Veritas™ Dynamic Multi-Pathing Installation Guide

HP-UX 11i v3

5.1 Service Pack 1

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: 5.1 SP1

Document version: 5.1SP1.0

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 website.

http://www.symantec.com/business/support/overview.jsp?pid=15107

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:

docs@symantec.com

About Symantec Connect

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

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

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

Technical Support 4

Section 1 Installation overview and planning 11

Chapter 1 Introducing Veritas Dynamic Multi-Pathing 13

About Veritas Dynamic Multi-Pathing 13

Chapter 2 Planning to install Veritas Dynamic Multi-Pathing 15

About planning for DMP installation 15
About installation and configuration methods 15

Chapter 3 System requirements 17

Release notes 17
Hardware compatibility list (HCL) 17
Supported HP-UX operating systems 18
Disk space requirements 18

Chapter 4 Licensing Veritas products 19

About Veritas product licensing 19
Setting or changing the product level for keyless licensing 20
Installing Veritas product license keys 22

Section 2 Installation of Veritas Dynamic Multi-Pathing 23

Chapter 5 Preparing to install Veritas Dynamic Multi-Pathing 25

Installation preparation overview 25
About configuring ssh or remsh using the Veritas installer 26
Creating the /opt directory 27

Setting environment variables 27
Mounting the product disc 27
Assessing system preparedness 28
Symantec Operations Readiness Tools 29
Prechecking your systems using the Veritas installer 29

Chapter 6 Installing Veritas Dynamic Multi-Pathing using the script-based installer 31

About the Veritas installer 31
Installing Veritas Dynamic Multi-Pathing 32
Performing a postcheck on a node 34

Chapter 7 Installing Veritas Dynamic Multi-Pathing using the web-based installer 35

About the Web-based installer 35
Features not supported with Web-based installer 36
Before using the Veritas Web-based installer 36
Starting the Veritas Web-based installer 37
Obtaining a security exception on Mozilla Firefox 37
Performing a pre-installation check with the Veritas Web-based installer 38
Installing DMP with the Web-based installer 38

Section 3 Verification of the installation 41

Chapter 8 Verifying the Veritas Dynamic Multi-Pathing installation 43

Verifying that the products were installed 43
Installation log files 43
Starting and stopping processes for the Veritas products 44

Section 4 Uninstallation of Veritas Dynamic Multi-Pathing 45

Chapter 9 Uninstalling Veritas Dynamic Multi-Pathing 47

Uninstalling DMP with the Veritas Web-based installer 47
Uninstalling Veritas Dynamic Multi-Pathing 48
Removing license files (Optional) 49

Section 5 Installation reference 51

Appendix A Installation scripts 53

Command options for the installation script 53
Command options for uninstall script 58

Appendix B Response files 61

About response files 61
Installing DMP using response files 61
Uninstalling DMP using response files 62
Syntax in the response file 63
Response file variable definitions 63

Appendix C Configuring the secure shell or the remote shell for communications 67

About configuring secure shell or remote shell communication modes before installing products 67
Configuring and enabling ssh 68
Enabling remsh 72

Appendix D Veritas Dynamic Multi-Pathing components 73

Veritas Dynamic Multi-Pathing installation depots 73

Appendix E Troubleshooting installation issues 75

Restarting the installer after a failed connection 75
What to do if you see a licensing reminder 75
Incorrect permissions for root on remote system 76
Resource temporarily unavailable 77
Inaccessible system 78

Index 79

Section 1

Installation overview and planning

- Chapter 1. Introducing Veritas Dynamic Multi-Pathing
- Chapter 2. Planning to install Veritas Dynamic Multi-Pathing
- Chapter 3. System requirements
- Chapter 4. Licensing Veritas products

Chapter 1

Introducing Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- About Veritas Dynamic Multi-Pathing

About Veritas Dynamic Multi-Pathing

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.

In previous Veritas releases, DMP was only available as a feature of Veritas Volume Manager (VxVM). DMP supported VxVM volumes on DMP metadevices, and Veritas File System (VxFS) file systems on those volumes.

This release extends DMP metadevices to support OS native logical volume managers (LVM). You can create LVM volumes and volume groups on DMP metadevices.

DMP does not support migrating the root LVM volume group onto DMP.

In this release, Veritas Dynamic Multi-Pathing does not support Veritas File System (VxFS) on DMP devices.

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

Chapter 2

Planning to install Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- About planning for DMP installation
- About installation and configuration methods

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 website.

http://www.symantec.com/business/support/overview.jsp?pid=15107

Document version: 5.1SP1.0.

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 one of the Veritas Dynamic Multi-Pathing products by Symantec.

Several component products are bundled with each of these DMP products.

About installation and configuration methods

You can install and configure DMP with Veritas installation programs or with 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. Otherwise, installing with the installation script is identical to 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.
  In this release, there are some limitations in the Web-based installer.
  See "About the Web-based installer" on page 35.
- 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 other systems.
  See "About response files" on page 61.

Chapter 3

System requirements

This chapter includes the following topics:

- Release notes
- Hardware compatibility list (HCL)
- Supported HP-UX operating systems
- Disk space requirements

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:

http://www.symantec.com/business/support/overview.jsp?pid=15107

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://entsupport.symantec.com/docs/330441

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

Supported HP-UX operating systems

This release of Veritas products can only be installed on a system running HP-UX B.11.31.1009, HP-UX 11i Version 3 September 2010 Operating Environments Update Release or later on the PA-RISC or Itanium platforms.

