM disk group versions" on page 127.

15 Enable I/O fencing if required. Follow the below steps to enable the fencing.

- Stop VCS from any one node as below:

```
# /opt/VRTS/bin/hastop -all
```

- Execute the following steps on all the nodes:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode

# /sbin/init.d/vxfen stop

# /sbin/init.d/vxfen start
```

- Set the clusterwide attribute "UseFence" to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

```
UseFence=SCSI3
```

- Verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file by running the following commands:

```
# cd /etc/VRTSvcs/conf/config

# /opt/VRTS/bin/hacf -verify .
```

- Start the VCS engine on each system:

```
# /opt/VRTS/bin/hastart
```

Upgrading from SFHA or SFORAHA 4.1 or 5.0 on HP-UX 11i v2 to SFHA or SFORAHA 5.0.1 on HP-UX 11i v3

Storage Foundation HA or Storage Foundation for Oracle HA can be upgraded from 4.1 or 5.0 on HP-UX 11i v2 to 5.0.1 on HP-UX 11i v3 using phased or full upgrade procedure.

Performing phased upgrade of Storage Foundation HA and Storage Foundation for Oracle HA from versions 4.1x or 5.0x on HP-UX 11i v2

The phased upgrade involves the following steps:

- Upgrading the first half of the cluster, system01 and system02.

  Note: Your downtime starts after you complete the upgrade of the first half of the cluster.

- Stopping the second half of the cluster, system03 and system04.
- Bringing online the first half of the cluster, system01 and system02.

  Note: Your downtime ends after you bring the first half of the cluster online.

- Upgrading the second half of the cluster, system03 and system04.

Perform the following steps on the first half of the cluster, system01 and system02, to upgrade the first half of the cluster.

To upgrade the first half of the cluster

1. Stop all the applications that are not configured under VCS.
2. Switch the failover groups from the first half of the cluster to one of the nodes in the second half of the cluster:

   ```
   # hagrp -switch failover_group -to system03
   ```

3. Stop all VCS service groups.

   ```
   # hagrp -offline group_name -sys system01
   # hagrp -offline group_name -sys system02
   ```

4 Freeze the nodes in the first half of the cluster

```
# haconf makerw
# hasys -freeze -persistent system01
# hasys -freeze -persistent system02
# haconf -dump -makero
```

5 Stop VCS on the first half of the cluster:

```
# hastop -local -force
```

6 If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.

7 Set the LLT_START attribute to 0 in the `/etc/rc.config.d/lltconf` file:

```
LLT_START=0
```

8 On each node of the first half of the cluster, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

9 If the cluster-wide attribute `UseFence` is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file.

10 Stop all the modules on the first half of the cluster.

The first and fifth steps regarding odm apply only if you are upgrading SF Oracle HA.

```
# /sbin/init.d/odm stop
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule odm=unused
# kcmodule gab=unused
# lltconfig -U
# kcmodule llt=unused
```

11 On each node of the first half of the cluster, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
```

12 Upgrade the HP-UX operating system to HP-UX 11iv3 Mar 09 fusion.

See "Upgrading the operating system" on page 89.

13 Upgrade the Veritas product:.

To upgrade Storage Foundation HA:

```
# ./installsf [-rsh] system01 system02
```

To upgrade Storage Foundation Oracle HA:

```
# ./installsfora [-rsh] system01 system02
```

Note: DO NOT reboot the cluster.

Perform the following steps on the second half of the cluster, system03 and system04, to stop the second half of the cluster.

Note: The downtime starts now.

To stop the second half of the cluster

1 Stop all the applications that are not configured under VCS.

2 Stop all VCS service groups.

```
# hagrp -offline group_name -sys system03
# hagrp -offline group_name -sys system04
```

3 Freeze the VCS service groups on the second half of the cluster:

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

4 Stop VCS on the second half of the cluster:

```
# hastop -local -force
```

5 If you created local VxFS mount points on VxVM volumes and added them to /etc/fstab, comment out the mount point entries in the /etc/fstab file.

6 Set the LLT_START attribute to 0 in the `/etc/rc.config.d/lltconf` file:

```
LLT_START=0
```

7 On each node of the second half of the cluster, edit the `/etc/vxfenmode` file to configure I/O fencing in disabled mode:

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

8 If the cluster-wide attribute `UseFence` is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file.

9 Stop all the modules on the second half of the cluster:

The first and fifth steps regarding odm apply only if you are upgrading SF Oracle HA.

```
# /sbin/init.d/odm stop
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule odm=unused
# kcmodule gab=unused
# lltconfig -U
# kcmodule llt=unused
```

10 On each node of the second half of the cluster, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
```

Perform the following steps on the first half of the cluster, system01 and system02, to bring the first half of the cluster online.

To bring the first half of the cluster online

1 Uncomment the VxFS mount point entries in the **/etc/fstab** file.

2 Mount the VxFS file systems that were commented in step 6

3 Enable fencing:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

4 Remove the following line from `/etc/VRTSvcs/conf/config/main.cf`:

```
Frozen=1
```

5 Set the clusterwide attribute `UseFence` to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

```
UseFence=SCSI3
```

6 Remove the following file located in the directory `/opt/VRTS/install`:

For SF HA upgrade, remove the file: `.SF.upgrade`

For SF Oracle HA upgrade, remove the file: `.SFORA.upgrade`

7 Reboot the first half of the cluster:

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

8 After the nodes come up, seed the cluster membership:

```
# gabconfig -x
```

The first half of the cluster is now up and running.

Note: The downtime ends here.

Perform the following steps on the second half of the cluster, system03 and system04, to upgrade the second half of the cluster.

To upgrade the second half of the cluster

1 Upgrade the operating system.

See "Upgrading the operating system" on page 89.

2 Upgrade the Veritas product:.

To upgrade Storage Foundation HA:

```
# ./installsf [-rsh]  system03 system04
```

To upgrade Storage Foundation Oracle HA:

```
# ./installsfora [-rsh]  system03 system04
```

Note: DO NOT reboot the cluster.

---

3 Uncomment the VxFS mount point entries in the **/etc/fstab** file.

4 Mount the VxFS file systems that were commented in step 5

5 Enable fencing:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
```

6 Remove the following file located in the directory `/opt/VRTS/install`:

For SF HA upgrade, remove the file: `.SF.upgrade`

For SF Oracle HA upgrade, remove the file: `.SFORA.upgrade`

7 Reboot the second half of the cluster:

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

The nodes system03 and system04 now join the first half of the cluster.

8 Start the applications that are not configured under VCS. Use native application commands to start the applications.

9 Perform the post-upgrade tasks.

See "Post-upgrade tasks" on page 118.

Performing a full upgrade from SFHA or SFORAHA 4.1 or 5.0 on HP-UX 11i v2 to SFHA or SFORAHA 5.0.1 on HP-UX 11i v3

If your systems are already running Storage Foundation High Availability 4.1 or 5.0 on HP-UX 11i v2, you must upgrade the operating system to HP-UX 11i v3. Then upgrade Storage Foundation High Availability to Storage Foundation High Availability 5.0.1.

- Prepare to upgrade Veritas products
  See "Preparing to upgrade the Veritas software" on page 91.
- Prepare to upgrade SFHA or SFORAHA on HP-UX 11iv2 to HP-UX 11iv3
  See "Preparing to upgrade SFHA or SFORAHA on HP-UX 11i v2 to HP-UX 11i v3" on page 114.
- Upgrade HP-UX
  See "Upgrading HP-UX" on page 116.
- Upgrade SFHA
  See "Upgrading SFHA or SFORA HA on HP-UX 11i v2 to 5.0.1" on page 116.

Preparing to upgrade SFHA or SFORAHA on HP-UX 11i v2 to HP-UX 11i v3

Perform the following steps before you upgrade SFHA or SFORAHA on HP-UX 11i v2 to SFHA on HP-UX 11i v3.

