Veritas Storage Foundation™ Cluster File System Installation Guide

HP-UX

5.0.1

Veritas Storage Foundation™ Cluster File System Installation Guide

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 Cluster File System

This chapter includes the following topics:

Veritas Storage Foundation Cluster File System suites

The following table lists the Symantec products and optionally licensed features available with each Veritas Storage Foundation Cluster File System (SFCFS) product suite.

Table 1-1 Contents of Veritas Storage Foundation Cluster File System products

Storage Foundation Cluster File System version	Products and features
Storage Foundation Cluster File System	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 Optionally licensed features: Veritas Volume Replicator

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

Storage Foundation Cluster File System version	Products and features
Storage Foundation Cluster File System 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 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 Cluster File System 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 Cluster File System will be installed.

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

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

- Veritas Storage Foundation Cluster File System
- Veritas Storage Foundation Cluster File System High Availability (HA)

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

See "Veritas Storage Foundation Cluster File System 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.

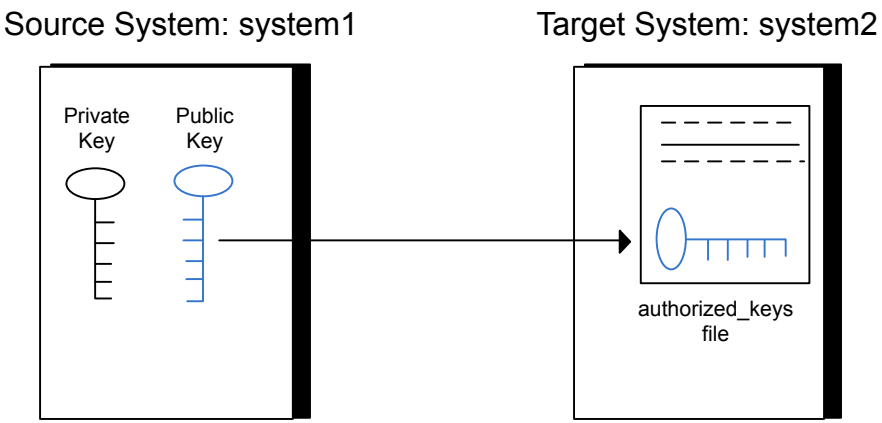
Configuring and enabling ssh

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.

Prerequisites for Storage Foundation Cluster File System

Each cluster node must be connected to the public network and each must have a unique host name by which it can be addressed on the public network. The local node from which you install does not have to be part of the cluster.

Provide the following information when installing the SFCFS:

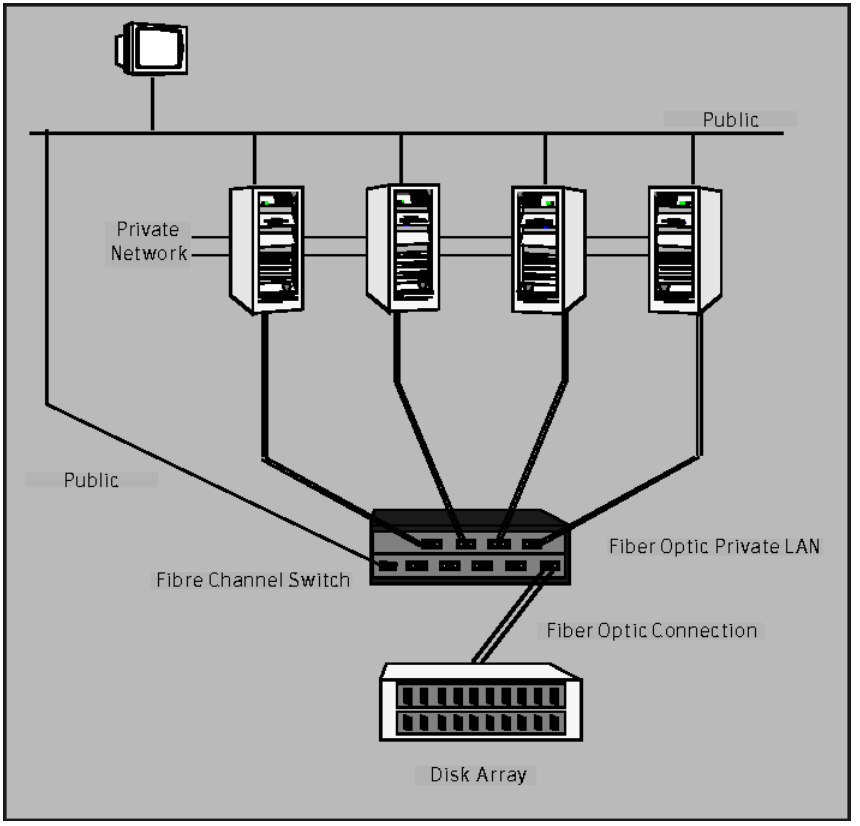
- The cluster name, beginning with a letter (a-z, A-Z).
- A unique ID from 0-65535 for the cluster. Within the public subnet, a new cluster using a duplicate cluster ID can cause existing clusters to fail.
- The host names of the cluster nodes.
- The device names of the network interface cards (NICs) used for the private networks among nodes.
- 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 `rsh` (remote shell) or `ssh` (secure shell) utilities as root on all cluster nodes or remote systems.
- Symantec recommends configuring the cluster with I/O fencing enabled. I/O fencing requires shared devices to support SCSI-3 Persistent Reservations (PR). Enabling I/O fencing prevents data corruption caused by a split brain scenario.
  The Storage Foundation Cluster File System is supported without I/O fencing enabled. However, without I/O fencing enabled, split brain scenarios can result in data corruption.

Hardware overview and requirements for Storage Foundation Cluster File System

VxFS cluster functionality runs optimally on a Fibre Channel fabric. Fibre Channel technology provides the fastest, most reliable, and highest bandwidth connectivity currently available. By employing Fibre Channel technology, SFCFS can be used in conjunction with the latest Veritas Storage Area Network (SAN) applications to provide a complete data storage and retrieval solution.

Figure 2-2 shows the configuration of a cluster file system on a Fibre Channel fabric with a disk array.

Figure 2-2 Four Node SFCFS Cluster Built on Fibre Channel Fabric



Shared storage

Shared storage can be one or more shared disks or a disk array connected either directly to the nodes of the cluster or through a Fibre Channel Switch. Nodes can also have non-shared or local devices on a local I/O channel. It is advisable to have `/`, `/usr`, `/var` and other system partitions on local devices.

Fibre Channel switch

Each node in the cluster must have a Fibre Channel I/O channel to access shared storage devices. The primary component of the Fibre Channel fabric is the Fibre Channel switch.

Cluster platforms

There are several hardware platforms that can function as nodes in a Storage Foundation Cluster File System (SF CFS) cluster.

See the *Veritas Storage Foundation Release Notes*.

Install the HP-UX 11i 64-bit operating system with the March 2009 HP-UX 11i Version 3.0 or later on each node and install a Fibre Channel host bus adapter to allow connection to the Fibre Channel switch.

Note: For a cluster to work correctly, all nodes must have the same time. If you are not running the Network Time Protocol (NTP) daemon, make sure the time on all the systems comprising your cluster is synchronized.

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 28.

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 60.

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 117.

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 32.

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.symantec.com/sfm

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 release of Storage Foundation Cluster File System requires 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 Cluster File System 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 Cluster File System.

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.

Storage Foundation Cluster File System node requirements

All nodes in a Cluster File System must have the same operating system version and update level.

