Veritas™ Dynamic Multi-Pathing Installation Guide

Solaris

6.0.1

July 2012

Symantec

Veritas™ Dynamic Multi-Pathing Installation Guide

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

Product version: 6.0.1

Document version: 6.0.1 Rev 0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Documentation

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

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Support agreement resources

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

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

Contents

Section 1

Installation overview and planning

Chapter 1

Introducing Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

About Veritas Dynamic Multi-Pathing (DMP)

Veritas Dynamic Multi-Pathing (DMP) provides multi-pathing functionality for the operating system native devices configured on the system. DMP creates DMP metadevices (also known as DMP nodes) to represent all the device paths to the same physical LUN.

DMP is also available as a stand-alone product, which extends DMP metadevices to support ZFS. You can create ZFS pools on DMP metadevices. DMP supports only non-root ZFS file systems.

Veritas Dynamic Multi-Pathing can be licensed separately from Storage Foundation products. Veritas Volume Manager and Veritas File System functionality is not provided with a DMP license.

DMP functionality is available with a Storage Foundation (SF) Enterprise license, a SF HA Enterprise license, and a Storage Foundation Standard license.

Veritas Volume Manager (VxVM) volumes and disk groups can co-exist with ZFS pools, but each device can only support one of the types. If a disk has a VxVM label, then the disk is not available to ZFS. Similarly, if a disk is in use by ZFS, then the disk is not available to VxVM.

Chapter 2

System requirements

This chapter includes the following topics:

Release notes

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

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

https://sort.symantec.com/documents

Hardware compatibility list (HCL)

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

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

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

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

Supported operating systems

For information on supported operating systems, see the *Veritas Dynamic Multi-Pathing Release Notes*.

Disk space requirements

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

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

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

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

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

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

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

See "About the Veritas installer" on page 22.

Discovering product versions and various requirement information

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

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

Information the `version` option or the `showversion` script discovers on systems includes the following:

- The installed version of all released Storage Foundation and High Availability Suite of products

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

To run the version checker

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

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

Chapter 3

Planning to install DMP

This chapter includes the following topics:

About planning for DMP installation

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

https://sort.symantec.com/documents

Document version: 6.0.1 Rev 0.

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

Follow the preinstallation instructions if you are installing Veritas Dynamic Multi-Pathing.

See the chapter, "Preparing to install Veritas Dynamic Multi-Pathing" for more information.

About installation and configuration methods for DMP

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

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

- The Veritas product installer
  The installer displays a menu that simplifies the selection of installation options.
- The product-specific installation scripts
  The installation scripts provide a command-line interface to install a specific product. The product-specific scripts enable you to specify some additional command-line options. Installing with the installation script is also the same as specifying DMP from the installer menu.
- The Web-based Veritas installer
  The installer provides an interface to manage the installation from a remote site using a standard Web browser.
  See "About the Web-based installer" on page 41.
- Silent installation with response files
  You can use any of the above options to generate a response file. You can then customize the response file for another system. Run the product installation script with the response file to install silently on one or more systems.
  See "About response files" on page 137.
- JumpStart
  You can use the Veritas product installer or the product-specific installation script to generate a Jumpstart script file. Use the generated script to install Veritas packages from your JumpStart server.

About the Veritas installer

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

- The general product installer. The general product installer enables you to install and configure the product, verify preinstallation requirements, and view the product's description. You perform the installation from a disc, and you are prompted to choose a product to install.
  See "Installing DMP" on page 37.
- Product-specific installation scripts. If you obtained a standalone Veritas product from an electronic download site, the single product download files do not contain the general product installer. Use the product installation script to install the individual products. You can find these scripts at the root of the product media in the scripts directory. These scripts are also installed with the product.

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

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

Table 3-1 Product installation scripts

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

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

For example, for the 6.0.1 version:

```
# /opt/VRTS/install/installdmp601 -configure
```

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

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

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

See "Command options for the installation script" on page 127.

See "Command options for uninstall script" on page 134.

Chapter 4

Licensing DMP

This chapter includes the following topics:

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

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

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

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 26.
  See the `vxkeyless(1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
  See "Installing Veritas product license keys" on page 28.
  See the `vxlicinst(1m)` manual page.

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

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

Setting or changing the product level for keyless licensing

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

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

http://go.symantec.com/vom

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

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

To set or change the product level

1 Change your current working directory:

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

2 View the current setting for the product level.

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

3 View the possible settings for the product level.

```
# ./vxkeyless displayall
```

4 Set the desired product level.

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

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

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

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

To clear the product license level

1 View the current setting for the product license level.

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

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

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

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

Installing Veritas product license keys

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin

# ./vxlicinst -k license key
```

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

```
# ./vxkeyless display
```

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

Section 2

Installation of DMP

Chapter 5

Preparing to install DMP

This chapter includes the following topics:

Installation preparation overview

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

Table 5-1 Installation overview

Installation task	Section
Obtain product licenses.	See "About Veritas product licensing" on page 25.
Download the software, or insert the product DVD.	See "Mounting the product disc" on page 34.
Set environment variables.	See "Setting environment variables" on page 33.
Create the `/opt` directory, if it does not exist.	See "Creating the /opt directory" on page 34.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Configure the secure shell (ssh) or remote shell (rsh) on all nodes.	See "About using ssh or rsh with the Veritas installer" on page 33.
Verify that hardware, software, and operating system requirements are met.	See "Release notes" on page 17.
Check that sufficient disk space is available.	See "Disk space requirements" on page 18.
Use the installer to install the products.	See "About the Veritas installer" on page 22.

Creating root user

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

To change root role into a user

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

```
% su  - root
```

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

```
# roles admin

root

# usermod -R " " admin
```

3 Change the root role into a user.

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

4 Verify the change.

- `# getent user_attr root`

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

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

- `# userattr type root`

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

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

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

See "Changing root user into root role" on page 67.

Setting environment variables

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

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

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

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

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

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

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

About using ssh or rsh with the Veritas installer

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

abruptly, use the installation script's `-comcleanup` option to remove the ssh or rsh configuration from the systems.

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

- When you perform installer sessions using a response file.

See "About configuring secure shell or remote shell communication modes before installing products" on page 153.

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.

Mounting the product disc

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

To mount the product disc

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

   The systems must be in the same subnet.

2. Insert the product disc into a DVD drive that is connected to your system.
3. If Solaris volume management software is running on your system, the software disc automatically mounts as /cdrom/cdrom0.
4. If Solaris volume management software is not available to mount the DVD, you must mount it manually. After you insert the software disc, enter:

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

   Where c0t6d0s2 is the default address for the disc drive.

Assessing the system for installation readiness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Veritas Dynamic Multi-Pathing 6.0.1.

Symantec Operations Readiness Tools	Symantec Operations Readiness Tools (SORT) is a Web-based application that is designed to support Symantec enterprise products. See "About Symantec Operations Readiness Tools" on page 35.
Prechecking your systems using the installer	Performs a pre-installation check on the specified systems. The Veritas product installer reports whether the specified systems meet the minimum requirements for installing Veritas Dynamic Multi-Pathing 6.0.1. See "Prechecking your systems using the Veritas installer" on page 36.

About Symantec Operations Readiness Tools

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

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

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

To access SORT, go to:

https://sort.symantec.com

Prechecking your systems using the Veritas installer

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

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

To use the precheck option

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

   See "Installing DMP with the Web-based installer" on page 44.

2. Select the precheck option:

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

     ```
     # ./installer
     ```

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

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

Chapter 6

Installing DMP using the script-based installer

This chapter includes the following topics:

Installing DMP

Use the installer program to install Veritas Dynamic Multi-Pathing (DMP) on your system.

The following sample procedure installs DMP on a single system.

To install DMP

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

   See "About configuring secure shell or remote shell communication modes before installing products" on page 153.

2. Load and mount the software disc.

   See "Mounting the product disc" on page 34.

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

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

4 From this directory, type the following command to install on the local system. Also use this command to install on remote systems provided that the secure shell (SSH) or remote shell (rsh) utilities are configured:

```
# ./installer
```

5 Enter I to install and press the Return key.

6 When the list of available products is displayed, to select **Veritas Dynamic Multi-Pathing**, enter the corresponding number, and press the Return key.

7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA). Press the return key to proceed.

8 Select one of the following installation options:

- A minimal installation installs packages for minimal functionality for the selected product.
- A recommended installation installs the recommended DMP packages that provide complete functionality of the product.
  Note that this option is the default.
- The display selection displays all packages and provides information about them. Note that the recommended installation installs the minimum and the recommended packages.

9 When the installer prompts you, indicate the systems where you want to install DMP. Enter one or more system names, separated by spaces.

10 The installer program verifies the system for installation. If the installer does not verify a system, fix the issue and return to the installer.

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

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

12 The installer program prompts you to choose a licensing method.

If you have a valid license key, select 1 and enter the license key at the prompt.

To install through keyless licensing, select 2.

Note: With the keyless license option, you must manage the systems with a management server.

For more information, go to the following Web site:

http://go.symantec.com/sfhakeyless

---

13 The installer installs the product packages. Next, at the prompt, specify whether you want to send your installation information to Symantec. Note that the information sent to Symantec is only to help improve the installer software.

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

14 The installer program completes the installation and starts the DMP processes.

If required, check the log files to confirm the installation.

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

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

Installer also generate a summary file of the whole procedure, you can view your summary file by answering **y:**

```
Would you like to view the summary file? [y,n,q] (n)
```

15 Reboot the systems if the installer prompts for a reboot, to enable DMP native support.

Installing language packages

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

To install the language packages on the server

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

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

Performing a postcheck on a node

The installer's `postcheck` command can help you to determine installation-related problems.

To run the postcheck command on a node

- Run the installer with the `-postcheck` option.