To prepare for upgrading SFHA or SFORAHA on HP-UX 11i v2 to HP-UX 11iv3

1 Freeze all the service groups in the configuration.

```
# haconf -makerw
# hagrp -freeze servicegroup -persistent
# haconf -dump -makero
```

2 Stop VCS if it is already running. On any node, run the following command:

```
# hastop -all -force
```

3 If fencing is configured with VCS, you must disable fencing before proceeding to upgrade.

To disable fencing, perform the following steps:

- If the cluster-wide attribute “UseFence” is set to SCSI3, reset the value to NONE in the /etc/VRTSvcs/conf/config/main.cf file.
- On each node, edit /etc/vxfenmode to configure vxfen in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

- Stop I/O fencing on each node:

```
# /sbin/init.d/vxfen stop
```

```
# /sbin/vxfenconfig -U
```

4 Stop GAB on each node:

```
# /sbin/gabconfig -U
```

5 Stop LLT on each node:

```
# /sbin/lltconfig -Uo
```

6 Change LLT_START=0 in "/etc/rc.config.d/lltconf" on each node.

7 Remove LLT, GAB, and VxFEN device files on each node:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
```

Upgrading HP-UX

Upgrade the HP-UX operating system to the latest available HP-UX 11i v3 fusion release. The Base-VxFS-50, Base-VxVM-50 and Base-VxTools-50 bundles need to be selected while upgrading using update-ux(1M).

If patches to HP-UX 11i v3 are required, apply the patches before upgrading the Veritas product.

Upgrading SFHA or SFORA HA on HP-UX 11i v2 to 5.0.1

Use the product installer to upgrade the packages from SFHA 4.1 or 5.0 to SFHA 5.0.1. SFHA 5.0.1 is only supported on HP-UX 11i v3. If you are already running Storage Foundation High Availability or Storage Foundation for Oracle 4.1 or 5.0 on HP-UX 11i v2, you must upgrade the operating system to HP-UX 11i v3. Then upgrade Storage Foundation High Availability to Storage Foundation High Availability 5.0.1.

To upgrade from Storage Foundation HA or SF Oracle HA 4.1 or 5.0 on HP-UX 11i v2 to Storage Foundation HA or SF Oracle HA 5.0.1

1. Check if the VEA service is running:

```
# /opt/VRTS/bin/vxsvcctrl status
```

2. If the VEA service is running, stop it:

```
# /opt/VRTS/bin/vxsvcctrl stop
```

3. Insert the appropriate software disc into your system's DVD drive.
4. Create a directory in which to mount the software disc and mount the disc using the appropriate drive name. For example:

```
# mkdir -p /dvdrom
# /usr/sbin/mount -F cdfs /dev/dsk/c3t2d0 /dvdrom
```

5. Change to the top-level directory on the disc:

```
# cd /dvdrom
```

6. Install Storage Foundation 5.0.1 for HP-UX 11i v3 using the installer script.

```
# ./installer [-rsh]
```

7. From the Installation menu, choose the `I` option for Install and enter the number for Veritas Storage Foundation High Availability. Press **Return**.

8 Enter `y` to upgrade to version 5.0 on these systems using the current configuration.

```
Are you sure you want to upgrade SFORA? [y,n,q,?] (y)

Are you ready to begin the Veritas Storage Foundation for
Oracle upgrade at this time? [y,n,q,?] (y)
```

9 Uncomment the entries in `/etc/fstab` which were commented as part of the pre-upgrade steps.

10 Reboot all the nodes.

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

11 Configure Storage Foundation 5.0.1 for HP-UX 11i v3

For SFHA upgrade, use the following command:

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

# ./ installsf [-rsh] -configure
```

For SFORAHA upgrade, use the following command:

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

# ./ installsfora [-rsh] -configure
```

12 Check if the VEA service was restarted:

```
# /opt/VRTS/bin/vxsvcctrl status
```

13 If the VEA service is not running, restart it:

```
# /opt/VRTS/bin/vxsvcctrl start
```

14 Disk groups that were created using VxVM 4.1 can be imported after upgrading to VxVM 5.0. However, we recommend upgrading the VxVM disk groups to the latest version.

See "Upgrading VxVM disk group versions" on page 127.

15 Enable I/O fencing if required. Follow the below steps to enable the fencing.

- Stop VCS from any one node as below:

```
# /opt/VRTS/bin/hastop -all
```

- Execute the following steps on all the nodes:

  ```
  # cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode

  # /sbin/init.d/vxfen stop

  # /sbin/init.d/vxfen start
  ```

- Set the clusterwide attribute "UseFence" to use SCSI3. Add the following line to the `/etc/VRTSvcs/conf/config/main.cf` file:

  ```
  UseFence=SCSI3
  ```

- Verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file by running the following commands:

  ```
  # cd /etc/VRTSvcs/conf/config

  # /opt/VRTS/bin/hacf -verify .
  ```

- Start the VCS engine on each system:

  ```
  # /opt/VRTS/bin/hastart
  ```

Post-upgrade tasks

The tasks in the following sections must be performed after upgrade, to restore the previous configurations and set up Storage Foundation 5.0.1 correctly. Perform the tasks required for the products and features that are relevant to your installation.

Linking the Veritas extension for Oracle Disk Manager library into Oracle home

If the Veritas extension for Oracle Disk Manager library is not linked into Oracle home, perform the following procedure. The steps vary depending on the Oracle version.

To link the Veritas extension for Oracle Disk Manager library into Oracle home for Oracle 11g

1. Shut down the database instance before linking the Oracle Disk Manager library.
2. Use the `mv` and `ln` commands as follows.

   For HP-UX PA, enter:

   ```
   # mv ${ORACLE_HOME}/lib/libodm11.sl \
   ${ORACLE_HOME}/lib/libodm11.sl.orig
   # ln -s /opt/VRTSodm/lib/libodm.sl \
   ${ORACLE_HOME}/lib/libodm11.sl
   ```

   For HP-UX IA, enter:

   ```
   # mv ${ORACLE_HOME}/lib/libodm11.so \
   ${ORACLE_HOME}/lib/libodm11.so.orig
   # ln -s /opt/VRTSodm/lib/libodm.sl \
   ${ORACLE_HOME}/lib/libodm11.so
   ```

3. Start the database instance after linking the Oracle Disk Manager library.

To link the Veritas extension for Oracle Disk Manager library into Oracle home for Oracle 10g

1. Shut down the database instance before linking the Oracle Disk Manager library.
2. Use the `mv` and `ln` commands as follows:

   For HP-UX PA, enter:

   ```
   # mv ${ORACLE_HOME}/lib/libodm10.sl \
   ${ORACLE_HOME}/lib/libodm10.sl.orig
   # ln -s /opt/VRTSodm/lib/libodm.sl \
   ${ORACLE_HOME}/lib/libodm10.sl
   ```

   For HP-UX IA, enter:

   ```
   # mv ${ORACLE_HOME}/lib/libodm10.so \
   ${ORACLE_HOME}/lib/libodm10.so.orig
   # ln -s /opt/VRTSodm/lib/libodm.sl \
   ${ORACLE_HOME}/lib/libodm10.so
   ```

3. Start the database instance after linking the Oracle Disk Manager library.

To link the Veritas extension for Oracle Disk Manager library into Oracle home for Oracle9i

1. Shut down the database instance before linking the Oracle Disk Manager library.
2. Use the `mv` and `ln` commands as follows.

   For HP-UX PA, enter:

   ```
   # mv ${ORACLE_HOME}/lib/libodm9.sl \
   ${ORACLE_HOME}/lib/libodm9.sl.orig
   # ln -s /opt/VRTSodm/lib/libodm.sl \
   ${ORACLE_HOME}/lib/libodm9.sl
   ```

   For HP-UX IA, enter:

   ```
   # mv ${ORACLE_HOME}/lib/libodm9.so \
   ${ORACLE_HOME}/lib/libodm9.so.orig
   # ln -s /opt/VRTSodm/lib/libodm.sl \
   ${ORACLE_HOME}/lib/libodm9.so
   ```

   When Oracle Disk Manager is enabled, a message similar to the following is sent to the alert log: "`Oracle instance running with ODM: Veritas #.# ODM Library, Version #.#`."

   When the system and instance are configured correctly, the Oracle Disk Manager feature is used, by default, for accessing any database storage.
3. Start the database instance after linking the Oracle Disk Manager library.

Upgrading to the new repository database for Oracle

When you install or upgrade Veritas Storage Foundation for Oracle, you need to either create a new repository database or migrate your old repository database to a new one. To use the `dbed_update` command, you must be the instance owner or database administrator.

To upgrade your repository for releases before 5.0

1. Create and configure the new repository database with the `sfua_db_config` command.

   ```
   # /opt/VRTSdbcom/bin/sfua_db_config
   ```

2. Migrate your old repository information into the new repository database.

3 If you are upgrading Veritas Storage Foundation for Oracle in a single-host environment, run the `dbed_update` command.

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

If you are upgrading Veritas Storage Foundation for Oracle in a high availability (HA) environment, run the `dbed_update` command with the `-G` option.

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

4 After the upgrade, the old repository database is marked with a hidden file name, such as `/etc/vx/vxdba/.instance_name`, to prevent further updates. If you need to perform an additional upgrade, the file must be removed.

To upgrade your repository database for releases after 5.0

1 In a standalone instance, run sfua_db_config once:

```
# /opt/VRTSdbcom/bin/sfua_db_config
```

This step completes the upgrade of the repository in a standalone configuration.

2 In a cluster environment, complete the remaining steps.

3 Unconfigure the SFUA repository from the VCS configuration:

```
# /opt/VRTSdbcom/bin/sfua_db_config -o unconfig_cluster
```

4 Mount the repository file system manually.

5 Run the sfua_db_config command again with no options.

```
# /opt/VRTSdbcom/bin/sfua_db_config
```

Changing permissions for Storage Foundation for Databases

After installing Veritas Storage Foundation 5.0.1, follow these post-installation steps to ensure Veritas Storage Foundation for Oracle commands work correctly.

Note: Do not recursively change permissions, groups, or owners

To change permissions

1. Change permissions for the following directory, depending on which product you have installed:

   For Veritas Storage Foundation for Oracle:

   ```
   # chmod 550 /opt/VRTSdbed
   ```

2. Reset owner and group settings to the appropriate owner and group for the database administrators on your system.

   For example, in Veritas Storage Foundation for Oracle, to change owner to the user oracle and the group dba, run the following command:

   ```
   # chown oracle:dba /opt/VRTSdbed
   ```

Editing the snapplan after upgrading Veritas Storage Foundation for Oracle

After you upgrade to Veritas Storage Foundation for Oracle 5.0.1, upgrade any existing snapplan from a previous release. Complete this procedure before you re-validate the snapplan.

To upgrade the snapplan

1 Change to the directory containing the snapplan file:

```
# cd /snapplan
```

2 View the snapplan.

```
# cat snap1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg1
SNAPSHOT_DG=SNAP_PRODdg1
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
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=2
```

3 Open the snapplan in a text editor such as vi:

```
# vi snap1
```

4 Remove the line containing following parameter:

```
SNAPSHOT_DG=<Some text string>
```

5 Add one more line to the snapplan with the following parameter:

```
SNAPSHOT_DG_PREFIX=SNAP_
```

6 Save the snapplan file and exit.

7 View the snapplan.

```
# cat snap1
SNAPSHOT_VERSION=5.0
PRIMARY_HOST=host1
SECONDARY_HOST=host1
PRIMARY_DG=PRODdg1
ORACLE_SID=PROD
ARCHIVELOG_DEST=/prod_ar
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=2
SNAPSHOT_DG_PREFIX=SNAP_
```

8 Proceed to re-validate the snapplan.

Migrating from /etc/vx/vxdba to /var/vx/vxdba for Oracle

If you are upgrading Veritas Storage Foundation for Oracle, you can migrate to `/var/vx/vxdba` to save space under the root partition. Migrating to `/var/vx/vxdba` is optional. However, if you do not perform this migration, you cannot remove any file or directory from `/etc/vx/vxdba` to ensure proper operation. This procedure can be done at any time.

To migrate from /etc/vx/vxdba to /var/vx/vxdba

1 Copy the `/etc/vx/vxdba` directory and contents to `/var/vx/vxdba`.

```
# cp -rp /etc/vx/vxdba /var/vx/vxdba
```

2 Remove /etc/vx/vxdba.

```
# rm -rf /etc/vx/vxdba
```

3 Link the two directories.

```
# ln -s /var/vx/vxdba /etc/vx/vxdba
```

Optional configuration steps

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

You can perform the following optional configuration steps:

- If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:
  - Reattach the RLINKs.
  - Associate the SRL.
- To encapsulate and mirror the boot disk, follow the procedures in the "Administering Disks" chapter of the *Veritas Volume Manager Administrator's Guide*.
- If you want to use features of Veritas Storage Foundation 5.0.1 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 127.

About upgrading disk layout versions

You must upgrade your older disk layout versions to make use of the extended features available in theVeritas File System 5.0.1 release.

See the *Veritas Storage Foundation Release Notes 5.0.1* for information on new features.

Use the `vxfsconvert` or `vxupgrade` utilities to upgrade older disk layout versions to disk layout Version 7.

Warning: Never upgrade the `/` and `/stand` file systems to disk layout Version 7. The HP-UX bootloader does not support disk layout Version 7.

Upgrading VxFS disk layout versions

Veritas File System 5.0.1 allows Version 4, 5, 6 and 7 for locally mounted file systems and disk layout Versions 6 and 7 for cluster mounted file systems. If you have cluster-mounted file systems with disk layout Versions lower than 6, then after upgrading to VxFS 5.0.1, upgrade the disk layout. Perform the following additional steps to prepare the file system for being mounted on all nodes of the cluster.

Disk layout Versions 1, 2, and 3 are not supported by VxFS 5.0.1. All file systems created on VxFS 5.0.1 use disk layout Version 7 by default.

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

To upgrade VxFS disk layout versions

1. Select one of the nodes of the cluster and mount the file system locally on this node. Use the `mount`, but without the `-o cluster` option. For example:

   ```
   # mount -F vxfs /dev/vx/dsk/sharedg/vol1 /mnt1
   ```

2. To find the current disk layout version on a file system:

   ```
   # fstyp -v <char_device_path> | grep version | \
     awk '{print $2}'
   ```

3. On the node selected in step 1, incrementally upgrade the disk layout of this file system to layout Version 6 or 7.

   For example, if you had a cluster mounted file system of disk layout Version 4 running with previous version of VxFS, after upgrading to VxFS 5.0.1, you would need to upgrade the disk layout to Version 6 or 7. The incremental upgrade is as follows:

   ```
   # vxupgrade -n 5 /mnt1
   # vxupgrade -n 6 /mnt1
   # vxupgrade -n 7 /mnt1
   ```

4. On the node selected in step 1, after the disk layout has been successfully upgraded, unmount the file system:

   ```
   # umount /mnt1
   ```

5. This file system can be mounted on all nodes of the cluster.

When to use vxfsconvert

You can use the `vxfsconvert` command to convert an unmounted HFS file system to a Veritas file system with disk layout Version 7.