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
```

Chapter 4

Installing Storage Foundation Cluster File System

This chapter includes the following topics:

About installing Veritas Storage Foundation Cluster File System on HP-UX

This release of Veritas Storage Foundation Cluster File System requires the March 2009 HP-UX 11i version 3.0 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 Cluster File System that you are upgrading, you must perform an upgrade to move to the 5.0.1 versions of the Veritas products.

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.
  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.
- If patches for the operating system are required, install the patches before upgrading the product.
  See "Required HP-UX patches" on page 60.
- Mount the disk.
  See "Mounting a software disc" on page 34.
- Install the 5.0.1 Veritas Storage Foundation product.
  Start the installer and select 'I' for install, or run the appropriate installation script.
- 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 41.

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.

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 117.

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 118.

Installing Storage Foundation Cluster File System using the common product installer

The product installer is the recommended method to license and install Storage Foundation Cluster File System.

For a simple initial installation on new system, you can use the following procedure.

The following sample procedure is based on the installation of a Veritas Storage Foundation Cluster File System HA cluster with two nodes: "system01" and "system02." If you are installing on standalone systems only, some steps are unnecessary, and these are indicated.

Default responses are enclosed by parentheses. Press Return to accept defaults.

To install the Storage Foundation Cluster File System

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 18.

2. Load and mount the software disc.

   See "Mounting a software disc" on page 34.

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

4. From this directory, type the following command to install if you are 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. From the Installation menu, choose the `I` option for Install and enter the number for Veritas Storage Foundation Cluster File System. Press **Return**.

6. You are prompted to enter one or more system names to install SFCFS.

   ```
   Enter the system names separted by spaces on which to install
   SFCFS: system01 system02
   ```

7 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 18.

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 SFCFS license key for system01?
```

9 Enter `y` to accept another license key or enter `n` to proceed.

```
Do you want to enter another license key for system01?
[y,n,q] (n) n
```

10 You can choose to install required depots or all depots.

```
1)Required Veritas Storage Foundation Cluster File System depots -
1566 MB required
2)All Veritas Storage Foundation Cluster File System depots -
1623 MB required
3)Storage Foundation for Oracle RAC depots - 2029 MB required

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

11 A list includes the items in the selected option. Press **Return** to continue.

12 Reboot all the nodes on which SFCFS is installed.

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

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
Windows XP, NT, Me, 2000, or 98	300MHz Pentium with at least 256MB of memory

For the VEA client to function properly with the Java Runtime Environment 1.5 (JRE 1.5), install the latest patches for JRE 1.5. To obtain patch information, see the Sun Microsystems Web site.

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 34.
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 and Windows 95 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.
- Java Runtime Environment 1.1 or later must be present.
- 100MHz Pentium with 256MB memory or higher specification.
- 22MB 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 Cluster File System

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.

Configuring Storage Foundation Cluster File System

This section describes configuring Storage Foundation Cluster File System using the Veritas product installer. If you configured Storage Foundation Cluster File System during the installation process, you do not need to perform the procedure in this section.

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

To configure Storage Foundation Cluster File System

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 Cluster File System (SFCFS), 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, "system01" and "system02") 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 SFCFS: 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 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 18.

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

   ```
   Checking system licensing

   SFCFS license registered on system01

   Do you want to enter another license key for system01?
   [y,n,q] (n) n
   ```

6. Any running SFCFS processes are stopped. Press **Return** to continue.

7 Starting I/O Fencing in enabled mode requires manual intervention after SFCFS Configuration. I/O Fencing can be configured in disabled mode now and it does not require any manual intervention after SFCFS Configuration.

Determine at this time if you plan to configure I/O Fencing in enabled mode or disabled mode, as well as the number of network interconnects (NICS) required on your systems. If you configure I/O Fencing in enabled mode only a single NIC is required, though at least two is recommended.

```
Will you be configuring I/O Fencing in enabled mode?
[y,n,q,?] (y) n
```

In this release, you must enter `n` for configuring I/O Fencing in disabled mode.

See the *Storage Foundation Release Notes* for more information.

8 No configuration changes are made to the systems until all configuration questions are completed and confirmed. Press **Return** to continue.

All systems are configured to create one cluster.

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
```

9 The installer discovers the NICs available on the first system and reports them.

```
Discovering NICs on host1 ... discovered lan0 lan1 lan2 lan3 lan4 lan5
```

10 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`, be sure that the same NICs are available on each system; the installer may not verify this.

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.

11 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.

12 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
```

13 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 by running the `vxdctl defaultdg` *`diskgroup`* command on a system.

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
```

14 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. [?] diskgroup001
```

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

16 The Veritas Storage Foundation Cluster File System software is verified and configured.

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
```

18 Configure the Storage Foundation Cluster File System and Cluster Volume Manager agents as required.

For more information about configuring agents, see the *Storage Foundation Cluster File System Administrator's Guide*.

To use volumes as part of an Replicated Volume Group (RVG), configure the required RVG agents. The CVMVolDg resource does not support managing or monitoring volumes that are part of RVG.

For more information about RVG agents, see the *Veritas Cluster Server Agents for Veritas Volume Replicator Configuration Guide*.

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
```

Chapter 6

Upgrading Storage Foundation Cluster File System

This chapter includes the following topics:

About upgrading Storage Foundation Cluster File System and High Availability

Perform the procedures in the following sections to upgrade Storage Foundation Cluster File System and High Availability. You can perform an upgrade to Storage Foundation using the Veritas product installer or product installation script if you already have Storage Foundation Cluster File System installed.

Planning the upgrade

Complete the following tasks in advance of upgrading:

- Review the *Veritas Storage Foundation Release Notes* for any late-breaking information on upgrading your system.
- Be sure that the administrator doing the upgrade has root access and a working knowledge of system administration.
- Schedule sufficient outage time for the upgrade.
- Make sure that the prerequisite patches required for SFCFS 5.0.1 are accessible.

Preparing the system and backing up files before upgrading

Before upgrading an installed Veritas Storage Foundation Cluster File System, preserve the existing configuration information.

To preserve the existing configuration information, perform the following actions:

- Make a record of the mount points for VxFS file systems and VxVM volumes that are defined in the `/etc/fstab` file. You will need to recreate these entries in the `/etc/fstab` file on the freshly installed system.
- Before upgrading, 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.
- Use the `vxlicrep` command to make a record of the currently installed Veritas licenses.
- Back up the configuration files.

  ```
  #cp -r /etc/VRTSvcs/conf/ backupdirectory/
  ```

- If Veritas Volume Replicator (VVR) is configured, do the following steps in the order shown:
  - Make sure that the disk groups that contain RVGs are at least at disk group version 110.

    ```
    # vxdg list diskgroup
    ```

  - Make sure the size of the SRL volume is greater than 110 MB.

Refer to the *Veritas Volume Replicator Administrator's Guide*.

- Stop all the applications involved in replication. For example, if a data volume contains a file system, unmount it.
- Verify that all of the Primary RLINKs are up to date:

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

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

Upgrade paths for Veritas Storage Foundation Cluster File System

Table 6-1 shows the upgrade paths for Veritas Storage Foundation Cluster File System.

Table 6-1 Supported upgrade paths

Storage Foudation Cluster File System version	HP-UX version	Upgrade steps
Storage Foudation Cluster File System 5.0, including Maintenance Packs and Rolling Patches	HP-UX 11i v3	Upgrade to latest OS. Install Storage Foudation Cluster File System See "Upgrading from SFCFS 5.0 on HP-UX 11i v3 to SFCFS 5.0.1 on HP-UX 11i v3" on page 54.
Storage Foudation Cluster File System 5.0, including Maintenance Packs and Rolling Patches	HP-UX 11i v2	Upgrade to latest OS. Install Storage Foudation Cluster File System See "Upgrading from SFCFS 4.x or 5.0x on HP-UX 11i v2 to SFCFS 5.0.1" on page 64.

Table 6-1 Supported upgrade paths *(continued)*

Storage Foudation Cluster File System version	HP-UX version	Upgrade steps
Storage Foudation Cluster File System 4.1, including Maintenance Packs and Rolling Patches	HP-UX 11i v2	Upgrade to latest OS. Install Storage Foudation Cluster File System See "Upgrading from SFCFS 4.x or 5.0x on HP-UX 11i v2 to SFCFS 5.0.1" on page 64.
Storage Foudation Cluster File System 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 3.5 to 5.0.1" on page 74.

Overview of procedures

There are two ways to upgrade cluster nodes to the latest version of Storage Foundation Cluster File System: phased and full.

There are two ways to upgrade cluster nodes to the latest version of Storage Foundation High Availability or Storage Foundation for Oracle High Availability: phased and full.

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 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 from SFCFS 5.0 on HP-UX 11i v3 to SFCFS 5.0.1 on HP-UX 11i v3

Storage Foundation Cluster File System (SFCFS) 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 Cluster File System 5.0.1

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

Be sure to include the cvm group.