```
# ./installer -postcheck system_name
```

The installer reports some errors or warnings if any processes or drivers do not start.

Chapter 7

Installing DMP using the web-based installer

This chapter includes the following topics:

About the Web-based installer

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

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

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

The Web installer creates log files whenever the Web installer is operating. While the installation processes are operating, the log files are located in a session-based directory under the `/var/tmp` directory. After the install process completes, the

log files are located in the `/opt/VRTS/install/logs` directory. It is recommended that you keep these files for auditing, debugging, and future use.

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

See "Before using the Veritas Web-based installer" on page 42.

See "Starting the Veritas Web-based installer" on page 42.

Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

Table 7-1 Web-based installer requirements

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

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

1 Start the Veritas XPortal Server process `xprtlwid`, on the installation server:

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

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

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

---

2 On the administrative server, start the Web browser.

3 Navigate to the URL that the script displayed.

4 Certain browsers may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

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

5 Log in as superuser.

Obtaining a security exception on Mozilla Firefox

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

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

To obtain a security exception

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

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

3 Click **Get Certificate** button.

4 Uncheck **Permanently Store this exception checkbox (recommended)**.

5 Click **Confirm Security Exception** button.

6 Enter root in User Name field and root password of the web server in the Password field.

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

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

To perform a pre-installation check

1. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 42.

2. On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list. Select **Veritas Storage Foundation and High Availability** from the **Product** drop-down list and click **Next**.

3. Select the Veritas Dynamic Multi-Pathing from the **Product** drop-down list, and click **Next**.

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

5. The installer performs the precheck and displays the results.

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

Installing DMP with the Web-based installer

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

To install DMP using the Web-based installer

1. Perform preliminary steps.

   See "Performing a pre-installation check with the Veritas Web-based installer" on page 44.

2. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 42.

3. Select **Install a Product** from the **Task** drop-down list.

4. Select **Veritas Dynamic Multi-Pathing** from the Product drop-down list, and click Next.

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

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

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

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

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

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

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

- Keyless licensing

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

  For more information, go to the following website:

  http://go.symantec.com/sfhakeyless

  Click **Register**.

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

11 After the product is registered, the processes are started.

For information about migrating your data volumes to DMP devices, refer to the *Veritas Dynamic Multi-Pathing Administrator's Guide*.

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

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

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

Chapter 8

Installing DMP using operating system-specific methods

This chapter includes the following topics:

Installing DMP on Solaris 11 using Automated Installer

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

About Automated Installation

AI automates the installation of the Oracle Solaris 11 OS on one or more SPARC or x86 clients in a network. Automated Installation applies to Solaris 11 only. You

can install the Oracle Solaris OS on many different types of clients.The clients can differ in:

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

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

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

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

Using Automated Installer

To use Automated Installer to install systems over the network, set up DHCP and set up an AI service on an AI server. The DHCP server and AI server can be the same system or two different systems.

Make sure that the systems can access an Oracle Solaris Image Packaging System (IPS) package repository. The IPS package repository can reside on the AI server, on another server on the local network, or on the Internet.

An AI service is associated with a SPARC or x86 AI install image and one or more sets of installation instructions. The installation instructions specify one or more IPS package repositories from where the system retrieves the packages needed to complete the installation. The installation instructions also include the names of additional packages to install and information such as target device and partition information. You can also specify instructions for post-installation configuration of the system.

Consider the operating systems and packages you are installing on the systems. Depending on your configuration and needs, you may want do one of the following:

- If two systems have different architectures or need to be installed with different versions of the Oracle Solaris OS, create two AI services, and associate each AI service with a different AI image.

- If two systems need to be installed with the same version of the Oracle Solaris OS but need to be installed differently in other ways, create two sets of installation instructions for the AI service. The different installation instructions can specify different packages to install or a different slice as the install target.

The installation begins when you boot the system. DHCP directs the system to the AI install server, and the system accesses the install service and the installation instructions within that service.

For more information, see the *Oracle® Solaris 11 Express Automated Installer Guide*.

Using AI to install the Solaris 11 operating system and SFHA products

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

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

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

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

2. Set up the Symantec package repository.

   Run the following commands to start up necessary SMF services and create directories:

   ```
   # svcadm enable svc:/network/dns/multicast:default
   # mkdir /ai
   # zfs create -o compression=on -o mountpoint=/ai rpool/ai
   ```

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

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

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

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

Check the following URL on IE or Firefox browser:

http://<host>:10002

4 Run the following commands to setup IPS repository for Symantec Sparc packages:

```
# mkdir -p /ai/repo_symc_sparc
# pkgrepo create /ai/repo_symc_sparc
# pkgrepo add-publisher -s /ai/repo_symc_sparc Symantec
# pkgrecv -s <media_sparc>/pkgs/VRTSpkgs.p5p -d
/ai/repo_symc_sparc '*'
# svccfg -s pkg/server list
# svcs -a | grep pkg/server
# svccfg -s pkg/server add symcsparc
# svccfg -s pkg/server:symcsparc addpg pkg application
# svccfg -s pkg/server:symcsparc setprop pkg/port=10003
# svccfg -s pkg/server:symcsparc setprop pkg/inst_root=
/ai/repo_symc_sparc
# svccfg -s pkg/server:symcsparc addpg general framework
# svccfg -s pkg/server:symcsparc addpropvalue general/complete
astring: symcsparc
# svccfg -s pkg/server:symcsparc addpropvalue general/enable
boolean: true
# svcs -a | grep pkg/server
# svcadm refresh application/pkg/server:symcsparc
# svcadm enable application/pkg/server:symcsparc
```

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

```
# /usr/lib/pkg.depotd -d /ai/repo_symc_sparc -p 10003 > /dev/null &
```

Check the following URL on IE or Firefox browser:

http://<host>:10003

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

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

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

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

Check the following URL on IE or Firefox browser:

http://<host>:10004

6 Set up the install service on the AI server.

Run the following command:

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

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

Create an install service.

For example:

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

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

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

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

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

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

8 For each system, generate the system configuration and include the hostname, user accounts, and IP addresses. For example, enter one of the following:

```
# mkdir /ai/profiles
# sysconfig create-profile -o /ai/profiles/profile_client.xml
```

or

```
# cp /ai/aiboot/auto-install/sc_profiles/sc_sample.xml
/ai/profiles/profile_client.xml
```

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

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

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

Run the following command to add a SPARC system, for example:

```
# installadm create-client -e "<client_MAC>" -n sol11sparc
# installadm add-manifest -n sol11sparc -f \
/ai/manifests/vrts_manifest_sfha.xml
# installadm create-profile -n sol11sparc -f \
/ai/profiles/profile_client.xml -p profile_sc
# installadm set-criteria -n sol11sparc -m \
vrts_sfha -p profile_sc -c mac="<client_MAC>"
# installadm list -m -c -p -n sol11sparc
```

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

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

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

Manually installing packages on Oracle Solaris 11 systems

To install packages on Solaris 11 system

1. Copy the VRTSpkgs.p5p package from the pkgs directory from the installation media to the system at `/tmp/install` directory.
2. Disable the publishers that are not reachable as package install may fail if any of the already added repositories are unreachable.

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

3. Add a file-based repository in the system.

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

4. Install the required packages.

   ```
   # pkg install --accept VRTSvlic VRTSperl VRTSspt
   VRTSaslapm VRTSsfmh VRTSvxvm VRTSsfcpi601
   ```

5. Remove the publisher from the system.

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

6. Clear the state of the SMF service if non-global zones are present in the system. In presence of non-global zones, setting the file-based repository causes SMF service `svc:/application/pkg/system-repository:default` to go into maintenance state.

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

7. Enable the publishers that were disabled earlier.

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

Installing DMP on Solaris 10 using JumpStart

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

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

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

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

See "Using a Flash archive to install DMP and the operating system" on page 59.

Overview of JumpStart installation tasks

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

Summary of tasks

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

   See "Generating the finish scripts" on page 56.
4. Prepare shared storage installation resources.

   See "Preparing installation resources" on page 57.
5. Modify the rules file for JumpStart.

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

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

   See "About the Veritas installer" on page 22.

Generating the finish scripts

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

To generate the script

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

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

Or

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

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

For example:

```
# ./installdmp -jumpstart /js_scripts
```

2 JumpStart finish scripts and encapsulation scripts are generated in the directory you specified in step 1. Output resembles:

```
The finish scripts for DMP is generated at /js_scripts/
jumpstart_dmp.fin
```

Preparing installation resources

Prepare resources for the JumpStart installation.

To prepare the resources

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

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

2 Generate the response file with the list of packages.

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

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

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

Adding language pack information to the finish file

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

To add the language pack information to the finish file

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

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

If you downloaded the language pack:

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

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

3 The finish script resembles:

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

Using a Flash archive to install DMP and the operating system

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

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

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

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

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

Flash archive creation overview

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

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

   See "Creating the Veritas post-deployment scripts" on page 60.
6. Use the `flarcreate` command to create the Flash archive on the master system.
7. Copy the archive back to the JumpStart server.
8. Use JumpStart to install the Flash archive to the selected systems.
9. Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:

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

   See "About the Veritas installer" on page 22.
10. Perform post-installation and configuration tasks.

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

Creating the Veritas post-deployment scripts

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

To create the post-deployment scripts

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

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

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

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

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

Installing DMP using the system command

Installing DMP on Solaris 10 using the pkgadd command

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

To install DMP on Solaris 10 using the pkgadd command

1. Mount the software disc.

   See "Mounting the product disc" on page 34.

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

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

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

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

4 Use the product-specific install command with one of the following options to get a list of packages in the order to be installed:

- minpkgs
- recpkgs
- allpkgs

See "About the Veritas installer" on page 22.

5 Install the packages listed in step 4.

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

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

6 Verify that the packages are installed:

```
# pkginfo -l
   packagename
```

7 Start the processes.

Installing DMP on Solaris 11 using the pkg install command

To install DMP on Solaris 11 using the pkg install command

1 Mount the software disc.

See "Mounting the product disc" on page 34.

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

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

3 Use the product-specific install command with one of the following options to get a list of packages in the order to be installed:

- minpkgs
- recpkgs
- allpkgs

See "About the Veritas installer" on page 22.

4 Install the packages listed in step 3.

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

# /usr/bin/pkg install -accept pkgname

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

5 Verify that the packages are installed:

```
# pkg info packagename
```

6 Start the processes.

Section 3

Post-installation tasks

Chapter 9

Performing post-installation tasks

This chapter includes the following topics:

Changing root user into root role

On Oracle Solaris 11, to perform installation, you need to create root user. This means that a local user cannot assume the root role. After installation, you may want to turn root user into root role for a local user, who can log in as root.

1. Log in as root user.
2. Change the root account into role.

```
# rolemod -K type=role root

# getent user_attr root

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

3. Assign the root role to a local user who was unassigned the role.

```
# usermod -R root admin
```

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

Chapter 10

Verifying the DMP installation

This chapter includes the following topics:

Verifying that the products were installed

Verify that the DMP products are installed.

Use the pkginfo (Solaris 10) or pkg info (Solaris 11) command to check which packages have been installed.

Solaris 10:

```
# pkginfo -l VRTSvlic package_name package_name ...
```

Solaris 11:

```
# pkg info -| VRTSvlic package_name package_name
```

See "Veritas Dynamic Multi-Pathing installation packages" on page 161.

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

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

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

See "About the Veritas installer" on page 22.

Use the following sections to further verify the product installation.

Installation log files

The Veritas product installer or product installation script installdmp creates log files for auditing and debugging. After every product installation, configuration, or uninstall, the installer displays the name and location of the files. The files are located in the `/opt/VRTS/install/logs` directory. Symantec recommends that you keep the files for auditing, debugging, and future use.

The log files include the following types of text files:

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.
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.
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.

Starting and stopping processes for the Veritas products

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

To stop the processes

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

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

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

  or

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

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

  See "About the Veritas installer" on page 22.

To start the processes

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

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

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

  or

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

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

  See "About the Veritas installer" on page 22.

Section 4

Upgrade of DMP

Chapter 11

Planning to upgrade DMP

This chapter includes the following topics:

Upgrade methods for DMP

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

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

Upgrade types and considerations	Methods available for upgrade
Typical upgrades—use a Veritas provided tool or you can perform the upgrade manually. Requires some server downtime.	Script-based—you can use this to upgrade for the supported upgrade paths Web-based—you can use this to upgrade for the supported upgrade paths Manual—you can use this to upgrade from the previous release Response file—you can use this to upgrade from the supported upgrade paths
Native operating system upgrade—use the upgrade software that comes with the operating system. Note that not all operating systems support native upgrades.	Operating system specific methods Operating system upgrades

Supported upgrade paths for DMP

The following tables describe upgrading to 6.0.1.