```
# vxfsconvert /device_name
```

See the `vxfsconvert`(1M) and `fsadm_vxfs`(1M) manual pages.

When to use vxupgrade

You can use the `vxupgrade` command to upgrade older VxFS disk layouts to disk layout Version 7 while the file system remains mounted.

```
# vxupgrade -n 7 /mount_point
```

See the `vxupgrade`(1M) and `fsadm_vxfs`(1M) manual pages.

Warning: The contents of intent logs created on a previous disk layout version cannot be used after the disk layout version is upgraded.

Requirements for upgrading to disk layout Version 7

Converting a previous disk layout to a Version 7 disk layout requires adequate free space. The space and time required to complete the upgrade increases with the number of files, extended attributes, and hard links in the file system. Typical maximum space is at least two additional inodes with one block for every inode. Allow at least ten minutes to upgrade for every million inodes in the file system.

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 and 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, you need to upgrade existing disk groups.

After upgrading from Storage Foundation 4.x to 5.0.1, you must upgrade any existing disk groups which are organized by ISP. Without the version upgrade, configuration query operations continue to work fine. However, configuration change operations will not function correctly.

For 5.0.1, the Veritas Volume Manager disk group version is the same as it was for the VxVM 5.0 release. Upgrading the disk group version is only required if you upgraded from a version earlier than 5.0.

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 Volume Manager 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

In releases prior to Volume Manager 4.0, the default disk group was `rootdg` (the root disk group). For Volume Manager to function, the `rootdg` disk group had to exist and it had to contain at least one disk.

This requirement no longer exists; however, you may find it convenient to create a system-wide default disk group. 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 Volume Manager Administrator's Guide*.

If you want to confirm that the root disk is encapsulated, enter the command:

```
# vxdg bootdg
```

Upgrading the Array Support Library

VxVM provides support for new disk arrays in the form of Array Support Library (ASL) software package.

Converting from QuickLog to Multi-Volume support

The 4.1 release of the Veritas File System is the last major release to support QuickLog. The Version 6 or Version 7 disk layout does not support QuickLog. The functionality provided by the Veritas Multi-Volume Support (MVS) feature replaces most of the functionality provided by QuickLog.

The following procedure describes how to convert from QuickLog to MVS. Unlike QuickLog, which allowed logging of up to 31 VxFS file systems to one device, MVS allows intent logging of only one file system per device. Therefore, the following

procedure must be performed for each file system that is logged to a QuickLog device if Version 6 or Version 7 disk layout is used.

The QuickLog device did not need to be related to the file system. For MVS, the log volume and the file system volume must be in the same disk group.

To convert Quicklog to MVS

1. Select a QuickLog-enabled file system to convert to MVS and unmount it.

   ```
   # umount myfs
   ```

2. Detach one of the QuickLog volumes from the QuickLog device that the file system had been using. This volume will be used as the new intent log volume for the file system.

   ```
   # qlogdetach -g diskgroup log_vol
   ```

3. Create the volume set.

   ```
   # vxvset make myvset myfs_volume
   ```

4. Mount the volume set.

   ```
   # mount -F vxfs /dev/vx/dsk/rootdg/myvset /mnt1
   ```

5. Upgrade the volume set's file system to Version 6 or Version 7 disk layout.

   See "About upgrading disk layout versions" on page 125.

   For example:

   ```
   # vxupgrade -n 6 /mnt1
   ```

6. Add the log volume from step 2 to the volume set.

   ```
   # vxvset addvol myvset log_vol
   ```

7. Add the log volume to the file system. The size of the volume must be specified.

   ```
   # fsvoladm add /mnt1 log_vol 50m
   ```

8. Move the log to the new volume.

   ```
   # fsadm -o logdev=log_vol,logsize=16m /mnt1
   ```

Chapter 7

Verifying the Storage Foundation installation

This chapter includes the following topics:

Verifying that the products were installed

Verify that the Veritas Storage Foundation products are installed.

You can use the `swlist` command to check which packages have been installed:

```
# swlist -l product | grep VRTS
```

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 response file

The response file contains the configuration information that you entered during the procedure. 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.

Using the summary file

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

Checking 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 -e | grep vx
  ```

  Entries for the `vxiod`, `vxconfigd`, `vxnotify`, `vxesd`, `vxrelocd`, `vxpal`, `vxcached`, `vxconfigbackupd`, and `vxsvc` processes should appear in the output from this command. If you disable hot-relocation, the `vxrelocd` and `vxnotify` processes are not displayed.

  If you installed Storage Foundation for Oracle, the `vxodmd` and `vxdbd_11.31` processes are also displayed.

Checking Veritas File System installation

The Veritas File System package consists of a kernel component and administrative commands.

Command installation verification

The Veritas File System commands are installed in the `/opt/VRTS/bin` directory. To verify, determine that the subdirectory is present:

```
# ls /opt/VRTS/bin
```

Make sure you have adjusted your environment variables accordingly.

See "Setting environment variables" on page 19.

Chapter 8

Uninstalling Storage Foundation

This chapter includes the following topics:

Summary of Veritas Storage Foundation uninstallation tasks

Complete the following preparations to uninstall a Storage Foundation product.

Warning: Failure to follow the preparations that are outlined in this chapter can result in loss of data.

Uninstallation of Veritas Storage Foundation consists of the following tasks:

- Dropping the repository database if you are uninstalling Veritas Storage Foundation for Oracle.
- Shutting down cluster operations.
- Removing the root disk from VxVM control.
- Removing VxFS file systems and Storage Checkpoints.
- Moving volumes to disk partitions.
- Removing the Veritas Storage Foundation depots.
- Removing the license files (optional).

Warning: Failure to follow the instructions in the following sections may result in unexpected behavior.

Once you uninstall Veritas Volume Manager, you will be left without volume management software on your machine.

To uninstall Veritas Storage Foundation and Veritas Storage Foundation for Oracle, refer to the appropriate procedure.

See "Uninstalling Veritas Storage Foundation packages" on page 145.

Dropping the repository database for Oracle

When uninstalling Veritas Storage Foundation for Oracle, drop the repository database. If you want to recreate the repository database, you can drop the existing repository database using these steps.

To drop the repository database in a stand-alone configuration

1 Make sure the repository database volume is mounted using the `df` command.

If the repository database volume is not mounted, run the `sfua_rep_mount` command to mount the volume:

```
# /sbin/init.d/sfua_rep_mount start
```

2 Use the `sfua_db_config` command with the `-o dropdb` option to remove the database.

```
# /opt/VRTS/bin/sfua_db_config -o dropdb
```

To drop the repository database in an Oracle cluster or Oracle RAC configuration

1 Drop the repository database from the VCS configuration and deport the repository disk group.

```
# /opt/VRTS/bin/sfua_db_config -o unconfig_cluster
```

2 Import the repository database disk group.

```
# /opt/VRTS/bin/vxdg import repository_diskgroup_name
```

3 Run the `sfua_rep_mount` command to mount the repository database volume.

```
# /sbin/init.d/sfua_rep_mount start
```

4 Use the `sfua_db_config` command with the `-o dropdb` option to remove the database.

```
# /opt/VRTS/bin/sfua_db_config -o dropdb
```

5 Remove the mount point for the database repository.

```
# /sbin/init.d/sfua_rep_mount stop
```

Shutting down cluster operations

If the systems are running as an HA cluster, you have to take all service groups offline and shutdown VCS.

To take all service groups offline and shutdown VCS

- Use the `hastop` command as follows:

```
# /opt/VRTSvcs/bin/hastop -all
```

Warning: Do not use the `-force` option when executing `hastop`. This will leave all service groups online and shut down VCS, causing undesired results during uninstallation of the packages.