```
# 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.

```
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule vxglm=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 53.

13 Upgrade Storage Foundation Cluster File System:

```
# ./installsfcfs [-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.

Be sure to include the cvm group.

```
# 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:

```
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule vxglm=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 Uncommon 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 Add the include statements for `types.cf`, `CFSTypes.cf`and `CVMTypes.cf` in the `/etc/VRTSvcs/conf/config/main.cf` file.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
```

7 Remove the file `.SFCFS.upgrade` located in the directory `/opt/VRTS/install`.

8 Reboot the first half of the cluster:

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

9 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 53.

2 Upgrade Storage Foundation Cluster File System:

```
# ./installsfcfs [-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 file `.SFCFS.upgrade` located in the directory `/opt/VRTS/install`.

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.

Full Upgrade

The following procedure assumes a 2 node cluster system01, system02, where both the nodes are simultaneously upgraded from 5.0 to 5.0.1.

To perform a full upgrade

1 Log in as superuser to one of the nodes in the cluster.

2 If you have created VxFS mount points on VxVM volumes and added them to the `/etc/fstab file`, comment out the mount point entries in the `/etc/fstab file`.

3 Stop all applications that use VxFS or VxVM disk groups, whether local or CFS. If the applications are under VCS control:

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

If the applications are not under VCS control:

Use native application commands to stop the application.

4 Take offline all VCS groups that contain `CFSMount` and `CVMVolDg`

```
# hagrp -offline group -sys system01

# hagrp -offline group -sys system02
```

5 Unmount all the non-system VxFS file systems which are not under VCS control.

```
# umount /mount_point
```

6 Make sure that no processes which make use of mounted shared file system or shared volumes are running.

```
# fuser -cu mount-point
```

7 Stop all VCS service groups.

To view the current state of the service groups:

```
# hagrp -state
```

To stop each group:

```
# hagrp -offline servicegroup -sys node_name
```

8 Freeze all the VCS service groups by running the following commands:

```
# haconf -makerw

# hagrp -freeze servicegroup -persistent

# haconf -dump -makero
```

9 Stop VCS on all the nodes:

```
# hastop -all
```

10 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

11 On each node, edit the `etc/vxfenmode` file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode

vxfen_mode=disabled
```

12 If the HP-UX 11i v3 0903 OEUR release is not already installed, you can now upgrade the HP-UX operating system to the latest available HP-UX 11i version 3 fusion release.

13 Install all the prerequisite patches on all the nodes.

See "Required HP-UX patches" on page 60.

14 Insert the appropriate software disc into your system's DVD drive.

15 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.

16 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
```

17 Change to the top-level directory on the disc:

```
# cd /dvdrom
```

18 Install SFCFS 5.0.1.

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

From the Installation menu, choose the I option for install and enter the number for Veritas Storage Foundation Cluster File System.

19 Uncomment the entries for the non-system VxFS mounts from `/etc/fstab`

20 Reboot all the nodes

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

21 Change the configuration files by running the following commands from one of the nodes.

```
# /opt/VRTS/bin/hastart
```

```
# /opt/VRTS/bin/haconf -makerw
```

```
# /opt/VRTS/bin/hares -delete qlogckd
```

```
# /opt/VRTS/bin/haconf -dump -makero
```

```
# /opt/VRTS/bin/hastop -all -force
```

22 If you have configured the VCS Cluster Manager (Web Console), complete the following to modify the `/etc/VRTSvcs/conf/config/main.cf file`.

- Remove VRTSweb:

```
Process VRTSweb (
PathName = "/opt/VRTSvcs/bin/haweb"
Arguments = "10.129.96.64 8181")
```

- Replace it with:

```
VRTSWebApp VCSweb (
Critical =0
AppName = vcs InstallDir = "/opt/VRTSweb/VERITAS"
TimeForOnline = 5)
```

- Add the NIC resource in the ClusterService group. For example, where the name of the NIC resource is named csgnic and the public NIC device is hme0, add: NIC csgnic (Device = hme0
- Add new dependencies for the new resources in the ClusterService group. For example, using the names of the VRTSWebApp, NotifierMngr, IP, and NIC resources enter lines that resemble: VCSweb requires webip ntfr requires csgnic webip requires csgnic

23 Verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file by running the following commands on system01:

```
# cd /etc/VRTSvcs/conf/config

# /opt/VRTS/bin/hacf -verify .
```

24 Run the following command on all the nodes to start VCS.

```
# /opt/VRTS/bin/hastart
```

25 Configure SFCFS on all the nodes.

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

From the Installation menu, choose the C option for Configure and enter the number for Veritas Storage Foundation Cluster File System.

When the question “Do you want to upgrade to version 5.0.31.5 on these systems using the current configuration? [y,n,q,?] (y) “is asked, proceed with **y**.

26 Verify that the `CVMVolDg` resource type has the `CVMDGAction` attribute:

```
# /opt/VRTS/bin/haattr -display CVMVolDg | \
grep -w CVMDGAction
```

27 If the CVMVolDg resource type does not have the CVMDGAction attribute, then proceed to step 28.

If the CVMVolDg resource type does have the CVMDGAction attribute, perform the following steps:

- Display the current ArgList to check the position of the CVMDGAction attribute.

```
# /opt/VRTS/bin/hatype -display CVMVolDg | grep ArgList
```

The CVMDGAction attribute must be at the end of the ArgList, as follows:

```
# /opt/VRTS/bin/hatype -display CVMVolDg | grep ArgList
CVMVolDg        ArgList            CVMDiskGroup
CVMVolume       CVMActivation      CVMDGAction
```

If the CVMDGAction attribute is not at the end of the ArgList, then proceed to step 28 .

- If the CVMDGAction attribute is not at the end of the ArgList, modify the ArgList so that it is at the end, as follows.

```
# /opt/VRTS/bin/hatype -display CVMVolDg | grep ArgList
CVMVolDg         ArgList          CVMDiskGroup
CVMDGAction      CVMVolume        CVMActivation
```

In the above output, note the CVMDGAction attribute is not at the end of the ArgList. Do the following:

```
# /opt/VRTS/bin/haconf -makerw
# /opt/VRTS/bin/hatype -modify CVMVolDg ArgList \
CVMDiskGroup CVMVolume CVMActivation CVMDGAction
# /opt/VRTS/bin/haconf -dump -makero
```

- Verify that the CVMVolDg resource type has the CVMDGActionattribute at the end:

```
# /opt/VRTS/bin/haattr -display CVMVolDg | grep ArgList
CVMVolDg        ArgList            CVMDiskGroup        CVMVolume
CVMActivation      CVMDGAction
```

- Stop and restart the VCS service on all nodes:

```
# /opt/VRTS/bin/hastop -all -force
# /opt/VRTS/bin/hastart
```

28 Enable I/O fencing

- `# /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 SFCFS 4.x or 5.0x on HP-UX 11i v2 to SFCFS 5.0.1

Upgrade SFCFS from version 4.x or version 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 Cluster File System 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.

   Be sure to include the cvm group.

   ```
   # 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.

```
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule vxglm=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 53.

13 Upgrade Storage Foundation Cluster File System:

```
# ./installsfcfs [-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.

   Be sure to include the cvm group.

   ```
   # 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:

```
# /sbin/init.d/vxfen stop
# /sbin/gabconfig -U
# kcmodule vxfen=unused
# kcmodule vxglm=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 Add the include statements for `types.cf`, `CFSTypes.cf`, and `CVMTypes.cf` in the `/etc/VRTSvcs/conf/config/main.cf` file.

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
```

7 Remove the file `.SFCFS.upgrade` located in the directory `/opt/VRTS/install`.

8 Reboot the first half of the cluster:

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

9 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 53.