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

Veritas software versions	Solaris 9	Solaris 10	Solaris 11
5.1 SP1 and later	Upgrade the OS to at least Solaris 10, then use the installer to upgrade to 6.0.1.	Use the installer to upgrade to 6.0.1.	N/A.
6.0 and 6.0 RP1	N/A.	Use the installer to upgrade to 6.0.1.	N/A.
6.0 PR1	N/A	N/A.	Use the installer to upgrade to 6.0.1.

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

Veritas software versions	Solaris 10	Solaris 11
5.1 SP1* 5.1 SP1 RPx	Use the installer to upgrade to 6.0.1.	N/A.
6.0 and 6.0 RP1	Use the installer to upgrade to 6.0.1.	N/A.
6.0 PR1	N/A.	Use the installer to upgrade to 6.0.1.

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

Preparing to upgrade DMP

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

Getting ready for the upgrade

Complete the following tasks before you perform the upgrade:

- Review the Symantec Technical Support website for additional information: http://www.symantec.com/techsupp/
- For Solaris 10, make sure that all non-global zones are booted and in the running state before you use the Veritas product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.
  For Live Upgrade, if the alternative root environment also has a zone, you cannot install `VRTSodm`. You must remove the `VRTSodm` package first then install the Storage Foundation product. After you reboot the alternative root, you can install `VRTSodm`.
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.
- Make sure that all users are logged off and that all major user applications are properly shut down.
- Make sure that you have created a valid backup.
  See "Creating backups" on page 78.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the packages, for example `/packages/Veritas` when the root file system has enough space or `/var/tmp/packages` if the `/var` file system has enough space.
  Do not put the files under `/tmp`, which is erased during a system reboot. Do not put the files on a file system that is inaccessible prior to running the upgrade script.
  You can use a Veritas-supplied disc for the upgrade as long as modifications to the upgrade script are not required. If `/usr/local` was originally created as a slice, modifications are required.
- For any startup scripts in `/sbin/rcS.d`, comment out any application commands or processes that are known to hang if their file systems are not present.
- Make sure that the current operating system supports version 6.0.1 of the product. If the operating system does not support it, plan for a staged upgrade.
- Schedule sufficient outage time and downtime for the upgrade and any applications that use the Veritas products. Depending on the configuration, the outage can take several hours.

- Any swap partitions not in `rootdg` must be commented out of `/etc/vfstab`. If possible, swap partitions other than those on the root disk should be commented out of `/etc/vfstab` and not mounted during the upgrade. Active swap partitions that are not in `rootdg` cause `upgrade_start` to fail.
- Make sure the file systems are clean before upgrading.
- Symantec recommends that you upgrade VxFS disk layouts to a supported version prior to installing VxFS 6.0.1. Unsupported disk layout versions 4, 5, and 6 can be mounted for the purpose of online upgrading in VxFS 6.0.1. You can upgrade unsupported layout versions online before installing VxFS 6.0.1.
- Upgrade arrays (if required).
  See "Upgrading the array support" on page 78.
- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a failback point.

Creating backups

Save relevant system information before the upgrade.

To create backups

1. Log in as superuser.
2. Before the upgrade, ensure that you have made backups of all data that you want to preserve.

   Back up the `/etc/system` file.
3. Installer verifies that recent backups of configuration files in VxVM private region have been saved in `/etc/vx/cbr/bk`.

   If not, a warning message is displayed.

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

   ---
4. Run the `vxlicrep`, `vxdisk list`, and `vxprint -ht` commands and record the output. Use this information to reconfigure your system after the upgrade.

Upgrading the array support

The Storage Foundation 6.0.1 release includes all array support in a single package, VRTSaslapm. The array support package includes the array support previously included in the VRTSvxvm package. The array support package also includes

support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

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

See "Hardware compatibility list (HCL)" on page 17.

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

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

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

Chapter 12

Upgrading DMP

This chapter includes the following topics:

Upgrading Veritas Dynamic Multi-Pathing with the product installer when OS upgrade is not required

This section describes upgrading to the current Veritas Dynamic Multi-Pathing if the root disk is unencapsulated, and you do not intend to upgrade your Solaris version. Only use this procedure if you are already running a version of Solaris that is supported with 6.0.1.

To upgrade Veritas Dynamic Multi-Pathing

1. Log in as superuser.
2. If the root disk is encapsulated under VxVM, unmirror and unencapsulate the root disk as described in the following steps, to be performed in the order listed:
   - Use the `vxplex` command to remove all the plexes of the volumes `rootvol`, `swapvol`, `usr`, `var`, `opt` and `home` that are on disks other than the root disk.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 Stop the product's processes.

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

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

11 The installer stops, uninstalls, reinstalls, and starts specified packages.

12 If the upgrade was done from 5.0 or if the Veritas Dynamic Multi-Pathing was done without vxkeyless keys, the installer shows the following warning:

```
CPI WARNING V-9-40-5323 DMP license version 5.0 is not
updated to 6.0 on sys1. It's recommended to upgrade to a 6.0 key.
CPI WARNING V-9-40-5323 DMP license version 5.0 is not updated
to 6.0 on sys2. It's recommended to upgrade to a 6.0 key.
DMP is licensed on the systems.
Do you wish to enter additional licenses? [y,n,q,b] (n) n
```

13 The Veritas Dynamic Multi-Pathing software is verified and configured.

14 The installer prompts you to provide feedback, and provides the log location for the upgrade.

15 Reboot the systems if the installer prompts reboot to enable DMP native support.

Upgrading Veritas Dynamic Multi-Pathing to 6.0.1 using the product installer or manual steps

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

Upgrading Veritas Dynamic Multi-Pathing with the product installer

This section describes upgrading to the current Veritas Dynamic Multi-Pathing, and you do not intend to upgrade your Solaris version. Only use this procedure if you are already running a version of Solaris that is supported with 6.0.1.

To upgrade Veritas Dynamic Multi-Pathing

1. Log in as superuser.
2. Load and mount the disc.

   See "Mounting the product disc" on page 34.
3. To invoke the common installer, run the `installer` command on the disc as shown in this example:

   ```
   # cd /cdrom/cdrom0
   # ./installer
   ```
4. Enter `G` to upgrade and press Return.
5. You are prompted to enter the system names (in the following example, "host1"). Enter the system name or names and then press Return.

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

   Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.
6. Installer asks if you agree with the terms of the End User License Agreement. Press **y** to agree and continue.
7. You can perform this step if you upgrading from DMP 5.1 SP1 for Solaris; for x64 from DMP 5.1 SP1 RP1.

   The installer discovers if any of the systems that you are upgrading have mirrored and encapsulated boot disks. For each system that has a mirrored boot disk, you have the option to create a backup of the system's book disk group before the upgrade proceeds. If you want to split the boot disk group to create a backup, answer **y**.

   Note: Splitting the mirrors for the root disk group backup requires a reboot upon completion of the upgrade.

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

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

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

10 Stop the product's processes.

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

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

12 If the upgrade was done from 5.0 or if the Veritas Dynamic Multi-Pathing was done without vxkeyless keys, the installer shows the following warning:

```
CPI WARNING V-9-40-5323 DMP license version 5.0 is not
updated to 6.0 on sys1. It's recommended to upgrade to a 6.0 key.
CPI WARNING V-9-40-5323 DMP license version 5.0 is not updated
to 6.0 on sys2. It's recommended to upgrade to a 6.0 key.
DMP is licensed on the systems
Do you wish to enter additional licenses? [y,n,q,b] (n) n
```

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

14 Only perform this step if you have split the boot disk group into a backup disk group. After a successful reboot, verify the upgrade and re-join the backup disk group. If the upgrade fails, revert to the backup disk group.

Upgrading Veritas Dynamic Multi-Pathing using manual steps

This section describes upgrading from a previous version of Veritas Dynamic Multi-Pathing to the current Veritas Dynamic Multi-Pathing (6.0.1) when you do not intend to upgrade your Solaris version. Only use this procedure if you are already running a version of Solaris that is supported with 6.0.1.

To upgrade Veritas Dynamic Multi-Pathing

1. Unmount any mounted VxFS file systems.

   The installer supports the upgrade of multiple hosts, if each host is running the same version of VxVM and VxFS. Hosts must be upgraded separately if they are running different versions.

   If any VxFS file systems are mounted with the QuickLog feature, QuickLog must be disabled before upgrading. See the "Veritas QuickLog" chapter of the *Veritas File System Administrator's Guide* for more information.

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

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

   ```
   # pkgrm VRTSfsnbl
   ```

   or

   ```
   # pkg uninstall VRTSfsnbl
   ```

   Respond to any system messages as needed.

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

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

4. Load and mount the software disc.

   See "Mounting the product disc" on page 34.

5. Change to the directory containing the DMP packages.

   ```
   # cd /dvd_mount
   ```

6. Remove the Veritas packages from your existing installation.

   Refer to the *Veritas Dynamic Multi-Pathing Installation Guide* for the previous release to obtain the list of packages to remove.

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

   ```
   # ./installdmp -recpkgs
   ```

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

On Solaris 10:

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

On Solaris 11:

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

9 Configure the DMP installation using the `installdmp -configure` command.

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

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

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

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

To begin the upgrade

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

2 Load and mount the disc.

See "Mounting the product disc" on page 34.

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

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

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

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

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

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

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

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

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

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

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

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

- using the uninstalldmp script
- using pkgrm

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

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

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

Refer to the Solaris installation documentation.

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

- using the common installer
  See "To upgrade the Veritas Storage Foundation packages with the product installer" on page 89.
- using manual steps
  See "To upgrade the Veritas Storage Foundation packages with manual steps" on page 89.

To upgrade the Veritas Storage Foundation packages with the product installer

1. Load and mount the disc.

   See "Mounting the product disc" on page 34.

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

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

3. Select **I** to upgrade the product. The installer will ask you if you want to use the previous configuration.
4. Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.
5. If you commented out VxFS File System entries in the `/etc/vfstab` file, uncomment them.
6. Complete the upgrade by restoring the configuration.

To upgrade the Veritas Storage Foundation packages with manual steps

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

   For Veritas Storage Foundation for DB2:

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

   For Veritas Storage Foundation for Oracle:

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

2. Load and mount the software disc.
3. Change to the directory containing the packages.

   ```
   # cd /dvd_mount
   ```

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

```
./installdmp -recpkgs
```

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

```
./installdmp -allpkgs
```

5 Add packages with the `pkgadd` command.

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

7 Complete the upgrade by restoring the configuration.

Restoring the configuration and completing the upgrade

1 Complete the upgrade using the `upgrade_finish` script.

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

2 Configure the product using the following command:

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

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

- Reboot the systems.