Removing VxFS file systems and Storage Checkpoints

It is advisable to unmount any user VxFS file systems before uninstalling VxFS to help smooth uninstallation of VxVM package if VxFS file system is mounted on VxVM volumes. System partitions need not be unmounted as part of this operation. After you remove the `VRTSvxfs` package, VxFS file systems versions greater than those supported by OnlineJFS bundled with the HP-UX operating system are not mountable or accessible until another `VRTSvxfs` package supporting them is installed.

To unmount a file system

1. Check if any VxFS file systems are mounted.

```
# cat /etc/mnttab | grep vxfs
```

2. Unmount any file systems that are not system partitions.

```
# umount special | mount_point
```

Specify the file system to be unmounted as a *mount_point* or *special* (the device on which the file system resides).

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

If using VxFS file system, system partitions need not be unmounted.

To unmount a Storage Checkpoint

1. Check if any Storage Checkpoints are mounted.

```
# cat /etc/mnttab | grep vxfs
```

2. Unmount any Storage Checkpoints.

```
# umount /checkpoint_name
```

Removing the root disk from VxVM control

If the system's root disk is under VxVM control, use the following command to copy its contents to a new LVM root disk:

```
# /etc/vx/bin/vxres_lvmroot -v -b [-p c#t#d#2,c#t#d#3,...] c#t#d#
```

where `c#t#d#` is the access name of the new LVM root disk. If the root disk volumes are distributed over several disks, use the `-p` option to specify a comma-separated list of additional disks that are to be used to set up the LVM root volume group. The operation to clone a new LVM root volume group can take some time, so the `-v` (verbose) option is specified to show how far this has progressed.

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 for HP-UX

Use the following procedure to move volumes to disk partitions.

To move volumes to disk partitions

1. Evacuate disks using `vxdiskadm`, the GUI, or the `vxevac` script.

   Evacuation moves subdisks from the specified disks to target disks. The evacuated disks provide the initial free disk space for volumes to be moved to disk partitions.

2. Remove the evacuated disks from VxVM control by entering:

   ```
   # vxdg rmdisk diskname
   # vxdisk rm devname
   ```

3. Decide which volume to move first, and if the volume is mounted, unmount it.

4 If the volume is being used as a raw partition for database applications, make sure that the application is not updating the volume and that you have applied the `sync` command to the data on the volume.

5 Create a partition on free disk space of the same size as the volume using the `format` command.

If there is not enough free space for the partition, add a new disk to the system for the first volume removed. Subsequent volumes can use the free space generated by the removal of this first volume.

6 Copy the data on the volume onto the newly created disk partition using a command such as `dd`.

```
# dd if=/dev/vx/dsk/diskgroup/lhome of=/dev/dsk/c2t2d2
```

where `c2t2d2` is the disk outside of Volume Manager.

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 Remove the volume from VxVM using the command.

```
# vxedit -rf rm volume_name
```

10 Remove any free disks (those having no subdisks defined on them) by removing the volumes from VxVM control.

To check if there are still some subdisks remaining on a particular disk, use the `vxprint` command.

```
# vxprint -F '%sdnum' diskname
```

If the output is not 0, there are still some subdisks on this disk that you need to remove. If the output is 0, remove the disk from VxVM control.

```
# vxdg rmdisk diskname
# vxdisk rm devname
```

Use the free space created for adding the data from the next volume you want to remove.

11 After you successfully convert all volumes into disk partitions, reboot the system.

12 After the reboot, make sure none of the volumes are open by using the `vxprint` command.

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

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

Example of moving volumes to disk partitions on HP-UX

This example shows how to move the data on a volume to a disk partition. In the example, there are three disks: `disk1` and `disk2` are subdisks on volume `vol01` and `disk3` is a free disk. The data on `vol01` is copied to `disk3` using `vxevac`.

Diskgroup `voldg` content before the data on `vol01` is copied to `disk3`.

```
# vxprint -g voldg -ht
```

```
DG NAME         NCONFIG      NLOG     MINORS   GROUP-ID
DM NAME         DEVICE       TYPE     PRIVLEN  PUBLEN   STATE
RV NAME         RLINK_CNT    KSTATE   STATE    PRIMARY  DATAVOLS  SRL
RL NAME         RVG          KSTATE   STATE    REM_HOST REM_DG    REM_RLNK
V  NAME         RVG          KSTATE   STATE    LENGTH   READPOL   PREFPLEX
UTYPE
PL NAME         VOLUME       KSTATE   STATE    LENGTH   LAYOUT    NCOL/WID
MODE
SD NAME         PLEX         DISK     DISKOFFS LENGTH   [COL/]OFF DEVICE
MODE
SV NAME         PLEX         VOLNAME  NVOLLAYR LENGTH   [COL/]OFF AM/NM
MODE
DC NAME         PARENTVOL    LOGVOL
SP NAME         SNAPVOL      DCO

dg voldg        default      default  115000
1017856044.1141.hostname.veritas.com

dm disk1        c1t12d0  auto:hpdisk   2591     17900352 -
dm disk2        c1t14d0  auto:hpdisk   2591     17899056 -
dm disk3        c1t3d0   auto:hpdisk   2591     17899056 -

v  vol1         -            ENABLED  ACTIVE   4196448  ROUND     -
fsgen
pl pl1          vol1         ENABLED  ACTIVE   4196448  CONCAT    -
```

```
RW
sd sd1          pl1          disk1    0        2098224  0         c1t12d0
ENA
sd sd2          pl1          disk2    0        2098224  2098224   c1t14d0
ENA
```

Evacuate `disk1` to `disk3`.

```
# /etc/vx/bin/vxevac -g voldg disk1 disk3
# vxprint -g voldg -ht
```

```
DG NAME         NCONFIG      NLOG     MINORS   GROUP-ID
DM NAME         DEVICE       TYPE     PRIVLEN  PUBLEN   STATE
RV NAME         RLINK_CNT    KSTATE   STATE    PRIMARY  DATAVOLS  SRL
RL NAME         RVG          KSTATE   STATE    REM_HOST REM_DG    REM_RLNK
V  NAME         RVG          KSTATE   STATE    LENGTH   READPOL   PREFPLEX
UTYPE
PL NAME         VOLUME       KSTATE   STATE    LENGTH   LAYOUT    NCOL/WID
MODE
SD NAME         PLEX         DISK     DISKOFFS LENGTH   [COL/]OFF DEVICE
MODE
SV NAME         PLEX         VOLNAME  NVOLLAYR LENGTH   [COL/]OFF AM/NM
MODE
DC NAME         PARENTVOL    LOGVOL
SP NAME         SNAPVOL      DCO

dg voldg        default      default  115000
1017856044.1141.hostname.veritas.com

dm disk1        c1t12d0  auto:hpdisk   2591     17900352 -
dm disk2        c1t14d0  auto:hpdisk   2591     17899056 -
dm disk3        c1t3d0   auto:hpdisk   2591     17899056 -

v  vol1         -            ENABLED  ACTIVE   4196448  ROUND     -
fsgen
pl pl1          vol1         ENABLED  ACTIVE   4196448  CONCAT    -
RW
sd disk3-01     pl1          disk3    0        2098224  0         c1t3d0
ENA
sd sd2          pl1          disk2    0        2098224  2098224   c1t14d0
ENA
```