2 Upgrade Storage Foundation Cluster File System:

```
# ./installsfcfs [-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 file `.SFCFS.upgrade` located in the directory `/opt/VRTS/install`.

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.

Performing a full upgrade from SFCFS 4.x or 5.0x on HP-UX 11iv2

The following procedure assumes a 4 node cluster system01, system02, system03, system04 where all nodes are simultaneously upgraded from 5.0 to 5.0.1.

- Prepare for the upgrade
- If you have any external Array Policy Modules (APMs) installed, uninstall the APMs. The following warning message appears during the operating system upgrade, and when you issue an administrative command for HP-UX kernel modules after the upgrade, until SFCFS 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 SFCFS.
- Upgrade the HP-UX operating system
- Upgrade Storage Foundation Cluster File System using the product installer
- Post upgrade steps

Preparing to upgrade from Storage Foundation Cluster File System versions on HP-UX 11i v2 to Storage Foundation Cluster File System 5.0.1

Use these steps to prepare to upgrade from Storage Foundation Cluster File System 4.1x or 5.0x on HP-UX 11i v2 to Storage Foundation Cluster File System 5.0.1:

To prepare for upgrade from Storage Foundation Cluster File System versions on HP-UX 11i v2:

1. Log in as superuser to one of the nodes, *system01* for example, in the cluster.
2. Create a backup of the existing cluster configuration. Back up the main.cf and types.cf on all cluster nodes:

   ```
   # cp /etc/VRTSvcs/conf/config/main.cf \
   /etc/VRTSvcs/conf/config/main.cf.save
   # cp /etc/VRTSvcs/conf/config/types.cf \
   /etc/VRTSvcs/conf/config/types.cf.save
   ```

3. 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.

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

If the applications are under VCS control:

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

If the applications are not under VCS control:

Use native application commands to stop the application.

5 Take offline all VCS groups that contain CFSMount and CVMVolDg.

```
# hagrp -offline group -sys system01
```

```
# hagrp -offline group -sys system02
```

6 Unmount all the VxFS file system which is not under VCS control.

```
# umount /mount_point
```

7 Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```
# fuser -cu mount-point
```

8 Stop all VCS service groups.

To view the current state of the service groups:

```
# hagrp -state
```

To stop each group:

```
# hagrp -offline servicegroup -sys node_name
```

9 Freeze the VCS service groups. Run the following commands:

```
# haconf -makerw
# hagrp -freeze servicegroup -persistent
# haconf -dump -makero
```

10 Stop VCS on all nodes:

```
# hastop -all -force
```

11 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.

12 On each node, edit the /etc/vxfenmode file to configure I/O fencing in disabled mode.

```
# cat /etc/vxfenmode
vxfen_mode=disabled
```

Note that to upgrade from SFCFS 4.1on HP-UX 11iv2, create / etc/vxfenmode file and populate it as above.

13 On each node, change LLT_START=0 in the file /etc/rc.config.d/lltconf.

14 On each node, remove the following device files:

```
# rm -f /dev/llt
# rm -f /dev/gab*
# rm -f /dev/vxfen
```

Upgrading the HP-UX 11i v2 operating system to HP-UX 11i v3

Upgrade the operating system from HP-UX 11i v2 to HP-UX 11i v3.

To upgrade the HP-UX 11i v2 operating system to HP-UX 11i v3

1 Upgrade the operating system from HP-UX 11i v2 to HP-UX 11i v3.

To upgrade from Veritas 5.0 releases on 11i v2, select the Base-VxFS-50, Base-VxVM-50 and Base-VxTools-50 bundles while using update-ux(1M) .

See the *HP-UX Operating System* documentation.

2 If any patches to the HP-UX 11i v3 are required, install all the prerequisite patches on all nodes before upgrading the Veritas products.

See "Required HP-UX patches" on page 60.

Upgrading Storage Foundation Cluster File System using the product installer

Use these steps to upgrade Storage Foundation Cluster File System versions on HP-UX 11i v2 to Storage Foundation Cluster File System 5.0.1.

To perform a full upgrade

1 Log in as superuser.

2 Insert the appropriate software disc into your system's DVD drive.

3 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.

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 SFCFS 5.0.1.

```
# installer [-rsh]
```

7 From the installation menu, choose the I option for install and enter the number for Veritas Storage Foundation Cluster File System.

8 Select y to confirm that you want to upgrade SFCFS using the current configuration.

VCS configuration files are not changed during this configuration.

9 Uncomment the VxFS mount point entries in the /etc/fstab file.

10 Reboot all the nodes.

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

11 Configure SFCFS 5.0.1 on all the nodes using the installsfcfs script:

```
# cd /opt/VRTS/install
# ./installsfcfs [-configure] [-rsh]
```

Select y to confirm that you want to reuse the previous configuration of SFCFS.

Completing the configuration of SFCFS after upgrading to 5.0.1

After upgrading SFCFS, perform the following tasks

To perform post upgrade configuration

1 Enable fencing.

```
# hastop -all
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
# /sbin/init.d/vxfen stop
# /sbin/init.d/vxfen start
```

2 Set the clusterwide attribute "UseFence" to use SCSI3.

Add the following line to the /etc/VRTSvcs/conf/config/main.cf file:

```
UseFence=SCSI3
```

3 Start the VCS engine on each system:

```
# hastart
```

4 Complete other post-upgrade tasks.

See "Upgrading the disk layout versions" on page 78.

Upgrading from 3.5 to 5.0.1

SFCFS can be upgraded from 3.5 to 5.0.1 using full upgrade procedure. Phased upgrade from SFCFS 3.5 is not supported.

Full upgrade

The following procedure assumes a 4 node cluster, consisting of system01, system02, system03, system04, in which all nodes are simultaneously upgraded from 3.5 to 5.0.1.

To perform a full upgrade

1 Log in as superuser.

2 Insert the appropriate software disc into your system's DVD drive.

3 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.

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 Take offline all SFCFS resources on all nodes by running the following commands on one of the cluster nodes.

```
# hagrp -offline service_group -sys system01
# hagrp -offline service_group -sys system02
# hagrp -offline service_group -sys system03
# hagrp -offline service_group -sys system04
```

where *service_group* is the service group displayed by the `hagrp -dep cvm` command.

7 Remove the VRTScavf and VRTSglm 3.5 packages from these nodes and run the following command on all the systems.

```
# hastop -local
# swremove VRTScavf VRTSglm
```

8 Uninstall VCS 3.5 from all the nodes. Run the following commands from one of the nodes.

See the *Veritas Cluster Server Installation Guide*.

```
# cd /opt/VRTSvcs/install
# ./uninstallvcs
```

Ignore any errors from the `uninstallvcs` script and proceed with the uninstall of VCS.

9 Reboot the nodes.

10 Unload the `llt` module:

```
# kmadmin -U llt
```

11 Uninstall the `llt` and `gab` packages from the nodes:

```
# swremove -x autoreboot=true VRTSllt VRTSgab
```

12 Reboot the nodes.

13 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

14 If system partitions other than `/stand` have disk layout Version 2 or 3, upgrade those partitions to disk layout Version 5 using the `vxupgrade`command. Partitions with disk layout Version 4 need not be upgraded.

15 Upgrade the operating system from HP-UX 11i Version 1 to HP-UX 11i Version 2 on all the nodes. Then upgrade from HP-UX 11i Version 2 to HP-UX 11i Version 3.

See the *HP-UX Operating System* documentation.

16 Install all the prerequisite patches on all the nodes.

See "Required HP-UX patches" on page 60.

17 Install SFCFS 5.0.1 and reboot all the nodes.

See "Installing Storage Foundation Cluster File System using the common product installer" on page 36.

Do not configure SFCFS after reboot.

18 Start `vxfen` on all the nodes. `vxfen` can be started either in disable or enable mode. For starting `vxfen` in disabled mode, run the following commands:

```
# echo vxfen_mode=disabled > /etc/vxfenmode
# /sbin/init.d/vxfen start
```

See the *Veritas Cluster Server Installation Guide*.