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

Upgrading Veritas Dynamic Multi-Pathing using the Veritas Web-based installer

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

To upgrade DMP

1. Perform the required steps to save any data that you wish to preserve. For example, make configuration file backups.
2. Start the Web-based installer.

   See "Starting the Veritas Web-based installer" on page 42.
3. On the Select a task and a product page, select **Upgrade a Product** from the Task drop-down menu.

   The installer detects the product that is installed on the specified system. Click **Next**.
4. Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click **Next**.
5. Click **Next** to complete the upgrade.

   After the upgrade completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.
6. If you are prompted to reboot the systems, enter the following reboot command:

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

Upgrading the Solaris operating system

If you are running Veritas Dynamic Multi-Pathing 6.0.1 with an earlier release of the Solaris operating system, you can upgrade the Solaris operating system using the following procedure.

Warning: You should only use this procedure to upgrade the Solaris operating system if you are running Veritas Dynamic Multi-Pathing 6.0.1.

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

To upgrade the Solaris operating system only

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

   ```
   # init S
   ```

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

2. Load and mount the software disc from the currently installed version of Veritas Dynamic Multi-Pathing.

   See "Mounting the product disc" on page 34.

3. Change directory:

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

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

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

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

   ```
   # ./upgrade_start
   ```

6. Bring the system down to run level 0.

   ```
   # init 0
   ```

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

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

8. After installing the Solaris operating system, install any Solaris patches required by Veritas Dynamic Multi-Pathing 6.0.1.

   See the *Veritas Dynamic Multi-Pathing Release Notes*.

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

```
# init S
```

10 Ensure that `/opt` is mounted.

11 Load and mount the software disc from the currently installed version of Veritas Dynamic Multi-Pathing.

12 If you upgraded to Solaris 10, you must reinstall certain Veritas Dynamic Multi-Pathing packages in order to support Solaris 10 functionality.

To reinstall the required packages, follow the steps below:

- Remove the existing packages in the reverse order of their installation. For example, if you chose the installation of all packages then uninstall those in the following order.
- Run the following commands.
  To obtain a list of recommended packages to install:

  ```
  # ./installdmp -recpkgs
  ```

  Or
  To obtain a list of all packages to install:

  ```
  # ./installdmp -allpkgs
  ```

- Change to the directory containing the appropriate packages.

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

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

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

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

Upgrading language packages

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

Install the language packages as for an initial installation.

See “Installing language packages” on page 39.

Chapter 13

Upgrading DMP using Live Upgrade

This chapter includes the following topics:

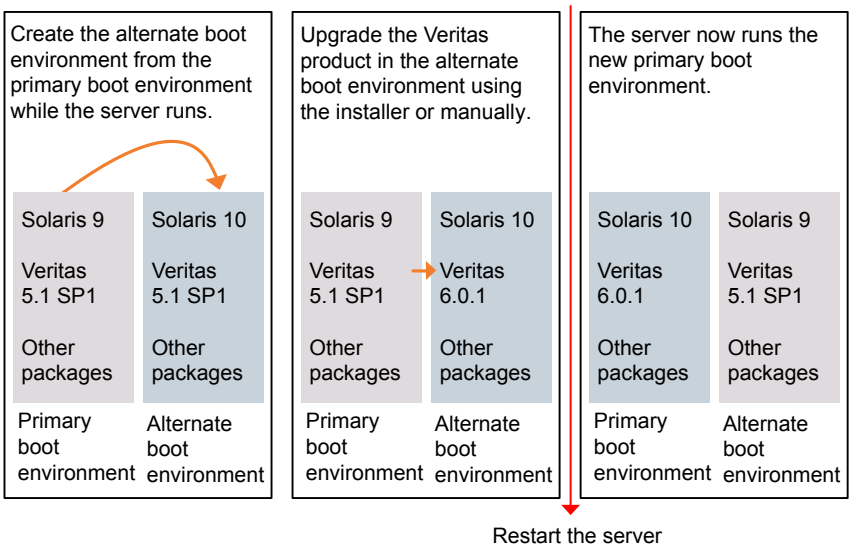
About Live Upgrade

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

- Upgrade the operating system and DMP.
  See "Upgrading DMP and Solaris using Live Upgrade" on page 98.
- Upgrade the operating system.
  See "Upgrading Solaris using Live Upgrade" on page 102.
- Upgrade DMP.
  See "Upgrading DMP using Live Upgrade" on page 103.

Figure 13-1 illustrates an example of an upgrade of Veritas products from 5.1 SP1 to 6.0.1, and the operating system from Solaris 9 to Solaris 10.

Figure 13-1 Live Upgrade process



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

Supported upgrade paths for Live Upgrade

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

DMP version must be at least 5.1 SP1.

You can use Live Upgrade in the following virtualized environments:

Table 13-1 Live Upgrade support in virtualized environments

Environment	Procedure
Solaris native zones	Perform Live Upgrade to upgrade both global and non-global zones. See "Upgrading DMP and Solaris using Live Upgrade" on page 98.

Table 13-1 Live Upgrade support in virtualized environments *(continued)*

Environment	Procedure
Solaris branded zones (BrandZ)	Perform Live Upgrade to upgrade the global zone. See "Upgrading DMP and Solaris using Live Upgrade" on page 98. Manually upgrade the branded zone separately. Note that while you can perform a Live Upgrade in the presence of branded zones, the branded zones are not upgraded.
Oracle VM Server for SPARC	Perform Live Upgrade on the Control domain only. Perform Live Upgrade on the Guest domain only. Use the standard Live Upgrade procedure for both types of logical domains. See "Upgrading DMP and Solaris using Live Upgrade" on page 98.

Before you upgrade DMP using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1. Make sure that the DMP installation media and the operating system installation images are available and on hand.
2. On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.
3. On the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.
4. The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     All Solaris versions: SUNWluu, SUNWlur packages.
     Solaris 10 update 7 or later also requires: SUNWlucfg package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:

All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.

Solaris installation media comes with a script for this purpose named liveupgrade20. Find the script at */cdrom/solaris_release*/Tools/Installers/liveupgrade20. If scripting, you can use:

```
# /cdrom/solaris_release/Tools/Installers/liveupgrade20 \
-nodisplay -noconsole
```

5 If the specified image is missing patches that are installed on the primary boot disk, note the patch numbers. To ensure that the alternate boot disk is the same as the primary boot disk, you need to install any missing patches on the alternate boot disk.

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

Upgrading DMP and Solaris using Live Upgrade

Upgrading DMP using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See "Before you upgrade DMP using Solaris Live Upgrade" on page 97.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 99.
- Upgrade to Veritas Dynamic Multi-Pathing 6.0.1 on the alternate boot environment manually or using the installer.

  To upgrade DMP manually, refer to the following procedure:

  - See "Upgrading DMP manually" on page 100.

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

  - See "Upgrading DMP using the installer for a Live Upgrade" on page 99.
- Switch the alternate boot environment to be the new primary.
  See "Completing the Live Upgrade " on page 101.
- Verify Live Upgrade of DMP.
  See "Verifying Live Upgrade of DMP" on page 101.

Creating a new boot environment on the alternate boot disk

Note: This step can take several hours to complete. Do not interrupt the session as it may leave the boot environment unstable.

At the end of the process:

- The Solaris operating system on the alternate boot disk is upgraded, if you have chosen to upgrade the operating system.
- A new boot environment is created on the alternate boot disk by cloning the primary boot environment.

To create a new boot environment on the alternate boot disk

1. View the list of VxVM disks on which you want to create the new boot environment.

   ```
   # vxdisk list
   ```

2. Review the output and note the new mount points. If the system is rebooted before completion of the upgrade or if the mounts become unmounted, you may need to remount the disks.

   If you need to remount, run the command:

3. After the alternate boot disk is created and mounted on */altroot.5.10*, install any operating system patches or packages on the alternate boot disk that are required for the Veritas product installation:

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

Upgrading DMP using the installer for a Live Upgrade

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

At the end of the process the following occurs:

- Veritas Dynamic Multi-Pathing 6.0.1 is installed on the alternate boot disk.

To perform Live Upgrade of DMP using the installer

1. Insert the product disc with Veritas Dynamic Multi-Pathing 6.0.1 or access your copy of the software on the network.
2. Run the installer script specifying the root path as the alternate boot disk, enter the following:

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

3 Enter the names of the nodes that you want to upgrade to Veritas Dynamic Multi-Pathing 6.0.1.

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

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

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

```
# pkginfo -R /altroot.5.10 -l VRTSpkgname
```

For example:

Review the installation logs at `/altroot.5.10/opt/VRTS/install/logs`.

Upgrading DMP manually

At the end of the process the following occurs:

- Veritas Dynamic Multi-Pathing 6.0.1 is installed on the alternate boot disk.

To perform Live Upgrade of DMP manually

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

- For Dynamic Multi-Pathing (DMP):

```
# pkgrm -R /altroot.5.10 \
VRTSsfmh VRTSaslapm VRTSvxvm VRTSspt VRTSvlic VRTSperl
```

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

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

- For DMP:

```
VRTSvlic.pkg VRTSperl.pkg VRTSspt.pkg VRTSvxvm.pkg VRTSaslapm.pkg
VRTSsfmh.pkg
```

For example:

```
# pkgadd -R /altroot.5.10 -d package_name.pkg
```

Where you replace *package_name.pkg* with a package's name, for example VRTSperl.pkg.

```
# pkgadd -R /altroot.5.10 -d VRTSperl.pkg
```

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

```
# pkginfo -R /altrootpath -l VRTSpkgname
```

For example:

```
# pkginfo -R /altroot.5.10 -l VRTSvxvm
```

Completing the Live Upgrade

At the end of the process:

- The alternate boot environment is activated.
- The system is booted from the alternate boot disk.

To complete the Live Upgrade

- **Note:** Do not use the reboot, halt, or uadmin commands to reboot the system. Use either the init or the shutdown commands to enable the system to boot using the alternate boot environment.

You can ignore the following error if it appears: ERROR: boot environment <dest.13445> already mounted on </altroot.5.10>.

```
# shutdown -g0 -y -i6
```

Verifying Live Upgrade of DMP

To ensure that Live Upgrade has completed successfully, vverify that the system have booted from the alternate boot environment.

To verify that Live Upgrade completed successfully

1 Verify that the alternate boot environment is active.

```
# lustatus
```

If the alternate boot environment is not active, you can revert to the primary boot environment.

See "Reverting to the primary boot environment" on page 104.

2 Perform other verification as required to ensure that the new boot environment is configured correctly.

Upgrading Solaris using Live Upgrade

Upgrading Solaris using Live Upgrade involves the following steps:

- Preparing to upgrade using Solaris Live Upgrade.
  See "Before you upgrade DMP using Solaris Live Upgrade" on page 97.
- Creating a new boot environment on the alternate boot disk
  See "Creating a new boot environment on the alternate boot disk" on page 99.
- Removing and reinstalling Veritas Dynamic Multi-Pathing 6.0.1 on the alternate boot environment:
  See "Removing and reinstalling DMP using the installer" on page 102.