Evacuate `disk2` to `disk3`.

```
# /etc/vx/bin/vxevac -g voldg disk2 disk3
# vxprint -g voldg -ht
```

```
DG NAME         NCONFIG      NLOG     MINORS   GROUP-ID
DM NAME         DEVICE       TYPE     PRIVLEN  PUBLEN   STATE
RV NAME         RLINK_CNT    KSTATE   STATE    PRIMARY  DATAVOLS  SRL
RL NAME         RVG          KSTATE   STATE    REM_HOST REM_DG    REM_RLNK
V  NAME         RVG          KSTATE   STATE    LENGTH   READPOL   PREFPLEX
UTYPE
PL NAME         VOLUME       KSTATE   STATE    LENGTH   LAYOUT    NCOL/WID
MODE
SD NAME         PLEX         DISK     DISKOFFS LENGTH   [COL/]OFF DEVICE
MODE
SV NAME         PLEX         VOLNAME  NVOLLAYR LENGTH   [COL/]OFF AM/NM
MODE
DC NAME         PARENTVOL    LOGVOL
SP NAME         SNAPVOL      DCO

dg voldg        default      default  115000
1017856044.1141.hostname.veritas.com

dm disk1        c1t12d0  auto:hpdisk   2591     17900352 -
dm disk2        c1t14d0  auto:hpdisk   2591     17899056 -
dm disk3        c1t3d0   auto:hpdisk   2591     17899056 -

v  vol1         -            ENABLED  ACTIVE   4196448  ROUND     -
fsgen
pl pl1          vol1         ENABLED  ACTIVE   4196448  CONCAT    -
RW
sd disk3-01     pl1          disk3    0        2098224  0         c1t3d0
ENA
sd disk3-02     pl1          disk3    2098224  2098224  2098224   c1t3d0
ENA
```

Remove the evacuated disks from VxVM control.

```
# vxdisk -g voldg list
DEVICE       TYPE                    DISK         GROUP        STATUS
c1t3d0              auto:hpdisk           disk3        voldg
online
c1t12d0            auto:hpdisk           disk1        voldg
online
c1t14d0            auto:hpdisk           disk2        voldg
online
```

```
# vxdg rmdisk disk1
# vxdg rmdisk disk2
# vxdisk rm c1t12d0
# vxdisk rm c1t14d0
```

Verify that the evacuated disks have been removed from VxVM control.

```
# vxdisk -g voldg list
DEVICE       TYPE              DISK    GROUP     STATUS
c1t3d0       auto:hpdisk      disk3    voldg     online
```

Check to see whether the volume you want to move first is mounted.

```
# mount | grep vol1
/vol1 on /dev/vx/dsk/voldg/vol1
read/write/setuid/log/nolargefiles/dev=12dc138 on Wed Apr  3
10:13:11 2002
```

Copy the data on `vol01` to the newly created disk partition.

```
# dd if=/dev/vx/dsk/voldg/vol01 of=/dev/dsk/c1t12d0
```

In the `/etc/fstab` file, remove the following entry.

```
/dev/vx/dsk/voldg/vol1 /dev/vx/rdsk/voldg/vol1 /vol1 vxfs 4
yes rw
```

Replace it with an entry for the newly created partition.

```
/dev/dsk/c1t12d0 /dev/rdsk/c1t12d0 /vol01 vxfs 4  yes rw
```

Mount the disk partition.

```
# mount -F vxfs /dev/dsk/c1t12d0 /vol01
```

Remove `vol01` from VxVM.

```
# vxedit -rf rm /dev/vx/dsk/voldg/vol01
```

To complete the procedure, perform the remaining steps.

Shutting down Veritas Volume Manager

Use the following procedure to shut down Veritas Volume Manager.

To shut down Veritas Volume Manager

- Enter the `vxdctl` and `vxiod` commands as follows:

```
# vxdctl stop
# vxiod -f set 0
```

Uninstalling Veritas Storage Foundation packages

Use the following procedure to shut down and remove the installed Veritas Storage Foundation packages.

To shut down and remove the installed Veritas Storage Foundation packages

1. In a stand-alone configuration, if you are uninstalling Veritas Storage Foundation for Oracle, stop the repository database and unmount the database repository volume.

   ```
   # /opt/VRTS/bin/sfua_db_config -o stopdb
   ```

   ```
   # /sbin/init.d/sfua_rep_mount stop
   ```

2. In an HA configuration, stop VCS processes on either the local system or all systems.

   To stop VCS processes on the local system:

   ```
   # hastop -local
   ```

   To stop VCS processes on all systems:

   ```
   # hastop -all
   ```

3. Move to the /opt/VRTS/install directory and run the uninstall script.

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

   For Veritas Storage Foundation

   ```
   # ./uninstallsf
   ```

   For Veritas Storage Foundation for Oracle

   ```
   # ./uninstallsfora
   ```

   You can use these commands to remove the packages from one or more systems.

   To remove packages from remote systems, configure `ssh` or `rsh`.

   See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

   Not all these packages may be installed on your system depending on the choices that you made when you installed VxVM.

   If you have obtained a Veritas product from an electronic download site, the single product download files do not contain the `uninstallsf` installation script, so you must use the product uninstallation script to uninstall the product. For example, if you download Veritas Volume Manager, use the `uninstallvm` script instead of the `uninstallsf` script.

Uninstalling Veritas Volume Manager

This section describes how to uninstall Veritas Volume Manager and the product license.

To uninstall Veritas Storage Foundation or Veritas Storage Foundation for Oracle, use the Storage Foundation procedure.

See "Uninstalling Veritas Storage Foundation packages" on page 145.

To uninstall Veritas Volume Manager

1. Log in as superuser.
2. Run the `installer` command to uninstall Veritas Volume Manager. For example:

```
# cd /dvdrom
# ./installer
```

3. From the product installer, choose the `U` option for Uninstall, and select `Veritas Volume Manager`.
4. Enter one or more system names from which Veritas Volume Manager is to be uninstalled. For example:

```
Enter the system names separated by spaces on which to
uninstall VxVM: system01
```

5. After the system check completes successfully, press Return to continue.
6. Enter `y` to uninstall the VxVM depots. For example:

```
Are you sure you want to uninstall VxVM? [y,n,q] (y)
```

7. After VxVM is successfully stopped, the system will tell you the location of log files. You should save these files for future reference.
8. After uninstallation completes, reboot the system.

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

Uninstalling the VCS agents for VVR

To uninstall the VCS Agents for VVR, you must first disable the agents.

If VCS Agents for VVR are not installed on your system, go to Uninstalling Veritas Volume Replicator (VVR).

Disabling the agents on a system

This section explains how to disable a VCS agent for VVR on a system. To disable an agent, you must change the service group containing the resource type of the agent to an OFFLINE state. Then, you can stop the application or switch the application to another system.

To disable the agents

1. Check whether any service group containing the resource type of the agent is online by typing the following command:

   ```
   # hagrp -state service_group -sys system_name
   ```

   If none of the service groups is online, skip to 3.

2. If the service group is online, take it offline.

   To take the service group offline without bringing it online on any other system in the cluster, enter:

   ```
   # hagrp -offline service_group -sys system_name
   ```

3. Stop the agent on the system by entering:

   ```
   # haagent -stop agent_name -sys system_name
   ```

   When you get the message `Please look for messages in the log file`, check the file `/var/VRTSvcs/log/engine_A.log` for a message confirming that each agent has stopped.

   You can also use the `ps` command to confirm that the agent is stopped.

4. Remove the system from the `SystemList` of the service group. If you disable the agent on all the systems in the `SystemList`, you can also remove the service groups and resource types from the VCS configuration.

   Read information on administering VCS from the command line.

   Refer to the *Veritas Cluster Server User's Guide*.

Uninstalling Veritas Volume Replicator (VVR)

This section describes how to uninstall Volume Replicator.

Note: If you are upgrading Veritas Volume Replicator, do not remove the Replicated Data Set, but only remove the VVR packages.

Uninstalling Veritas Volume Replicator (VVR) involves performing the following tasks in the order indicated:

- Removing the Replicated Data Set
- Removing the VVR packages

For more information about VVR commands, refer to the *Veritas Volume Replicator Administrator's Guide*.

Removing the Replicated Data Set

This section gives the steps to remove a Replicated Data Set (RDS) when the application is either active or stopped.

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.

Go on to uninstalling Volume Manager to uninstall VVR.