19 Change the configuration files by running the following commands from one of the nodes.

```
# /opt/VRTS/bin/hastart
# /opt/VRTS/bin/haconf -makerw
# /opt/VRTS/bin/hatype -add CVMVxconfigd
# /opt/VRTS/bin/hatype -modify CVMVxconfigd Operations \
    OnOnly
# /opt/VRTS/bin/hares -add cvm_vxconfigd CVMVxconfigd cvm
# /opt/VRTS/bin/hares -modify cvm_vxconfigd Enabled 1
# /opt/VRTS/bin/hares -delete qlogckd
# /opt/VRTS/bin/haconf -dump -makero
# /opt/VRTS/bin/hastop -all -force
```

If you have configured the VCS Cluster Manager (Web Console), complete the following to modify the `/etc/VRTSvcs/conf/config/main.cf` file.

- Remove VRTSweb:

```
Process VRTSweb (
          PathName = "/opt/VRTSvcs/bin/haweb"
          Arguments = "10.129.96.64 8181"
          )
```

- Replace it with:

```
VRTSWebApp VCSweb (
         Critical =0
         AppName = vcs
         InstallDir = "/opt/VRTSweb/VERITAS"
         TimeForOnline = 5
         )
```

- Add the NIC resource in the ClusterService group. For example, where the name of the NIC resource is named csgnic and the public NIC device is hme0, add:

```
NIC csgnic (
       Device = hme0
```

- Add new dependencies for the new resources in the ClusterService group. For example, using the names of the VRTSWebApp, NotifierMngr, IP, and NIC resources, enter lines that resemble:

```
VCSweb requires webip
ntfr requires csgnic
webip requires csgnic
```

20 Verify the syntax of the `/etc/VRTSvcs/conf/config/main.cf` file by running the following command on system01:

```
# cd /etc/VRTSvcs/conf/config
# /opt/VRTS/bin/hacf -verify .
```

21 Run the following command on all the nodes to start VCS.

```
# /opt/VRTS/bin/hastart
# echo 3.5 > /opt/VRTS/install/.SFCFS.upgrade
```

22 Configure SFCFS on all nodes.

See “Configuring Storage Foundation Cluster File System” on page 41.

VCS configuration files are not changed during this configuration.

23 Upgrade file systems to proper disk layout version.

See “Upgrading the disk layout versions” on page 78.

24 Verify that all the file systems are working properly and data is intact.

See `cfsmount`(1M) manual page.

Upgrading the disk layout versions

SFCFS 5.0.1 supports disk layouts Versions 4, 5, 6 and 7 for locally mounted file systems and disk layouts 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 SFCFS 5.0.1, perform the following additional steps to prepare the file system for being mounted on all nodes of the cluster:

To upgrade the disk layout versions

1 Select one of the nodes of the cluster and `mount` the file system locally on this node. For example, mount it without the `-o cluster` option. Enter,

```
# mount -F vxfs block_device_path /mnt1
```

2 Current disk layout version on a file system can be found using

```
# fstyp -v char_device_path | grep version | \
    awk '{print $2}'
```

3 On the node selected in 1, incrementally upgrade the disk layout of this file system to layout Version 6 or layout Version 7. For example, if you had a cluster mounted file system of disk layout Version 4 while running with SFCFS 3.5 on HP-UX 11i Version 1, after upgrading to SFCFS 5.0.1, you would need to upgrade the disk layout to version 6 or version 7 incrementally as follows:

```
# vxupgrade -n 5 /mnt1
# vxupgrade -n 6 /mnt1
# vxupgrade -n 7 /mnt1
```

4 On the node selected in 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 using `cfsmount`.

Chapter 7

Adding and removing a node

This chapter includes the following topics:

Adding a node to a cluster

If you want to add a new node to a multi-node cluster, first prepare the new system hardware. Physically connect the new node to the cluster using private networks and attach to any shared storage. Then install the required OS software. Install all the prerequisite patches.

Note: For a cluster to work correctly, all nodes must have the same time. If you are not running the Network Time Protocol (NTP) daemon, make sure the time on all the nodes comprising your cluster is synchronized.

To add a node to a cluster

1. Log into the new node 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 node.

3 Run the following commands to start Portable File System (PFS):

```
# nohup pfs_mountd &
# nohup pfsd &
```

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 Add `/opt/VRTS/bin` to your `PATH` and `/opt/VRTS/man` to your `MANPATH` environment variables.

6 Change to the SFCFS directory.

```
# cd sfcfs
```

7 Run the `installsfcfs` script with `-installonly` option to install all the required SFCFS packages on the new node.

```
# ./installsfcfs -installonly
```

8 Enter **y** to install SFCFS on these systems.

```
Do you want to install SFCFS on these systems? [y,n,q] (y)
```

9 Enter the system name of the new node to install SFCFS.

```
Enter the system names separted by spaces on which to install
SFCFS: system03
```

10 Enter a license key for the new node.

```
Enter a SFCFS license key for system03:[?]
XXXX-XXXX-XXXX-XXXX-XXXX-X
```

11 Enter **y** or **n** for another license key. You are prompted to press Return to continue.

```
Do you want to enter another license key for system03?
[y,n,q,?] (n)
```

12 Enter `1` or `2` to be installed on all systems.

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

13 Press Return to continue.

```
Press [Return] to continue:
```

Do not reboot the machine now.

14 Create the `/etc/llttab` file the same as it looks on another node in the cluster.

- Change the `set-node` line to the name of the new node, set the `set-cluster` line to the cluster ID, and specify that the LAN ports for the public and private networks are configured the same as on the other cluster nodes:

```
set-node system03
set-cluster 100

link lan1 /dev/lan:1 - ether - -
link lan2 /dev/lan:2 - ether - -
```

- Copy `/etc/llthosts` from one other node of the cluster and add a new line to it with the name of this node.
- Edit the `/etc/llthosts` file and add the new node to the file. For example:

```
0 system01
1 system02
2 system03
```

- Copy the `/etc/llthosts` file from one of the existing systems over to the new system. The `/etc/llthosts` file must be identical on all nodes in the cluster.

15 Create an `/etc/gabtab` file and add the following command to the file:

```
/sbin/gabconfig -c -nN
```

Where *N* is the number of nodes in the cluster. For a three node cluster, *N* would equal 3.

16 There is no need to reboot the other nodes, just update the `/etc/gabtab` file on the other nodes in the cluster. Edit the `/etc/gabtab` file on each of the existing systems, changing the content to match the file on the new system.

17 Start VxVM on the system that has been added.

```
# vxinstall
```

18 After starting VxVM, proceed to Configuring Storage Foundation Cluster File System and Cluster Volume Manager agents on the new node.

Configuring Storage Foundation Cluster File System and Cluster Volume Manager agents on the new node

This section describes how to configure SFCFS and CVM agents on the new node.

To configure SFCFS and CVM agents on the new node

1 Verify if the `/etc/VRTSvcs/conf/config/.stale` file is present, before starting VCS.

If the `/etc/VRTSvcs/conf/config/.stale` file is not present, enter:

```
# touch /etc/VRTSvcs/conf/config/.stale
```

2 Start the VCS server and `vxfen` on the new node:

- Start LLT and GAB on the new node:

```
# /etc/init.d/llt start
# /etc/init.d/gab start
```

- For starting `vxfen` in the disable mode, run the following commands on system03:

```
# echo vxfen_mode=disabled > /etc/vxfenmode
# /sbin/init.d/vxfen start
```

- For starting `vxfen` in the enabled mode:
  - Copy the following files from one of the existing cluster nodes to the new node:

```
/etc/vxfenmode
/etc/vxfendg
```

  - Run the following command:

```
# /sbin/init.d/vxfen start
```

3 On the new node, verify that the GAB port memberships are `a` and `b`. Run the following command:

```
# /sbin/gabconfig -a
```

4 Determine the CVM master node:

```
# vxdctl -c mode
```

5 Make a backup copy of the `main.cf` file. Enter the following commands:

```
# cd /etc/VRTSvcs/conf/config
# cp main.cf main.cf.2node
```

6 Open the VCS configuration for writing and add the new node. For example:

```
# haconf -makerw
# hasys -add system03
```

7 Add the new node to the CVM system list and specify a failover priority of 2:

```
# hagrp -modify cvm SystemList -add system03 X
```

where *X* is one more than the index of the last system in System list of CVM service group in `/etc/VRTSvcs/conf/config/main.cf`.