Note: Do NOT configure the Veritas Dynamic Multi-Pathing 6.0.1

- Switching the alternate boot environment to be the new primary
  See "Completing the Live Upgrade " on page 101.
- Verifying Live Upgrade of DMP.
  See "Verifying Live Upgrade of DMP" on page 101.

Removing and reinstalling DMP using the installer

DMP has kernel components that are specific for Solaris operating system versions. When you use Solaris Live Upgrade to upgrade the Solaris operating system, you must complete these steps to ensure the correct version of DMP components are installed.

At the end of the process the following occurs:

- Veritas Dynamic Multi-Pathing 6.0.1 is installed on the alternate boot disk, with the correct binaries for the new operating system version

To remove and reinstall DMP using the installer

1 Uninstall using the uninstaller script, specifying the alternate boot disk as the root path:

```
# /opt/VRTS/install/uninstalldmp<version>
 -rootpath altrootpath
```

Where <version> is the specific release version.

See "About the Veritas installer" on page 22.

2 Enter the names of the nodes that you want to uninstall.

The installer displays the list of packages that will be uninstalled.

3 Press **Return** to continue.

4 DMP is uninstalled from the alt disk.

5 Insert the product disc with Veritas Dynamic Multi-Pathing 6.0 or access your copy of the software on the network.

6 Run the `installdmp` command specifying the rootpath, for example:

```
# installdmp -rootpath altrootpath
```

7 Enter the names of the systems where you plan to install the software. The installer displays the list of installation packages.

8 Press **Return** and continue with the installation.

Upgrading DMP using Live Upgrade

Perform the Live Upgrade manually or use the installer. The nodes will not form a cluster until all of the nodes are upgraded to Veritas Dynamic Multi-Pathing 6.0.1. At the end of the Live Upgrade of the last node, all the nodes must boot from the alternate boot environment and join the cluster.

Upgrading DMP using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See "Before you upgrade DMP using Solaris Live Upgrade" on page 97.
- Create a new boot environment on the alternate boot disk.
  See "Creating a new boot environment on the alternate boot disk" on page 99.
- Upgrade to Veritas Dynamic Multi-Pathing 6.0.1 on the alternate boot environment manually or using the installer. Refer to one of the following:

  To upgrade DMP manually:

- See “Upgrading DMP manually” on page 100.

To upgrade DMP using the installer:

- See “Upgrading DMP using the installer for a Live Upgrade” on page 99.

- Switch the alternate boot environment to be the new primary.
  See “Completing the Live Upgrade ” on page 101.
- Verify Live Upgrade of DMP.
  See “Verifying Live Upgrade of DMP” on page 101.

Administering boot environments

Use the following procedures to perform relevant administrative tasks for boot environments.

Reverting to the primary boot environment

If the alternate boot environment fails to start, you can revert to the primary boot environment.

Start the system from the primary boot environment in the PROM monitor mode.

Chapter 14

Performing post-upgrade tasks

This chapter includes the following topics:

Updating variables

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

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

Upgrading the Array Support Library

VxVM provides support for new disk arrays in the form of Array Support Library (ASL) software package.

Adding JBOD support for storage arrays for which there is not an ASL available

If an array is of type A/A-A, A/P or ALUA and a suitable ASL is not available, the array must be claimed as an JBOD of type A/P. This is to prevent path delays and I/O failures arising. As JBODs are assumed to be type A/A by default, you must create appropriate JBOD entries for such arrays.

To configure an A/A-A, A/P or ALUA array as a JBOD

1. Stop all applications, such as databases, from accessing VxVM volumes that are configured on the array, and unmount all VxFS file systems and Storage Checkpoints that are configured on the array.
2. Add the array as a JBOD of type A/P:

```
# vxddladm addjbod vid=SUN pid=T300 policy=ap
```

3. If you have not already done so, upgrade the Storage Foundation or VxVM software to 6.0.1. Device discovery will be performed during the upgrade, and the array will be claimed as a JBOD of appropriate type.

   If you have already upgraded your system to 6.0.1, run the following command to perform device discovery:

```
# vxdctl enable
```

4. Verify that the array has been added with the policy set to `APdisk`:

```
# vxddladm listjbod
VID   PID     Opcode Page Code Page Offset SNO length Policy
============================================================
SUN   T300    18     -1        36          12         APdisk
```

5. Check that the correct devices are listed for the array:

```
# vxdisk list
DEVICE     TYPE          DISK    GROUP    STATUS
APdisk_0   auto:cdsdisk  -       -        online invalid
APdisk_1   auto:cdsdisk  -       -        online invalid
APdisk_2   auto:cdsdisk  -       -        online invalid
...
```

Unsuppressing DMP for EMC PowerPath disks

This section is only applicable if you are upgrading a system that includes EMC PowerPath disks.

In releases of VxVM before 4.1, a combination of DMP subpaths and the controllers of DMP subpaths were usually suppressed to prevent interference between DMP and the EMC PowerPath multi-pathing driver. Suppression has the effect of hiding these subpaths and their controllers from DMP, and as a result the disks on these subpaths and controllers cannot be seen by VxVM.

VxVM 4.1 and later releases have the ability to discover EMCpower disks, and configure them as autodiscovered disks that DMP recognizes are under the control of a separate multi-pathing driver. This has the benefit of allowing such disks to reconfigured in cluster-shareable disk groups. Before upgrading to VxVM 6.0.1, you must remove the suppression of the subpaths and controllers so that DMP can determine the association between EMCpower metadevices and `c#t#d#` disk devices.

In the following scenarios, you may need to unsuppress DMP subpaths and controllers:

- Converting a foreign disk
  See "Converting a foreign disk to auto:simple" on page 107.
- Converting a defined disk
  See "Converting a defined disk to auto:simple" on page 110.
- Converting a powervxvm disk
  See "Converting a powervxvm disk to auto:simple" on page 113.

Because emcpower disks are auto-discovered, the powervxvm script should be disabled and removed from the startup script. To remove the powervxvm script, use the command:

```
# powervxvm remove
```

Converting a foreign disk to auto:simple

Release 4.0 of VxVM provided the `vxddladm addforeign` command to configure foreign disks with default disk offsets for the private and public regions, and to define them as simple disks. A foreign disk must be manually converted to `auto:simple` format before upgrading to VxVM 6.0.1.

If the foreign disk is defined on a slice other than `s2`, you must copy the partition entry for that slice to that for `s0` and change the tag. If the tag of the original slice is changed, the status of the disk is seen as `online:aliased` after the upgrade.

The following example is used to illustrate the procedure. The `vxdisk list` command can be used to display the EMCpower disks that are known to VxVM:

```
# vxdisk list
DEVICE          TYPE            DISK    GROUP   STATUS
c6t0d12s2       auto:sliced     -       -       online
emcpower10c     simple          fdisk   fdg     online
...
```

The `vxprint` command is used to display information about the disk group, `fdg`:

```
# vxprint
Disk group: fdg
TY NAME    ASSOC        KSTATE   LENGTH    PLOFFS   STATE TUTIL0 PUTIL0
dg fdg     fdg          -        -         -        -     -      -
dm fdisk   emcpower10c  -        17673456  -        -     -      -
...
```

To convert a foreign disk to `auto:simple` format

1 Stop all the volumes in the disk group, and then deport it:

```
# vxvol -g fdg stopall
# vxdg deport fdg
```

2 Use the `vxddladm` command to remove definitions for the foreign devices:

```
# vxddladm rmforeign blockpath=/dev/dsk/emcpower10c \
  charpath=/dev/rdsk/emcpower10c
```

If you now run the `vxdisk list` command, the EMCpower disk is no longer displayed:

```
# vxdisk list
DEVICE       TYPE           DISK   GROUP   STATUS
c6t0d12s2    auto:sliced    -      -       online
...
```

3 Run the `vxprtvtoc` command to retrieve the partition table entry for the device:

```
# /etc/vx/bin/vxprtvtoc -f /tmp/vtoc /dev/rdsk/emcpower10c
```

4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```
# /etc/vx/bin/vxedvtoc -f /tmp/vtoc /dev/rdsk/emcpower10c

# THE ORIGINAL PARTITIONING IS AS FOLLOWS:
# SLICE     TAG  FLAGS   START  SIZE
  0         0x0  0x201   0      0
  1         0x0  0x200   0      0
  2         0x5  0x201   0      17675520

# THE NEW PARTITIONING WILL BE AS FOLLOWS:
# SLICE     TAG  FLAGS    START  SIZE
  0         0xf  0x201    0      17675520
  1         0x0  0x200    0      0
  2         0x5  0x201    0      17675520

DO YOU WANT TO WRITE THIS TO THE DISK ? [Y/N] :Y
WRITING THE NEW VTOC TO THE DISK #
```

5 Upgrade to VxVM 6.0.1 using the appropriate upgrade procedure.

6 After upgrading VxVM, use the `vxdisk list` command to validate the conversion to `auto:simple` format:

```
# vxdisk list
DEVICE          TYPE            DISK    GROUP   STATUS
c6t0d12s2       auto:sliced     -       -       online
emcpower10s2    auto:simple     -       -       online
...
```

To display the physical device that is associated with the metadevice, `emcpower10s2`, enter the following command:

```
# vxdmpadm getsubpaths dmpnodename=emcpower10s2
```

7 Import the disk group and start the volumes:

```
# vxdg import fdg
# vxvol -g fdg startall
```

You can use the `vxdisk list` command to confirm that the disk status is displayed as `online:simple`:

```
# vxdisk list
DEVICE          TYPE            DISK    GROUP   STATUS
c6t0d12s2       auto:sliced     -       -       online
emcpower10s2    auto:simple     fdisk   fdg     online
```

Converting a defined disk to auto:simple

In VxVM 4.0, and particularly in prior releases, EMCpower disks could be defined by a persistent disk access record (`darec`), and identified as simple disks. If an EMCpower disk is defined with a persistent `darec`, it must be manually converted to `auto:simple` format before upgrading to VxVM 6.0.1.

If the defined disk is defined on a slice other than `s2`, you must copy the partition entry for that slice to that for `s0` and change the tag. If the tag of the original slice is changed, the status of the disk is seen as `online:aliased` after the upgrade.

The following example is used to illustrate the procedure. The `ls` command shows the mapping of the EMC disks to persistent disk access records:

```
# ls -l /dev/vx/dmp/emcdisk1
lrwxrwxrwx 1 root other 36 Sep 24 17:59 /dev/vx/dmp/emcdisk1->
/dev/dsk/c6t0d11s5
# ls -l /dev/vx/rdmp/emcdisk1
```

```
lrwxrwxrwx 1 root other 40Sep 24 17:59 /dev/vx/rdmp/emcdisk1->
/dev/dsk/c6t0d11s5
```

Here the fifth partition of `c6t0d11s5` is defined as the persistent disk access record `emcdisk1`.

The `vxdisk list` command can be used to display the EMCpower disks that are known to VxVM:

```
# vxdisk list
DEVICE        TYPE           DISK   GROUP   STATUS
c6t0d12s2     auto:sliced    -      -       online
emcdisk1      simple         fdisk  fdg     online
...
```

The `vxprint` command is used to display information about the disk group, `fdg`:

```
# vxprint
Disk group: fdg
TY NAME    ASSOC     KSTATE  LENGTH    PLOFFS  STATE TUTIL0 PUTIL0
dg fdg     fdg       -       -         -       -     -      -
dm fdisk   emcdisk1  -       17673456  -       -     -      -
...
```

To convert a disk with a persistent disk access record to auto:simple format

1. Stop all the volumes in the disk group, and then deport it:

   ```
   # vxvol -g fdg stopall
   # vxdg deport fdg
   ```

2. Use the `vxdisk rm` command to remove the persistent record definitions:

   ```
   # vxdisk rm emcdisk1
   ```

   If you now run the `vxdisk list` command, the EMCpower disk is no longer displayed:

   ```
   # vxdisk list
   DEVICE       TYPE           DISK  GROUP   STATUS
   c6t0d12s2    auto:sliced    -     -       online
   ...
   ```

3. Use the `vxprtvtoc` command to retrieve the partition table entry for the device:

   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/hdisk /dev/rdsk/c6t0d11s2
   ```

4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```
# /etc/vx/bin/vxedvtoc -f /tmp/hdisk /dev/rdsk/c6t0d11s2

# THE ORIGINAL PARTITIONING IS AS FOLLOWS:
# SLICE     TAG  FLAGS    START   SIZE
  4         0x0  0x200    0       0
  5         0x0  0x200    3591000 2100375
  6         0x0  0x200    0       0

# THE NEW PARTITIONING WILL BE AS FOLLOWS:
# SLICE     TAG  FLAGS    START   SIZE
  4         0x0  0x200    0       0
  5         0xf  0x200    3591000 2100375
  6         0x0  0x200    0       0

DO YOU WANT TO WRITE THIS TO THE DISK ? [Y/N] :Y
WRITING THE NEW VTOC TO THE DISK #
```

5 Upgrade to VxVM 6.0.1 using the appropriate upgrade procedure.

6 After upgrading VxVM, use the `vxdisk list` command to validate the conversion to `auto:simple` format:

```
# vxdisk list
DEVICE           TYPE           DISK  GROUP  STATUS
c6t0d12s2        auto:sliced    -     -      online
emcpower10s2     auto:simple    -     -      online:aliased
...
```

To display the physical device that is associated with the metadevice, `emcpower10s2`, enter the following command:

```
# vxdmpadm getsubpaths dmpnodename=emcpower10s2
```

7 Import the disk group and start the volumes:

```
# vxdg import fdg
# vxvol -g fdg startall
```

You can use the `vxdisk list` command to confirm that the disk status is displayed as `online:simple`:

```
# vxdisk list
DEVICE            TYPE           DISK   GROUP  STATUS
c6t0d12s2         auto:sliced    -      -      online
emcpower10s2      auto:simple    fdisk  fdg    online:aliased
```

To allow DMP to receive correct enquiry data, the common Serial Number (C-bit) Symmetrix Director parameter must be set to enabled.

Converting a powervxvm disk to auto:simple

In VxVM 4.0, and particularly in prior releases, EMCpower disks could be defined by a persistent disk access record (darec) using powervxvm script, and identified as simple disks. If an EMCpower disk is used using powervxvm, it must be manually converted to auto:simple format before upgrading to VxVM 6.0.1.

If there are any controllers or devices that are suppressed from VxVM as powervxvm requirement, then such controllers/disks must be unsuppressed. This is required for Veritas DMP to determine the association between PowerPath metanodes and their subpaths. After the conversion to auto:simple is complete, the powervxvm script is no longer useful, and should be disabled from startup script.

The following example is used to illustrate the procedure. The `ls` command shows the mapping of the EMC disks to persistent disk access records:

```
# ls -l /dev/vx/rdmp/
crw-------   1 root     root     260, 76 Feb  7 02:36 emcpower0c

# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
emcpower0c   simple          ppdsk01      ppdg         online

# vxprint
Disk group: fdg
TY NAME     ASSOC      KSTATE  LENGTH   PLOFFS STATE TUTIL0 PUTIL0
dg ppdg     ppdg       -       -        -      -     -      -
dm ppdsk01  emcpower0c -       2094960  -      -     -      -
```

To convert an EMCpower disk (defined using powervxvm) to auto:simple format

1 Stop all the volumes in the disk group, and then deport it:

```
# vxvol -g ppdg stopall
# vxdg deport ppdg
```

2 Use the `vxdisk rm` command to remove all emcpower disks from VxVM:

```
# vxdisk rm emcpower0c
```

If you now run the `vxdisk list` command, the EMCpower disk is no longer displayed:

```
# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
```

3 Use the `vxprtvtoc` command to retrieve the partition table entry for this device:

```
# /etc/vx/bin/vxprtvtoc -f /tmp/vtoc /dev/vx/rdmp/emcpower0c
```

4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```
# /etc/vx/bin/vxedvtoc -f /tmp/vtoc /dev/vx/rdmp/emcpower0c
# THE ORIGINAL PARTITIONING IS AS FOLLOWS:
# SLICE     TAG  FLAGS   START  SIZE
  0         0x0  0x201   0      0
  1         0x0  0x200   0      0
  2         0x5  0x201   0      17675520

# THE NEW PARTITIONING WILL BE AS FOLLOWS:
# SLICE     TAG  FLAGS   START  SIZE
  0         0xf  0x201   0      17675520
  1         0x0  0x200   0      0
  2         0x5  0x201   0      17675520

DO YOU WANT TO WRITE THIS TO THE DISK ? [Y/N] :Y
WRITING THE NEW VTOC TO THE DISK #
```

5 Upgrade to VxVM 6.0.1 using the appropriate upgrade procedure.

6 After upgrading VxVM, use the `vxdisk list` command to validate the conversion to auto:simple format:

```
# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
emcpower0s2  auto:simple       -            -          online
```

7 Import the disk group and start the volumes.

```
# vxdg import ppdg
# vxvol -g ppdg startall
# vxdisk list

DEVICE       TYPE            DISK         GROUP        STATUS
c6t0d12s2    auto:sliced       -            -          online
emcpower0s2  auto:simple     ppdsk01       ppdg         online
```

Verifying the Veritas Dynamic Multi-Pathing upgrade

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

See "Verifying that the products were installed" on page 69.

Section 5

Uninstallation of DMP

Chapter 15

Uninstalling DMP

This chapter includes the following topics:

About removing Veritas Dynamic Multi-Pathing

This section covers uninstallation requirements and steps to uninstall the Veritas software.

Only users with superuser privileges can uninstall Veritas Dynamic Multi-Pathing.

Warning: Failure to follow the instructions in the following sections may result in unexpected behavior.

Preparing to uninstall

Review the following removing the Veritas software.

Remote uninstallation

You must configure remote communication to uninstall DMP on remote systems. In a High Availability environment, you must meet the prerequisites to uninstall on all nodes in the cluster at one time.

The following prerequisites are required for remote uninstallation:

- Communication protocols must exist between systems.By default, the uninstall scripts use ssh.
- You must be able to execute ssh or rsh commands as superuser on all systems.
- The ssh or rsh must be configured to operate without requests for passwords or passphrases.

See "About configuring secure shell or remote shell communication modes before installing products" on page 153.

Uninstalling DMP

Use the following procedure to remove Veritas Dynamic Multi-Pathing (DMP).

To uninstall DMP

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

   See "About configuring secure shell or remote shell communication modes before installing products" on page 153.

2. On the system where you plan to remove DMP, move to the /opt/VRTS/install directory.

3. Run the `uninstalldmp` command.

   ```
   # ./uninstalldmp<version>
   ```

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

   See "About the Veritas installer" on page 22.

4. When the installer prompts you, enter the names of each system where you want to uninstall DMP. Separate system names with spaces.

5. The installer program checks the systems. It then asks you if you want to stop DMP processes.

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

   If you respond yes, the processes are stopped and the packages are uninstalled.

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

7 Reboot all the nodes.

Uninstalling DMP with the Veritas Web-based installer

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

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

To uninstall DMP

1 Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 42.

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

4 Select **Veritas Dynamic Multi-Pathing** from the Product drop-down list, and click **Next**.

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

6 After the validation completes successfully, click **Next** to uninstall DMP on the selected system.

7 If there are any processes running on the target system, the installer stops the processes. Click **Next**.

8 After the installer stops the processes, the installer removes the products from the specified system.

Click **Next**.

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

10 Click **Finish**.

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

Uninstalling Veritas Dynamic Multi-Pathing using the pkgrm or pkg uninstall command

Use the following procedure to uninstall Veritas Dynamic Multi-Pathing using the pkgrm command.

If you are uninstalling Veritas Dynamic Multi-Pathing using the pkgrm command, the packages must be removed in a specific order, or else the uninstallation will fail. Removing the packages out of order will result in some errors, including possible core dumps, although the packages will still be removed.

To uninstall Veritas Dynamic Multi-Pathing

1 Unmount all mount points for file systems and Storage Checkpoints.

```
# umount /mount_point
```

Note: Comment out or remove any Veritas File System (VxFS) entries from the file system table `/etc/vfstab`. Failing to remove these entries could result in system boot problems later.

2 Stop all applications from accessing VxVM volumes, and close all volumes.

3 Stop various daemons, if applicable.

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

4 Remove the packages in the following order:

For Veritas Dynamic Multi-Pathing (Solaris 10):

```
# pkgrm VRTSsfcpi601 VRTSsfmh VRTSaslapm VRTSvxvm
VRTSspt VRTSperl VRTSvlic
```

For Veritas Dynamic Multi-Pathing (Solaris 11):

```
# pkg uninstall VRTSsfcpi601 VRTSsfmh VRTSaslapm VRTSvxvm
VRTSspt VRTSperl VRTSvlic
```

Uninstalling the language packages using the pkgrm command

If you would like to remove only the language packages, you can do so with the `pkgrm` command.

If you use the product installer menu or the uninstallation script, you can remove the language packages along with the English packages.

To remove the language packages

- Use the `pkgrm` command to remove the appropriate packages.

```
# pkgrm package_name package_name ...
```

Because the packages do not contain any dependencies, you can remove them in any order.

Section 6

Installation reference

Appendix A

Installation scripts

This appendix includes the following topics:

Command options for the installation script

The `installdmp` command usage takes the following form:

```
installdmp [ system1 system2... ]
 [ -configure | -license | -precheck | -requirements
  | -start | -stop | -upgrade | -postcheck ]
 [ -logpath log_path ]
 [ -responsefile response_file ]
 [ -tmppath tmp_path ]
 [ -tunablesfile tunables_file ]
 [ -timeout timeout_value ]
 [ -hostfile hostfile_path ]

 [ -keyfile ssh_key_file ]

 [ -pkgpath pkg_path ]

 [ -rootpath root_path ]
```

Only on Solaris 10:

```
 [ -jumpstart jumpstart_path ]

 [ -flash_archive flash_archive_path ]
```

Only on Solaris 11:

```
 [ -ai ai_path ]

[ -rsh | -redirect | -installminpkgs | -installrecpkgs
        | -installallpkgs    | -minpkgs | -recpkgs | -allpkgs
        | -pkgset | -pkginfo | -serial | -comcleanup | -makeresponsefile
        | -pkgtable | -version | -nolic | -settunables | -tunables ]
```

Table A-1 lists the `installdmp` command options.