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
```

6 Uninstall the VVR packages.

See "Removing the VVR packages" on page 150.

Removing the VVR packages

Use the uninstall program to remove the VVR software packages.

To remove the VVR packages

1 Insert the software disc, mount it, and enter the following commands:

```
# cd /disc_path/depot

# ./installer
```

2 Select Uninstall from the menu.

3 Select VVR.

The program prompts you to confirm whether you want to remove the packages that are being used by other Veritas products.

4 Answer the set of questions depending on your requirements. Note that if you uninstall the `VRTSvxvm` package you will not be able to use the Veritas Volume Manager functionality.

The program asks you to confirm that you want to remove VVR and then removes all the packages except the infrastructure packages. If open volumes exist, the program prompts you to stop the open volumes and unmount the file systems.

The output is similar to the following:

```
uninstallvvr is now ready to uninstall VVR packages.
All VVR processes that are currently running will be stopped.
Are you sure you want to uninstall VVR packages? [y,n,q] (y)
```

5 Press Return to continue.

6 Confirm the depots have been removed.

```
# swlist | grep VRTS
```

If you do not have any other Veritas products installed on the system, you can remove the `/etc/vx` directory, the `/usr/lib/vxvm` directory, and the `/opt/VRTS*` directories.

Additional ways to remove VVR packages

Before removing the packages, determine whether any other Veritas products are installed on your system. Other products might depend on the packages you may be removing. A warning appears when you try to remove packages that are being used by other products.

To remove the VVR packages using the swremove command

1. Use the `swremove` command to remove the installed Veritas Volume Replicator software packages. Remove the packages in the order shown:

   ```
   # swremove VRTSvmdoc VRTSvrdoc VRTSvmman VRTSvcsvr VRTSap VRTStep
   ```

   You can also include `VRTSvlic` in the removal line, if you have not installed any other packages that use `VRTSvlic`.

2. Remove the Veritas Provider Packages, Veritas Virtual Disk Management Services Provider and Veritas Volume Replicator Management Services Provider, use the following commands:

   ```
   # swremove VRTSvmpro

   # swremove VRTSvrpro
   ```

3. Remove the Veritas Enterprise Administrator packages using the following commands:

   ```
   # swremove VRTSob

   # swremove VRTSobgui
   ```

4. Remove the Windows Client software. Perform the following tasks in the order indicated:

   - Click **Start > Settings > Control Panel > Add/Remove Software**
   - Choose Veritas Enterprise Administrator for removal.

5. Remove the Veritas Volume Replicator Web GUI (VRW) Application package:

   ```
   # swremove VRTSvrw
   ```

Note: The Veritas Web GUI Engine, `VRTSweb` is used by other Veritas products, such as GCM or QuickStart, that have Web GUIs. Do not perform 6 if you have other Veritas products with Web GUIs installed on your system.

---

6 Remove the Veritas Web GUI Engine `VRTSweb` by entering the following command:

```
# swremove VRTSweb
```

7 Remove `VRTSvxvm`.

For instructions, see the *Veritas Storage Foundation Installation Guide*.

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 Veritas Enterprise Administrator client

You should also remove the client software from any machines you used to access the Veritas software.

To remove the VEA client from an HP-UX system other than the server

1 Stop the VEA Service.

```
# /opt/VRTS/bin/vxsvcctrl stop
```

2 Use the `swremove` command to remove the VEA client packages.