8 Add the new node to the CVM AutoStartList:

```
# hagrp -modify cvm AutoStartList -add system03
```

9 Node ID can be obtained from `CVMNodeId` of `/etc/VRTSvcs/conf/config/main.cf`. Add the new node, `system03`, and its node ID, #, to the `cvm_clust` resource:

```
# hares -modify cvm_clust CVMNodeId -add system03 2
```

10 Write the new VCS configuration to disk:

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

11 Verify the syntax of `main.cf` file:

```
# hacf -verify .
```

12 To enable the existing cluster to recognize the new node, execute on all the nodes in the cluster:

```
# /etc/vx/bin/vxclustadm -m vcs -t gab reinit
# /etc/vx/bin/vxclustadm nidmap
```

13 Start CVM on the newly added node.

- Determine the node ID:

  ```
  # cat /etc/llthosts
  ```

- Verify that this host ID is seen by the GAB module:

  ```
  # gabconfig -a
  ```

- Start the VCS engine.
  - If on the newly added node ports `f`, `u`, `v`, or `w` are present before `hastart`, then the newly added node must be rebooted to properly start VCS. To properly start VCS:

    ```
    # shutdown -r
    ```

  - If on the newly added node ports `f`, `u`, `v` or `w` were not present before `hastart`, then use the following command to start VCS:

    ```
    # hastart
    ```

14 Check the system status to see whether the new node is online:

```
# hastatus -sum
-- SYSTEM STATE
-- System         State       Frozen
A      system01   RUNNING     0
A      system02   RUNNING     0
A      system03   RUNNING     0

-- GROUP STATE
-- Group   System     Probed  AutoDisabled  State
B cvm      system01   Y       N             ONLINE
B cvm      system02   Y       N             ONLINE
B cvm      system03   Y       N             ONLINE
```

15 Add shared disk groups to the cluster configuration:

```
# cfsdgadm add cfsdg system03=sw
```

16 Create a `/mnt` on system03 and run the following commands for the shared mount points:

```
# cfsmntadm modify /mnt add system03=rw
```

See `cfsmntadm`(1M) manual page.

17 Use the`cfsmount` command to cluster mount `/mnt` on the new node:

```
# cfsmount /mnt
```

Removing a node from a cluster

This section describes how to remove a node from a cluster. As in previous examples, the following removes the node system03 from a three-node cluster. The procedure can be done from any node remaining in the cluster or from a remote host.

To remove a node from a cluster

1 Log in as superuser on a node other than system03.

2 Use the `cfsumount` command to unmount the file system `/mnt` on all the nodes:

```
# cfsumount /mnt system03
```

3 Stop all the cluster components:

```
# cfscluster stop -f system03
```

4 Open the VCS configuration for writing:

```
# haconf -makerw
```

5 Remove system03 from the system list attribute of the CVM and SFCFS service groups:

```
# hagrp -modify service_group SystemList -delete system03
# hagrp -modify cvm SystemList -delete system03
```

where *service_group* is the name of the service group displayed by the `hagrp -dep cvm` command.

6 Write the new VCS configuration to disk:

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

7 Edit the `/etc/llthosts` file on the remaining nodes of the cluster, and remove the entry corresponding to the node being removed.

8 Edit the `/etc/gabtab` file on the remaining nodes of the cluster and edit the `gabconfig` command to reflect the correct and new number of nodes in the cluster.

9 Login to system03 and remove the following files:

```
# rm /etc/vxfenmode
# rm /etc/llthosts
# rm /etc/lltab
# rm /etc/gabtab
```

10 If fencing was enabled on the cluster, run the following commands:

```
# rm /etc/vxfentab
# rm /etc/vxfendg
```

11 If necessary, modify the `/etc/gabtab` file. No change is required to this file if the `/sbin/gabconfig` command has only the argument `-c`, although Symantec recommends using the `-n`*N* option, where *N* is the number of cluster nodes. If the command has the form `/sbin/gabconfig -c -n`*N*, where *N* is the number of cluster nodes, then make sure that *N* is not greater than the actual number of nodes in the cluster, or GAB does not automatically seed.

Modify `/etc/llthosts` file on each remaining nodes to remove the entry of the leaving node.

12 Reboot system03:

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

13 Change to the `install` directory:

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

14 Run the `uninstallsfcfs` script and remove SFCFS on system03:

```
# ./uninstallsfcfs
```

If you do not want to remove the Veritas Cluster Server software, enter **n** when prompted to uninstall VCS.

See the *Veritas Cluster Server Installation Guide*.

Chapter 8

Verifying the Storage Foundation Cluster File System 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 17.

Verifying the configuration files for Storage Foundation Cluster File System

You can inspect the contents of the configuration files that were installed and modified after a successful installation process. These files reflect the configuration based on the information you supplied.

To verify the configuration files

1. Log in as superuser to any system in the cluster.
2. Set up your environment `PATH` variable.

   ```
   # export PATH=$PATH:/sbin:/usr/sbin:/opt/VRTS/bin
   ```

Low Latency Transport configuration files

The following files are required by the VCS communication services for Low Latency Transport (LLT).

/etc/llthosts

The file `llthosts`(4M) is a database, containing one entry per system, that links the LLT system ID (in the first column) with the LLT host name. This file is identical on each system in the cluster.

For example, the file `/etc/llthosts` contains entries that resemble:

```
0    system01
1    system02
```

/etc/lltab

The file `lltab`(4M) contains information that is derived during installation and used by the utility `lltconfig`(1M). After installation, this file lists the network links that correspond to the specific system.

For example, the file `/etc/lltab` contains entries that resemble:

```
set-node system01
set-cluster 100

link lan1 lan:1 - ether - -
link lan2 lan:2 - ether - -
```

The first line identifies the local system name. The second line identifies the cluster (that is, the cluster ID you entered during installation). The next two lines, beginning with the `link` command, identify the two network cards used by the LLT protocol.

See the `lltab`(4M) manual page.

Checking Low Latency Transport operation

Use the `lltstat` command to verify that links are active for LLT. This command returns information about the links for LLT for the system on which it is typed. See the `lltstat`(1M) manual page.

In the following example, `lltstat -n` is typed on each system in the cluster.

To check LLT operation

1 Log into system01.

```
# lltstat -n
```

Output resembles:

```
   LLT  node  information:
    Node                        State             Links
*   0    system01               OPEN                  2
    1    system02               OPEN                  2
```

2 Log into system02.

```
  # lltstat -n
```

Output resembles:

```
   LLT  node  information:
    Node                        State             Links
    0    system01               OPEN                  2
*   1    system02               OPEN                  2
```

Each system has two links and that each system is in the OPEN state. An asterisk (*) denotes the system on which the command is typed.

With LLT configured correctly, the output of `lltstat -n` shows all of the systems in the cluster and two links for each system. If the output shows otherwise, you can use the verbose option of `lltstat`. For example, type `lltstat -nvv | more` on a system to view additional information about LLT. In the following example, `lltstat -nvv | more` is typed on a system in a two-node cluster.

3 Log into system01.

```
# lltstat -nvv | more
```

Output resembles:

```
Node        State       Link       Status      Address

*0 system01 OPEN       lan1       UP          08:00:20:93:0E:34
                        lan2        UP          08:00:20:93:0E:34
 1 system02  OPEN       lan1        UP          08:00:20:8F:D1:F2
                        lan2       DOWN        08:00:20:8F:D1:F2

 2           CONNWAIT
                        lan1        DOWN
                        lan2        DOWN
 .
 .
 .
 31          CONNWAIT
                        lan1        DOWN
                        lan2        DOWN
```

The output lists 32 nodes. It reports on the two cluster nodes, system01 and system02, plus non-existent nodes. For each correctly configured system, the information shows a state of OPEN, a status for each link of UP, and an address for each link. However, in the example above, the output shows that for node system02, the private network may have failed earlier, or the information in `/etc/lltab` may be incorrect.