Table A-1 installdmp options

Option and Syntax	Description
`-ai`	The `-ai` option is supported on Solaris 11 only, and is used to generate Automated Installation manifest. This can be used by Solaris Automated Installation Server to install the Symantec product, along with the Solaris 11 operation system. An available location to store the installation manifests must be specified as a complete path.
`-allpkgs`	View a list of all DMP packages and patches. The installdmp lists the packages and patches in the correct installation order. You can use the output to create scripts for command-line installation, or for installations over a network. See the -minpkgs and the -recpkgs options.
`-comcleanup`	The `-comcleanup` option removes the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.
`-configure`	Configure DMP after using `-install` option to install DMP.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
-hostfile*full_path_to_file*	Specifies the location of a file that contains the system names for the installer.
-installallpkgs	Selects all the packages for installation. See the -allpkgs option.
-installminpkgs	Selects the minimum packages for installation. See the -minpkgs option.
-installrecpkgs	Selects the recommended packages for installation. See the -recpkgs option.
-jumpstart *dir_path*	Use this option to generate the finish scripts that the Solaris JumpStart Server can use for Veritas products. The *dir_path* indicates the path to an existing directory where the installer must store the finish scripts.
-keyfile *ssh_key_file*	Specifies a key file for SSH. The option passes -i *ssh_key_file* with each SSH invocation.
-license	Register or update product licenses on the specified systems. This option is useful to replace a demo license.
-logpath *log_path*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where install log files, summary files, and response files are saved.
-makeresponsefile	Create a response file. This option only generates a response file and does not install DMP.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-minpkgs`	View a list of the minimal packages and the patches that are required for DMP. The installdmp lists the packages and patches in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -recpkgs options.
`-nolic`	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
`-osversion`	View the list of packages and patches that apply to the specified Solaris version. Valid values are `sol8`, `sol9`, or `sol10`. Use this option with one of the following options: ■ -allpkgs ■ -minpkgs ■ -recpkgs ■ -jumpstart
`-pkginfo`	Displays a list of packages in the order of installation in a user-friendly format. Use this option with one of the following options: ■ -allpkgs If you do not specify an option, -allpkgs is used by default. ■ -minpkgs ■ -recpkgs

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-pkgpath` *pkg_path*	Specifies that *pkg_path* contains all packages that the installdmp is about to install on all systems. The *pkg_path* is the complete path of a directory, usually NFS mounted.
`-pkgset`	Discovers and lists the 6.0.1 packages installed on the systems that you specify.
`-pkgtable`	Displays the DMP 6.0.1 packages in the correct installation order.
`-postcheck`	Checks that the processes are running and other post-installation checks.
`-precheck`	Verify that systems meet the installation requirements before proceeding with DMP installation. Symantec recommends doing a precheck before you install DMP.
`-recpkgs`	View a list of the recommended packages and the patches that are required for DMP. The installdmp lists the packages and patches in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -minpkgs options.
`-redirect`	Specifies that the installer need not display the progress bar details during the installation.
`-requirements`	View a list of required operating system version, required patches, file system space, and other system requirements to install DMP.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-responsefile` *response_file*	Perform automated DMP installation using the system and the configuration information that is 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. See "Installing DMP using response files" on page 138. See "Upgrading DMP using response files" on page 138.
`-rootpath` *root_path*	Specifies that root_path is the root location for the installation of all packages. On Solaris, `-rootpath` passes `-R` *root_path* to pkgadd command.
`-rsh`	Specifies that *rsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *rsh* commands between systems execute without prompting for passwords or confirmations
`-serial`	Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-settunables`	Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the `-tunablesfile` option.
`-start`	Starts the daemons and processes for DMP. If the installdmp failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -stop option. See "Starting and stopping processes for the Veritas products " on page 70.
`-stop`	Stops the daemons and processes for DMP. If the installdmp failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -start option. See "Starting and stopping processes for the Veritas products " on page 70.
`-timeout`	The `-timeout` option is used to specify the number of seconds that the script must wait for each command to complete before timing out. Setting the `-timeout` option overrides the default value of 1200 seconds. Setting the `-timeout` option to 0 prevents the script from timing out. The `-timeout` option does not work with the `-serial` option.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-tmppath` *tmp_path*	Specifies that *tmp_path* is the working directory for installdmp. This path is different from the /var/tmp path. This destination is where the installdmp performs the initial logging and where the installdmp copies the packages on remote systems before installation.
`-tunables`	Lists all supported tunables and create a tunables file template.
`-tunablesfile`	Specify this option when you specify a tunables file. The tunables file should include tunable parameters.
`-upgrade`	Upgrades the installed packages on the systems that you specify.
`-version`	Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.

Command options for uninstall script

The `uninstalldmp` command usage takes the following form:

```
uninstalldmp [ <system1> <system2>... ]
        [ -logpath <log_path> ]
        [ -responsefile <response_file> ]
        [ -tmppath <tmp_path> ]
        [ -timeout <timeout_value> ]
        [ -hostfile <hostfile_path> ]
        [ -keyfile <ssh_key_file> ]

     [ -rootpath <rootpath> ]
```

```
[ -rsh | -redirect | -serial | -comcleanup
          | -makeresponsefile | -version ]
```

Table A-2 lists the `uninstalldmp` command options.

Table A-2 uninstalldmp options

Option and Syntax	Description
`-comcleanup`	The `-comcleanup` option removes the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.
`-hostfile`*full_path_to_file*	Specifies the location of a file that contains the system names for the installer.
`-keyfile` *ssh_key_file*	Specifies a key file for SSH. The option passes `-i` *ssh_key_file* with each SSH invocation.
`-logpath` *log_path*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where uninstalldmp log files, summary file, and response file are saved.
`-makeresponsefile`	Use this option to create a response file or to verify that your system configuration is ready for uninstalling DMP.
`-redirect`	Displays progress details without showing progress bar.
`-responsefile` *response_file*	Perform automated DMP uninstallation using the system and the configuration information that is 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. See "Uninstalling DMP using response files" on page 139.
`-rootpath` *root_path*	Specifies that *root_path* is the root location for uninstalling all packages. On Solaris, `-rootpath` passes `-R` *root_path* to pkgrm command.
`-rsh`	Specifies that *rsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *rsh* commands between systems execute without prompting for passwords or confirmations

Table A-2 uninstalldmp options *(continued)*

Option and Syntax	Description
`-serial`	Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.
`-tmppath` *tmp_path*	Specifies that *tmp_path* is the working directory for uninstalldmp. This path is different from the /var/tmp path. This destination is where the uninstalldmp performs the initial logging and where the installdmp copies the packages on remote systems before installation.
`-timeout`	The -timeout option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the `-timeout` option overrides the default value of 1200 seconds. Setting the `-timeout` option to 0 will prevent the script from timing out. The `-timeout` option does not work with the `-serial` option.
`-version`	Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable.

Appendix B

Automated installation using response files

This appendix includes the following topics:

About response files

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

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

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

Installing DMP using response files

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

To install DMP using response files

1. Make sure the systems where you want to install DMP meet the installation requirements.
2. Make sure the preinstallation tasks are completed.
3. Copy the response file to the system where you want to install DMP.
4. Edit the values of the response file variables as necessary.
5. Mount the product disc and navigate to the directory that contains the installation program.
6. Start the installation from the system to which you copied the response file. For example:

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

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

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

   See "About the Veritas installer" on page 22.

Upgrading DMP using response files

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

To perform automated DMP upgrade

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

5 Mount the product disc and navigate to the folder that contains the installation program.

6 Start the upgrade from the system to which you copied the response file. For example:

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

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

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

See "About the Veritas installer" on page 22.

Uninstalling DMP using response files

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

To perform an automated uninstallation

1 Make sure that you meet the prerequisites to uninstall DMP.

2 Copy the response file to one of the cluster systems where you want to uninstall DMP.

3 Edit the values of the response file variables as necessary.

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

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

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

See "About the Veritas installer" on page 22.

Syntax in the response file

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

For example, in the case of a string value:

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

or, in the case of an integer value:

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

or, in the case of a list:

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

Response file variable definitions

Table B-1 lists the variables that are used in the response file and their definitions.

Table B-1 Response file variables

Variable	Description
CFG{opt}{install}	Installs DMP packages. Configuration can be performed at a later time using the `-configure` option. List or scalar: scalar Optional or required: optional
CFG{accepteula}	Specifies whether you agree with the EULA.pdf file on the media. List or scalar: scalar Optional or required: required
$CFG{opt}{vxkeyless}	Installs the product with keyless license. List of scalar: scalar Optional or required: optional
CFG{systems}	List of systems on which the product is to be installed, uninstalled, or configured. List or scalar: list Optional or required: required
CFG{prod}	Defines the product to be installed, uninstalled, or configured. List or scalar: scalar Optional or required: required

Table B-1 Response file variables *(continued)*

Variable	Description
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{patchpath}	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{pkgpath}	Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{rsh}	Defines that *rsh* must be used instead of ssh as the communication method between systems. List or scalar: scalar Optional or required: optional
$CFG{vm_restore_cfg}{system1}	Indicates whether a previous VM configuration should be restored. 0: indicates do not restore 1: indicates do restore. List or scalar: Scalar Optional or required: optional

Table B-1 Response file variables *(continued)*

Variable	Description
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional
CFG{opt}{configure}	Performs the configuration after the packages are installed using the `-install` option. List or scalar: scalar Optional or required: optional
CFG{opt}{upgrade}	Upgrades all packages installed, without configuration. List or scalar: list Optional or required: optional
CFG{opt}{uninstall}	Uninstalls DMP packages. List or scalar: scalar Optional or required: optional

Appendix C

Tunable files for installation

This appendix includes the following topics:

About setting tunable parameters using the installer or a response file

You can set non-default product and system tunable parameters using a tunables file. With the file, you can set tunables such as the I/O policy or toggle native multi-pathing. The tunables file passes arguments to the installer script to set tunables. With the file, you can set the tunables for the following operations:

- When you install, configure, or upgrade systems.

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

  See "Setting tunables for an installation, configuration, or upgrade" on page 144.

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

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

See "Setting tunables with no other installer-related operations" on page 145.

- When you apply the tunables file with an un-integrated response file.

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

See "Setting tunables with an un-integrated response file" on page 146.

See "About response files" on page 137.

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

See "Tunables value parameter definitions" on page 148.

Setting tunables for an installation, configuration, or upgrade

You can use a tunables file for installation procedures to set non-default tunables. You invoke the installation script with the `tunablesfile` option. The tunables file passes arguments to the script to set the selected tunables. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 148.

Note: Certain tunables only take effect after a system reboot.

To set the non-default tunables for an installation, configuration, or upgrade

1. Prepare the tunables file.

   See "Preparing the tunables file" on page 147.