```
# swremove VRTSobgui VRTSat VRTSpbx VRTSicsco
```

To remove the VEA client from a Windows system

1. Log in as the database administrator.
2. Select **Start > Settings > Control Panel**.
3. Double-click **Add/Remove Programs** to display a list of installed products.
4. Select **Veritas Enterprise Administrator** from the list, and click the **Remove** button.
5. Click **Yes** when a dialog box appears asking you to confirm the removal.

Appendix A

Installation scripts

This appendix includes the following topics:

About installation scripts

Veritas Storage Foundation and High Availability Solutions 5.0.1 provides several installation scripts.

To install a fresh installation on a system, or to upgrade from Veritas Storage Foundation and High Availability Solutions version prior to 5.0.1, the recommended installation method is to use the common product installer. To use the common product installer, run the `installer` command.

See "About the common product installer" on page 37.

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

The following product installation scripts are available:

Veritas Cluster Server (VCS)	`installvcs`
Veritas Volume Replicator (VVR)	`installvvr`
Veritas Storage Foundation (SF)	`installsf`
Veritas Storage Foundation for Oracle (SFORA)	`installsfora`

Veritas Storage Foundation Cluster File System (SFCFS)	`installsfcfs`
Veritas Storage Foundation for Oracle RAC (SFRAC)	`installsfrac`
Symantec Product Authentication Service (AT)	`installat`
Veritas Volume Manager	`installvm`

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

Installation script options

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

See "About installation scripts" on page 155.

Table A-1 Available command line options

Command Line Option	Function
system1 system2...	Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.
–configure	Configures the product after installation.
–enckeyfile *encryption_key_file*	Specifies the location of a file containing the key to decrypt encrypted passwords stored in response files. See the `-responsefile` and the `-encrypt` options.
–encrypt *password*	Encrypts *password* using the encryption key provided with the `-enckeyfile` option so that the encrypted password can be stored in response files.
-hostfile *full_path_to_file*	Specifies the location of a file that contains a list of hostnames on which to install.

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

Command Line Option	Function
–installpkgs	Displays all product packages in correct installation order. Output can be used to create scripts for command line installs, or for installations over a network. See the `requiredpkgs` option.
–installonly	Installs packages, but does not configure the product.
–keyfile *ssh_key_file*	Specifies a key file for secure shell (SSH) installs. This option passes `-i ssh_key_file` to every SSH invocation.
–license	Registers or updates product licenses on the specified systems.
–logpath *log_path*	Specifies a directory other than `/opt/VRTS/install/logs` as the location where installer log files, summary files, and response files are saved.
–noextrapkgs	Additional packages can be installed so that you can upgrade to another Symantec product simply by installing a new license. The `noextrapkgs` option bypasses installation of extra product packages to simplify future maintenance updates.
-nohapkgs	Limits the list of Storage Foundation packages to exclude the Veritas Cluster Server packages. This option only applies to the `installsf` script when one of the following options is specified: ■ -installpkgs ■ -requiredpkgs ■ -jumpstart
–nolic	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
–nooptionalpkgs	Bypasses installation of optional product packages such as manual pages.

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

Command Line Option	Function
–nostart	Bypasses startup of the product following installation and configuration.
–pkgpath *package_path*	Designates the path of a directory that contains all packages to install. The directory is typically an NFS-mounted location and must be accessible by all specified installation systems.
–precheck	Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.
–requiredpkgs	Displays all required product packages in correct installation order. Optional packages are not listed. Output can be used to create scripts for command line installs, or for installations over a network. See `installpkgs` option.
–responsefile *response_file* [–enckeyfile *encryption_key_file*]	Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. The `-enckeyfile` option and *encryption_key_file* name are required with the `-responsefile` option when the response file contains encrypted passwords.
–rootpath *root_path*	Specifies an alternative root directory on which to install packages. On HP-UX operating systems, `-rootpath` passes `-I path` to `swinstall`.
–rsh	Specify this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP. See "Configuring secure shell (ssh) or remote shell before installing products" on page 20.

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

Command Line Option	Function
-security	Enable or disable Symantec Product Authentication Service in a VCS cluster that is running. Install and configure Root Broker for Symantec Product Authentication Service. You can specify this option with the `installvcs`, `installsf` or `installsfcfs` scripts. For more information about Symantec Product Authentication Service in a VCS cluster, see the *Veritas Cluster Server Installation Guide*.
-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.
-timeout *timeout_value*	Specifies the timeout (in seconds) that the installer uses for each command it issues during the installation. The default timeout is set to 600 secs. Use the -timeout option to override the default value.
–tmppath *tmp_path*	Specifies a directory other than `/var/tmp` as the working directory for the installation scripts. This destination is where initial logging is performed and where packages are copied on remote systems before installation.
-verbose	Displays details during installation of product depots. By default, the installation displays only a progress bar.

Appendix B

Storage Foundation and High Availability components

This appendix includes the following topics:

Veritas Storage Foundation installation depots

Table B-1 shows the depot name and contents for each English language depot for Veritas Storage Foundation, Veritas Storage Foundation High Availability, Veritas Storage Foundation Cluster File System, and Veritas Storage Foundation for databases.

Table B-1 Storage Foundation depots

depot	Contents	Required/Optional
Veritas Volume Manager		
VRTSalloc	Veritas Volume Manager Veritas Intelligent Storage Provisioning Provides the volume tagging features, which is required for dynamic storage tiering (DST).	Required

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSddlpr	Veritas Device Discovery Layer Services Provider Provides the necessary management backend required to administer Veritas Volume Manager (VxVM) Dynamic Multipathing (DMP) features and objects like enclosures, controllers, and paths from the GUI.	Required
VRTSvdid	Veritas Device Identification API	Required
VRTSvmpro	Veritas Volume Manager Management Services Provider Provides the necessary management backend required to administer VxVM from the GUI.	Required
VRTSvxvm	Veritas Volume Manager binaries	Required
Veritas File System		
VRTSfsman	Veritas File System manual pages	Optional
VRTSfsmnd	Veritas File System Software Developer Kit manual pages	Optional
VRTSfspro	Veritas File System Management Services Provider Provides the necessary management for administering VxFS and other platform file systems from the GUI. Also, provides Dynamic Storage Tiering (DST) capability that allows users to do policy-based control for data placement.	Required

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSfssdk	Veritas File System Software Developer Kit For VxFS APIs, the package contains the public Software Developer Kit (SDK), which includes headers, libraries, and sample code. The SDK is required if some user programs use VxFS APIs.	Required
VRTSvxfs	Veritas File System binaries Required for VxFS file system support.	Required
Storage Foundation Cluster File System		
VRTScavf	Veritas Cluster Server Agents for Storage Foundation Cluster File System	Required
VRTSglm	Veritas Group Lock Manager for Storage Foundation Cluster File System	Required
VRTSgms	Veritas Group Messaging Services for Storage Foundation Cluster File System	Required
Databases		
VRTSdbcom	Veritas Storage Foundation Common Utilities for Databases	Required (for Storage Foundation for databases)
VRTSdbed	Veritas Storage Foundation for Oracle	Required (for Storage Foundation for Oracle)

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSodm	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 Oracle9i and 10g to improve performance and manage system bandwidth.	Required (for Storage Foundation for Oracle)
VRTSorgui	Veritas Storage Foundation for Oracle Graphical User Interface	Required (for Storage Foundation for Oracle)
VRTSvxmsa	Veritas Mapping Service, Application Libraries	Required (for Oracle product)
Veritas Enterprise Administrator		
VRTSaa	Veritas Enterprise Administrator Action Agent	Required
VRTSccg	Veritas Enterprise Administrator Central Control Grid	Required
VRTSob	Veritas Enterprise Administrator	Required
VRTSobc33	Veritas Enterprise Administrator Core	Required
VRTSobgui	Veritas Enterprise Administrator	Optional
Infrastructure		

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSat	Symantec Product Authentication Service Installs the Symantec Product Authentication Service, which provides authentication services to other Symantec products. This package contains a server and client component. The server provides services for a root broker, authentication broker, or both. The client allows Symantec products to communicate with the brokers.	Required
VRTSgapms	Veritas Generic Array Plugin	Required
VRTSicsco	Symantec Infrastructure Core Services Common	Required
VRTSvail	Veritas Array Integration Layer	Required
High Availability	Note: some of these depots are also required for Storage Foundation Cluster File System.	
VRTSacclib	Veritas Application Competency Center Library VRTSacclib is a set of Perl modules that many cluster server agents use.	Required Depends on VRTSvcs.
VRTScscm	Veritas Cluster Server Cluster Manager	Required Depends on VRTSvcs and VRTSjre15.
VRTScscw	Veritas Cluster Server configuration wizards	Required Depends on VRTSvcsag and VRTSjre15.
VRTScssim	Veritas Cluster Server Simulator	Optional
VRTScutil	Veritas Cluster Server Utilities	Required Depends on VRTSvcs.

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSgab	Veritas Cluster Server group membership and atomic broadcast services	Required Depends on VRTSllt.
VRTSjre15	Veritas Java Runtime Environment Redistribution This package installs the Java Runtime Environment for all Symantec products that require Java.	Required
VRTSllt	Veritas Cluster Server low-latency transport	Required
VRTSvcs	Veritas Cluster Server	Required Depends on VRTSut, VRTSperl, VRTSvxfen, VRTSgab, and VRTSllt.
VRTSvcsag	Veritas Cluster Server Bundled Agents	Required Depends on VRTSvcs.
VRTSvcsdb	Veritas High Availability Agent for DB2	Optional for VCS. Required to use VCS with the high availability agent for DB2. Depends on VRTSvcs.
VRTSvcsmg	Veritas Cluster Server English message catalogs	Required Depends on VRTSvcs.
VRTSvcsmn	Manual Pages for Veritas Cluster Server	Optional
VRTSvcsor	Veritas High Availability Agent for Oracle	Optional for VCS. Required to use VCS with the high availability agent for Oracle. Depends on VRTSvcs.

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSvcssy	Veritas High Availability Agent for Sybase	Optional for VCS. Required to use VCS with the high availability agent for Sybase. Depends on VRTSvcs.
VRTSvxfen	Veritas I/O Fencing	Required Depends on VRTSgab.
VRTSweb	Symantec Web Server	Required
Veritas Volume Replicator		
VRTSvcsvr	Veritas Cluster Server Agents for VVR	Required
VRTSvrpro	Veritas Volume Replicator Client Extension and Proivder for Veritas Enterprise Administrator	Required
Other depots		
VRTSdbms3	Veritas Shared DBMS	Required
VRTSdsa	Veritas Datacenter Storage Agent	Required
VRTSmapro	Veritas Storage Foundation GUI for Mapping	Required

Table B-1 Storage Foundation depots *(continued)*

depot	Contents	Required/Optional
VRTSpbx	Symantec Private Branch Exchange This package installs the Symantec Private Branch Exchange, which allows other Symantec products to share a common well-known port for publishing services and communicating.	Required If VRTSpbx is removed, Symantec products that use it are unable to communicate, which can cause the products to stop working. If VRTSat is configured to work with VRTSpbx, and VRTSpbx is removed, VRTSat continues to work. However, the Symantec Product Authentication Service remote administration functionality are not available. Removing VRTSat can affect Symantec products that use the Symantec Product Authentication Service remote administration feature, such as VEA.
VRTSperl	Perl 5.8.8 for Veritas	Required
VRTSspt	Veritas Software Support Tools	Required
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.	Required If VRTSvlic is removed, the Storage Foundation products may not be able to access their license information, The products may fail to start or fail to work properly.
windows/ vrtsobgui.msi	Veritas Enterprise Administrator for Windows	Optional

Obsolete packages in Storage Foundation 5.0.1

The following packages were included in previous releases of Storage Foundation but are now obsolete:

```
SYMClma
VRTSsmf
VRTScmcm
```

```
VRTSjre
VRTSvsvc
VRTSfsdoc
VRTSvmdoc
VRTSvrdoc
VRTSvcsdc
VRTSdbdoc
VRTScsdoc
VRTScfsdc
VRTSxrptl
VRTSdcli
VRTSmh
VRTScsocw
```

Index

V