To obtain information about the ports open for LLT, type `lltstat -p` on any system. In the following example, `lltstat -p` is typed on one system in the cluster.

4 Log into system01.

```
# lltstat -p
```

Output resembles:

```
LLT port information:
 Port     Usage     Cookie
 0        gab       0x0
          opens:           0 1 3 4 5 6 7 8 9 10 11 12 13...
          connects:        0 1
```

The two systems with node ID's 0 and 1 are connected.

See "/etc/llthosts" on page 94.

Group Membership and Atomic Broadcast configuration files

The following files are required by the VCS communication services for Group Membership and Atomic Broadcast (GAB).

/etc/gabtab

After installation, the file `/etc/gabtab` contains a `gabconfig`(1M) command that configures the GAB driver for use.

The file `/etc/gabtab` contains a line that resembles:

```
/sbin/gabconfig -c -nN
```

where the `-c` option configures the driver for use and `-nN` specifies that the cluster will not be formed until at least *N* systems are ready to form the cluster. *N* is the number of systems in the cluster.

Checking Group Membership and Atomic Broadcast operation

This section describes how to check GAB operation.

To check GAB operation

- Enter the following command on each node in the cluster.

  ```
  # gabconfig -a
  ```

  If GAB is operational, the following output displays with GAB port membership information:

  ```
  GAB Port Memberships
  ===============================================================
  Port a gen 1bbf01 membership 01
  Port b gen 1bbf06 membership 01
  Port f gen 1bbf0f membership 01
  Port h gen 1bbf03 membership 01
  Port v gen 1bbf0b membership 01
  Port w gen 1bbf0d membership 01
  ```

  If GAB is not operational, the following output display with no GAB port membership information:

  ```
  GAB Port Memberships
  ===============================================================
  ```

  See the *Veritas Cluster Server User's Guide*.

Checking cluster operation

This section describes how to check cluster operation.

To check cluster operation

1 Enter the following command on any system:

```
# hastatus -summary
```

The output for an SFCFS HA installation resembles:

```
-- SYSTEM STATE
-- System               State                Frozen

A  system01             RUNNING              0
A  system02             RUNNING              0

-- GROUP STATE
-- Group       System      Probed AutoDisabled   State

B  cvm         system01    Y      N              ONLINE
B  cvm         system02    Y      N              ONLINE
```

If the State value is running, VCS is successfully installed and running on that node.

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

See the *Veritas Cluster Server User's Guide*.

2 Enter the following command on any systems:

```
# hasys -display
```

See the *Veritas Cluster Server User's Guide*.

For more information on the `hasys -display` command, see the `hasys`(1M) manual page.

The example shows the output of system01. The list continues with similar information for system02 (not shown) and any other systems in the cluster. The output should be similar on each system.

Table 8-1 shows on each system, the output should be similar:

Table 8-1 System sample output for hasys -display

#System	Attribute	Value
system01	AgentsStopped	0
system01	AvailableCapacity	1

Table 8-1 System sample output for hasys -display *(continued)*

#System	Attribute	Value
system01	Capacity	1
system01	ConfigBlockCount	54
system01	ConfigCheckSum	29776
system01	ConfigDiskState	CURRENT
system01	ConfigFile	/etc/VRTSvcs/conf/config
system01	ConfigInfoCnt	0
system01	ConfigModDate	Tues June 25 23:00:00 2006
system01	CurrentLimits	
system01	DiskHbStatus	
system01	DynamicLoad	0
system01	Frozen	0
system01	GUIIPAddr	
system01	LLTNodeId	0
system01	Limits	
system01	LoadTimeCounter	1890
system01	LoadTimeThreshold	600
system01	LoadWarningLevel	80
system01	MajorVersion	2
system01	MinorVersion	0
system01	NodeId	0
system01	OnGrpCnt	1
system01	ShutdownTimeout	60
system01	SourceFile	./main.cf
system01	SysName	system01

Table 8-1 System sample output for hasys -display *(continued)*

#System	Attribute	Value
system01	SysState	RUNNING
system01	SystemLocation	
system01	SystemOwner	
system01	TFrozen	0
system01	TRSE	0
system01	UpDownState	Up
system01	UserInt	0
system01	UserStr	

Verifying agent configuration for Storage Foundation Cluster File System

This section describes how to verify the agent configuration.

To verify the agent configuration

- Enter the cluster status command from any node in the cluster:

```
# cfscluster status
```

Output resembles:

```
Node             :  system01
Cluster Manager  :  running
CVM state        :  running
No mount point registered with cluster configuration

Node             :  system02
Cluster Manager  :  running
CVM state        :  running
No mount point registered with cluster configuration
```

Synchronizing time on Cluster File Systems

SFCFS requires that the system clocks on all nodes are synchronized using some external component such as the Network Time Protocol (NTP) daemon. If the nodes are not in sync, timestamps for change (`ctime`) and modification (`mtime`) may not be consistent with the sequence in which operations actually happened.

Configuring VCS for Storage Foundation Cluster File System

Configuring VCS means conveying to the VCS engine the definitions of the cluster, service groups, resources, and resource dependencies. VCS uses two configuration files in a default configuration:

- The `main.cf` file defines the entire cluster.
- The `types.cf` file defines the resource types.

By default, both files reside in the directory `/etc/VRTSvcs/conf/config`. Additional files similar to `types.cf` may be present if agents have been added, such as `OracleTypes.cf`.

In a VCS cluster, the first system to be brought online reads the configuration file and creates an internal (in-memory) representation of the configuration. Systems brought online after the first system derive their information from systems running in the cluster. You must stop the cluster while you are modifying the files from the command line. Changes made by editing the configuration files take effect when the cluster is restarted. The node on which the changes were made should be the first node to be brought back online.

main.cf file

The VCS configuration file `main.cf` is created during the installation procedure. After installation, the `main.cf` file contains the base definitions of the cluster and its nodes. Additionally, the file `types.cf` listed in the include statement defines the bundled agents for VCS resources.

See the *Veritas Cluster Server User's Guide*.

A typical VCS configuration file for SFCFS file resembles:

```
include "types.cf"
include "CFSTypes.cf"
include "CVMTypes.cf"
```

```
cluster sfcfs_1 (
        HacliUserLevel = COMMANDROOT
        )

system thor150 (
        )

system thor151 (
        )

group cvm (
        SystemList = { thor150 = 0, thor151 = 1 }
        AutoFailOver = 0
        Parallel = 1
        AutoStartList = { thor150, thor151 }
        )

        CVMCluster cvm_clus (
                CVMClustName = sfcfs_1
                CVMNodeId = { thor150 = 0, thor151 = 1 }
                CVMTransport = gab
                CVMTimeout = 200
                )

        CVMVxconfigd cvm_vxconfigd (
                Critical = 0
                CVMVxconfigdArgs = { syslog }
                )

        cvm_clus requires cvm_vxconfigd


        // resource dependency tree
        //
        //      group cvm
        //      {
        //      CVMCluster cvm_clus
        //          {
        //          CVMVxconfigd cvm_vxconfigd
        //          }
        //      }
```

Storage Foundation Cluster File System HA Only

If you configured VCS Cluster Manager (Web Console), a service group, "ClusterService," was created that includes IP, Process, and Notifier resources. These resources were configured according to information you provided during the installation procedure. A resource dependency was also created.

Veritas Cluster Server application failover services

If you installed SFCFS HA, you can begin implementing the application monitoring failover services provided by the Veritas Cluster Server. Information about setting up VCS services is beyond the scope of this document.

See the *Veritas Cluster Server* documentation.

Chapter 9

Uninstalling Storage Foundation Cluster File System

This chapter includes the following topics:

Summary of Storage Foundation Cluster File System uninstallation tasks

Warning: Failure to follow the preparations that are outlined in this chapter can result in loss of data.

Uninstallation of Storage Foundation Cluster File System consists of the following tasks:

- 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 Storage Foundation Cluster File System 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.