2. Make sure the systems where you want to install DMP meet the installation requirements.
3. Complete any preinstallation tasks.
4. Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.
5. Mount the product disc and navigate to the directory that contains the installation program.
6. Start the installer for the installation, configuration, or upgrade. For example:

   ```
   # ./installer -tunablesfile /tmp/tunables_file
   ```

   Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with no other installer-related operations

You can use the installer to set tunable parameters without any other installer-related operations. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 148.

Note: Certain tunables only take effect after a system reboot.

To set tunables with no other installer-related operations

1 Prepare the tunables file.

See "Preparing the tunables file" on page 147.

2 Make sure the systems where you want to install DMP meet the installation requirements.

3 Complete any preinstallation tasks.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-settunables` option.

```
# ./installer -tunablesfile tunables_file_name -settunables [
sys123 sys234 ...]
```

Where /tmp/*tunables_file* is the full path name for the tunables file.

7 Proceed with the operation. When prompted, accept the tunable parameters.

Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See "Tunables value parameter definitions" on page 148.

Note: Certain tunables only take effect after a system reboot.

To set tunables with an un-integrated response file

1 Make sure the systems where you want to install DMP meet the installation requirements.

2 Complete any preinstallation tasks.

3 Prepare the tunables file.

See "Preparing the tunables file" on page 147.

4 Copy the tunables file to one of the systems that you want to tune.

5 Mount the product disc and navigate to the directory that contains the installation program.

6 Start the installer with the `-responsefile` and `-tunablesfile` options.

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

Where *response_file_name* is the full path name for the response file and *tunables_file_name* is the full path name for the tunables file.

7 Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

8 The installer validates the tunables. If an error occurs, exit the installer and check the tunables file.

Preparing the tunables file

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

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

To create a tunables file template

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

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

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

To manually format tunables files

- Format the tunable parameter as follows:

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

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

The following is an example of a tunables file.

```
#
# Tunable Parameter Values:
#
our %TUN;

$TUN{"tunable1"}{"*"}=1024;
$TUN{"tunable3"}{"sys123"}="SHA256";

1;
```

Setting parameters for the tunables file

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

See "Tunables value parameter definitions" on page 148.

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

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

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

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

Tunables value parameter definitions

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

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

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

Table C-1 Supported tunable parameters

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

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

Tunable	Description
dmp_fast_recovery	(Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_health_time	(Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_log_level	(Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_low_impact_probe	(Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_lun_retry_timeout	(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_fabric	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_ownership	(Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_multipathing	(Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

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

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

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

Tunable	Description
dmp_retry_count	(Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_scsi_timeout	(Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_sfg_threshold	(Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_stat_interval	(Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

Appendix D

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

About configuring secure shell or remote shell communication modes before installing products

Establishing communication between nodes is required to install Veritas software from a remote system, or to install and configure a system. The system from which the installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Veritas software.

You can install products to remote systems using either secure shell (ssh) or remote shell (rsh). Symantec recommends that you use ssh as it is more secure than rsh.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (system1) that

contains the installation directories, and a target system (system2). This procedure also applies to multiple target systems.

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

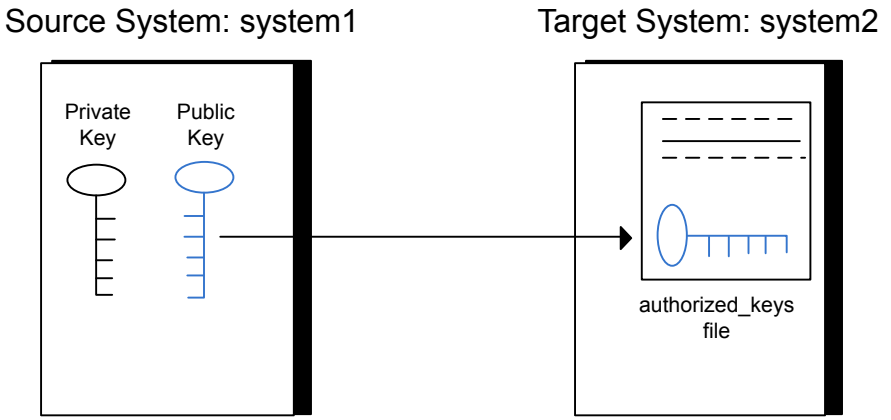
Manually configuring and passwordless ssh

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

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

Figure D-1 illustrates this procedure.

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



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

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

To create the DSA key pair

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

```
system1 # cd /
```

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

Solaris 10:

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

Solaris 11:

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

Change the permissions of this directory, to secure it.

Solaris 10:

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

Solaris 11:

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

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

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

System output similar to the following is displayed:

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

For Solaris 11:

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
```

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

5 When the program asks you to enter the passphrase, press the Enter key twice.

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

Do not enter a passphrase. Press Enter.

```
Enter same passphrase again:
```

Press Enter again.

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

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

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

```
PermitRootLogin           yes
  Subsystem          sftp      /usr/lib/ssh/sftp-server
```

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

To restart ssh on Solaris 10 and Solaris 11, type the following command:

```
system1 # svcadm restart ssh
```

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

Use the secure file transfer program.

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

Use the following command for secure file transfer:

```
system1 # sftp system2
```

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

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

4 Enter `yes`.

Output similar to the following is displayed:

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

5 Enter the root password of system2.

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

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

The following output is displayed:

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

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

```
sftp> quit
```

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

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

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

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

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

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

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

```
system2 # exit
```

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

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

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

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

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

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

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

To verify that you can connect to a target system

1 On the source system (system1), enter the following command:

```
system1 # ssh -l root system2 uname -a
```

where system2 is the name of the target system.

2 The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.

3 Repeat this procedure for each target system.

Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

To restart ssh

1 On the source installation system (system1), bring the private key into the shell environment.

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

2 Make the key globally available for the user `root`

```
system1 # ssh-add
```

Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system.

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

See "Manually configuring and passwordless ssh" on page 154.

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

To enable rsh

1. To determine the current status of `rsh` and `rlogin`, type the following command:

   ```
   # inetadm | grep -i login
   ```

   If the service is enabled, the following line is displayed:

   ```
   enabled online svc:/network/login:rlogin
   ```

   If the service is not enabled, the following line is displayed:

   ```
   disabled disabled svc:/network/login:rlogin
   ```

2. To enable a disabled `rsh`/`rlogin` service, type the following command:

   ```
   # inetadm -e rlogin
   ```

3. To disable an enabled `rsh`/`rlogin` service, type the following command:

   ```
   # inetadm -d rlogin
   ```

4. Modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. This file must be modified for each user who remotely accesses the system using rsh. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access `system1` from `system2`, you must add an entry for `system2.`*`companyname`*`.com` in the `.rhosts` file on `system1`.

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

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

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

Appendix E

DMP components

This appendix includes the following topics:

Veritas Dynamic Multi-Pathing installation packages

Table E-1 shows the package name and contents for each English language package for Veritas Dynamic Multi-Pathing. The table also gives you guidelines for which packages to install based whether you want the minimum, recommended, or advanced configuration.

Table E-1 Veritas Dynamic Multi-Pathing packages

packages	Contents	Configuration
VRTSaslapm	Veritas Array Support Library (ASL) and Array Policy Module(APM) binaries Required for the support and compatibility of various storage arrays.	Minimum
VRTSperl	Perl 5.14.2 for Veritas.	Minimum
VRTSvlic	Veritas License Utilities Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.	Minimum
VRTSvxvm	Veritas Volume Manager binaries	Minimum

Table E-1 Veritas Dynamic Multi-Pathing packages *(continued)*

packages	Contents	Configuration
VRTSsfcpi601	Veritas Storage Foundation Common Product Installer The Storage Foundation Common Product installer package contains the scripts that perform the following: ■ installation ■ configuration ■ upgrade ■ uninstallation ■ adding nodes ■ removing nodes ■ etc. You can use this script to simplify the native operating system installations, configurations, and upgrades.	Minimum
VRTSsfmh	Veritas Storage Foundation Managed Host Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at: http://www.symantec.com/business/storage-foundation-manager	Recommended
VRTSspt	Veritas Software Support Tools	Recommended

Appendix F

Troubleshooting installation issues

This appendix includes the following topics:

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

What to do if you see a licensing reminder

In this release, you can install without a license key. In order to comply with the End User License Agreement, you must either install a license key or make the host managed by a Management Server. If you do not comply with these terms within 60 days, the following warning messages result:

```
WARNING V-365-1-1 This host is not entitled to run Veritas Storage
Foundation/Veritas Cluster Server.As set forth in the End User
```

```
License Agreement (EULA) you must complete one of the two options
set forth below. To comply with this condition of the EULA and
stop logging of this message, you have <nn> days to either:
- make this host managed by a Management Server (see
  http://go.symantec.com/sfhakeyless for details and free download),
  or
- add a valid license key matching the functionality in use on this host
  using the command 'vxlicinst'
```

To comply with the terms of the EULA, and remove these messages, you must do one of the following within 60 days:

- Install a valid license key corresponding to the functionality in use on the host. After you install the license key, you must validate the license key using the following command:

  ```
  # /opt/VRTS/bin/vxlicrep
  ```

- Continue with keyless licensing by managing the server or cluster with a management server.
  For more information about keyless licensing, see the following URL: http://go.symantec.com/sfhakeyless

About the VRTSspt package troubleshooting tools

The VRTSspt package provides a group of tools for troubleshooting a system and collecting information on its configuration. If you install and use the VRTSspt package, it will be easier for Symantec Support to diagnose any issues you may have.

The tools can gather Veritas File System and Veritas Volume Manager metadata information and establish various benchmarks to measure file system and volume manager performance. Although the tools are not required for the operation of any Veritas product, Symantec recommends installing them should a support case be needed to be opened with Symantec Support. Use caution when you use the VRTSspt package, and always use it in concert with Symantec Support.

Incorrect permissions for root on remote system

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

```
Failed to setup rsh communication on 10.198.89.241:
```

```
'rsh 10.198.89.241 <command>' failed
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied

Failed to login to remote system(s) 10.198.89.241.
Please make sure the password(s) are correct and superuser(root)
can login to the remote system(s) with the password(s).
If you want to setup rsh on remote system(s), please make sure
rsh with command argument ('rsh <host> <command>') is not
denied by remote system(s).

Either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication

Would you like the installer to setup ssh/rsh communication
automatically between the nodes?
Superuser passwords for the systems will be asked. [y,n,q] (y) n

System verification did not complete successfully

The following errors were discovered on the systems:

The ssh permission denied on 10.198.89.241
rsh exited 1 on 10.198.89.241
either ssh or rsh is needed to be setup between the local node
and 10.198.89.241 for communication
```

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

See "About configuring secure shell or remote shell communication modes before installing products" on page 153.

Note: Remove remote shell permissions after completing the DMP installation and configuration.

Inaccessible system

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

```
 Verifying systems: 12% .....................................
 Estimated time remaining: 0:10 1 of 8
 Checking system communication ............................. Done
System verification did not complete successfully
The following errors were discovered on the systems:
cannot resolve hostname host1
Enter the  system names separated by spaces: q,? (host1)
```

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

Appendix G

Compatability issues when installing DMP with other products

This appendix includes the following topics:

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSpbx, VRTSicsco, and VRTSat.

Index