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 Storage Foundation Cluster File System

If you need to uninstall SFCFS software. Use the `uninstallsfcfs` script.

To uninstall SFCFS HA

1. Log in as superuser.
2. Stop the cluster:

   ```
   # hastop -all
   ```

   Do not use the `hastop -force` command to stop VCS.
3. Change directory to `/opt/VRTS/install`:

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

4 Run the `uninstallsfcfs` command to uninstall SFCFS. The `uninstallsfcfs` script uses ssh to communicate with remote nodes as default:

```
# ./uninstallsfcfs
```

If you want to use rsh you must specify on the command line:

```
# ./uninstallsfcfs -rsh
```

5 Enter the system names to uninstall SFCFS.

```
Enter the system names separated by spaces on which to
uninstall SFCFS: system01 system02
```

6 Enter **y** to uninstall SFCFS.

```
Are you sure you want to uninstall SFCFS? [y,n,q] (y)
```

7 Reboot the systems on which SFCFS is uninstalled after successful uninstallation.

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 35.

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 117.

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 18.

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 Cluster File System 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
```

Appendix C

Troubleshooting information

This appendix includes the following topics:

Storage Foundation Cluster File System installation issues

If you encounter any issues installing SFCFS, refer to the following paragraphs for typical problems and their solutions.

Incorrect permissions for root on remote system

The permissions are inappropriate. Make sure you have remote root access permission on each system to which you are installing.

```
Checking ssh communication with system01 ......... permission denied
installer requires that ssh commands used between systems execute without
prompting for passwords or confirmations.  Please run installer again with
the ssh configured for password free logins, or configure rsh and use the
-rsh option.
```

Suggested solution: You need to set up the systems to allow remote access using `ssh` or `rsh`.

See "Configuring secure shell (ssh) or remote shell before installing products" on page 18.

Note: Remove remote shell permissions after completing the Storage Foundation Cluster File System installation and configuration.

Resource temporarily unavailable

If the installation fails with the following error message on the console:

```
fork() failed: Resource temporarily unavailable
```

The value of `nkthread` tunable parameter may not be large enough. The `nkthread` tunable requires a minimum value of 600 on all systems in the cluster. To determine the current value of `nkthread`, enter:

```
# kctune -q nkthread
```

If necessary, you can change the value of `nkthread` using the SAM (System Administration Manager) interface, or by running the `kctune` command. If you change the value of `nkthread`, the kernel must be rebuilt for the new value to take effect. It is easier to change the value using SAM because there is an option to process the new kernel immediately.

See the `kctune`(1M) and `sam`(1M) manual pages.

Inaccessible system

The system you specified is not accessible. This could be for a variety of reasons such as, the system name was entered incorrectly or the system is not available over the network.

```
Checking communication with system01 ..............  FAILED
  System not accessible : system01
```

Suggested solution: Verify that you entered the system name correctly; use the `ping`(1M) command to verify the accessibility of the host.

If a system cannot access the software source depot, either `swagentd` is not running on the target system or the `swlist` command cannot see the source depot.

```
Correct /etc/{hosts, nsswitch.conf} and continue from here
Continue? [Y/N] :
```

Suggested solutions: check that `swagentd` is running. Check whether there is an entry for the target system in `/etc/hosts`. If there is no entry, then ensure the `hosts` file is not the primary lookup for the "hosts" entry.

Storage Foundation Cluster File System problems

If there is a device failure or controller failure to a device, the file system may become disabled cluster-wide. To address the problem, unmount file system on all the nodes, then run a full `fsck`. When the file system check completes, mount all nodes again.

Unmount failures

The `umount` command can fail if a reference is being held by an NFS server. Unshare the mount point and try the unmount again.

Mount failures

Mounting a file system can fail for the following reasons:

- The file system is not using disk layout Version 6 or 7.
- The mount options do not match the options of already mounted nodes.
- A cluster file system is mounted by default with the `qio` option enabled if the node has a Quick I/O for Databases license installed, even if the `qio` mount option was not explicitly specified. If the Quick I/O license is not installed, a cluster file system is mounted without the `qio` option enabled. So if some nodes in the cluster have a Quick I/O license installed and others do not, a cluster mount can succeed on some nodes and fail on others due to different mount options. To avoid this situation, ensure that Quick I/O licensing is uniformly applied, or be careful to mount the cluster file system with the `qio/noqio` option appropriately specified on each node of the cluster.
  See the `mount`(1M) manual page.
- A shared CVM volume was not specified.
- The device is still mounted as a local file system somewhere on the cluster. Unmount the device.
- The `fsck` or `mkfs` command is being run on the same volume from another node, or the volume is mounted in non-cluster mode from another node.
- The `vxfsckd` daemon is not running. This typically happens only if the `CFSfsckd` agent was not started correctly.
- If `mount` fails with an error message:

  ```
  vxfs mount: cannot open mnttab
  ```

  `/etc/mnttab` is missing or you do not have `root` privileges.

- If `mount` fails with an error message:

  ```
  vxfs mount: device already mounted, ...
  ```

  The device is in use by `mount`, `mkfs` or `fsck` on the same node. This error cannot be generated from another node in the cluster.

- If this error message displays:

  ```
  mount: slow
  ```

  The node may be in the process of joining the cluster.

- If you try to mount a file system that is already mounted without `-o cluster` option (that is, not in shared mode) on another cluster node,

  ```
  # mount -F vxfs /dev/vx/dsk/share/vol01 /vol01
  ```

  The following error message displays:

  ```
  vxfs mount: /dev/vx/dsk/share/vol01 is already mounted,
    /vol01 is busy, allowable number of mount points exceeded,
    or cluster reservation failed for the volume
  ```

Command failures

This section describes command failures.

- Manual pages not accessible with the `man` command. Set the MANPATH environment variable appropriately.
  See "Setting environment variables" on page 17.

- The `mount`, `fsck`, and `mkfs` utilities reserve a shared volume. They fail on volumes that are in use. Be careful when accessing shared volumes with other utilities such as `dd`, it is possible for these commands to destroy data on the disk.

- Running some commands, such as `vxupgrade -n 7/vol02`, can generate the following error message:

  ```
  vxfs vxupgrade: ERROR: not primary in a cluster file system
  ```

  This means that you can run this command only on the primary, that is, the system that mounted this file system first.

Performance issues

Quick I/O File system performance is adversely affected if a cluster file system is mounted with the `qio` option enabled, but the file system is not used for Quick I/O files. Because `qio` is enabled by default, if you do not intend to use a shared file system for Quick I/O, explicitly specify the `noqio` option when mounting.

High availability issues

This section describes high availability issues.

Network partition/jeopardy

Network partition (or split brain) is a condition where a network failure can be misinterpreted as a failure of one or more nodes in a cluster. If one system in the cluster incorrectly assumes that another system failed, it may restart applications already running on the other system, thereby corrupting data. CFS tries to prevent this by having redundant heartbeat links.

At least one link must be active to maintain the integrity of the cluster. If all the links go down, after the last network link is broken, the node can no longer communicate with other nodes in the cluster. Thus the cluster is in one of two possible states. Either the last network link is broken (called a network partition condition), or the last network link is okay, but the node crashed, in which case it is not a network partition problem. It is not possible to identify whether it is the first or second state, so a kernel message is issued to indicate that a network partition may exist and there is a possibility of data corruption.

Jeopardy is a condition where a node in the cluster has a problem connecting to other nodes. In this situation, the link or disk heartbeat may be down, so a jeopardy warning may be displayed. Specifically, this message appears when a node has only one remaining link to the cluster and that link is a network link. This is considered a critical event because the node may lose its only remaining connection to the network.

Warning: Do not remove the communication links while shared storage is still connected.

Low memory

Under heavy loads, software that manages heartbeat communication links may not be able to allocate kernel memory. If this occurs, a node halts to avoid any chance of network partitioning. Reduce the load on the node if this happens frequently.

A similar situation may occur if the values in the `/etc/lltab` files on all cluster nodes are not correct or identical.

Index

Q

R

S

T

V