To verify the operating system version use the `swlist` command as follows:

```
# swlist | grep HPUX11i
HPUX11i-DC-OE     B.11.31.1009   HP-UX Data Center Operating Environment
```

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

To verify that JFS is installed use the `swlist` command as follows:

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

Disk space requirements

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

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

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

Chapter 4

Licensing Veritas products

This chapter includes the following topics:

- About Veritas product licensing
- Setting or changing the product level for keyless licensing
- Installing Veritas product license keys

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

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

If you upgrade to this release from a prior release of the Veritas software, the product installer does not change the license keys that are already installed. The existing license keys may not activate new features in this release.

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 20.
  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 22.
  See the `vxlicinst(1m)` manual page.

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

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

Setting or changing the product level for keyless licensing

The keyless licensing method uses product levels to determine the Veritas products and functionality that are licensed. In order to use keyless licensing, you must set up a Management Server to manage your systems.

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

http://go.symantec.com/vom

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

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

To set or change the product level

1 View the current setting for the product level.

```
# vxkeyless -v display
```

2 View the possible settings for the product level.

```
# vxkeyless displayall
```

3 Set the desired product level.

```
# vxkeyless -q set prod_levels
```

where *prod_levels* is a comma-separated list of keywords, as shown in step 2

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin

# ./vxlicinst -k xxxx-xxxx-xxxx-xxxx-xxxx-xxx
```

Section 2

Installation of Veritas Dynamic Multi-Pathing

- Chapter 5. Preparing to install Veritas Dynamic Multi-Pathing
- Chapter 6. Installing Veritas Dynamic Multi-Pathing using the script-based installer
- Chapter 7. Installing Veritas Dynamic Multi-Pathing using the web-based installer

Chapter 5

Preparing to install Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- Installation preparation overview
- About configuring ssh or remsh using the Veritas installer
- Creating the /opt directory
- Setting environment variables
- Mounting the product disc
- Assessing system preparedness

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 19.
Download the software, or insert the product DVD.	See "Mounting the product disc" on page 27.
Set environment variables.	See "Setting environment variables" on page 27.
Create the `/opt` directory, if it does not exist.	See "Creating the /opt directory" on page 27.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Configure the secure shell (ssh) on all nodes.	See "About configuring secure shell or remote shell communication modes before installing products" on page 67.
Verify that hardware, software, and operating system requirements are met.	See "Supported HP-UX operating systems" on page 18. 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 31.

About configuring ssh or remsh using the Veritas installer

The installer can configure passwordless secure shell (ssh) or remote shell (remsh) communications among systems. The installer uses the ssh or remsh 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. Note that for security reasons, the installation program neither stores nor caches these passwords. 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 remsh on the target systems. In the following scenarios, you need to set up ssh or remsh manually:

- When the root broker is outside of the cluster that you plan to configure.
- When you add new nodes to an existing cluster.
- When the nodes are in a sub-cluster during a phased upgrade.
- When you perform installer sessions using a response file.

See "About configuring secure shell or remote shell communication modes before installing products" on page 67.

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.

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
```

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 system from which you install DMP need not be part of the cluster. The systems must be in the same subnet.

2. Insert the product disc in the appropriate drive on your local system.

3 Determine the block device file for the DVD drive:

```
# ioscan -fnC disk
```

Make a note of the device file as it applies to your system.

4 Create a directory in which to mount the software disc and mount the disc using the appropriate drive name. For example:

```
# mkdir -p /dvdrom
# mount /dev/rdsk/c0t0d0 /dvdrom
```

5 Verify that the disc is mounted:

```
# mount
```

Assessing system preparedness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Veritas Dynamic Multi-Pathing 5.1SP1.

Symantec Operations Readiness Tools	Symantec Operations Readiness Tools (SORT) is a Web-based application that is designed to support Symantec enterprise products. See "Symantec Operations Readiness Tools" on page 29.
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 5.1SP1. See "Prechecking your systems using the Veritas installer" on page 29.

Symantec Operations Readiness Tools

Symantec™ Operations Readiness Tools (SORT) is a set of Web-based tools that supports Symantec enterprise products. SORT increases operational efficiency and helps improve application availability.

Among its broad set of features, SORT provides patches, patch notifications, and documentation for Symantec enterprise products.

To access SORT, go to:

http://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.
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 Veritas Dynamic Multi-Pathing using the script-based installer

This chapter includes the following topics:

- About the Veritas installer
- Installing Veritas Dynamic Multi-Pathing
- Performing a postcheck on a node

About the Veritas installer

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

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

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.

Additional options are available for the installer.

Installing Veritas Dynamic Multi-Pathing

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 67.

2. Load and mount the software disc.
3. Move to the top-level directory on the disc.
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, 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 depots for minimal functionality for the selected product.
   - A recommended installation installs the recommended DMP depots that provide complete functionality of the product.
     Note that this option is the default.
   - The display selection displays all depots and provides information about them. Note that the recommended installation installs the minimum and the recommended depots.

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 depots 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.

```
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 prompts you to reboot the system.

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-****
```

15 Reboot the system.

16 Start the DMP processes.

See “Starting and stopping processes for the Veritas products ” on page 44.

Performing a postcheck on a node

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

Note: This command option requires downtime for the system.

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 Veritas Dynamic Multi-Pathing using the web-based installer

This chapter includes the following topics:

- About the Web-based installer
- Features not supported with Web-based installer
- Before using the Veritas Web-based installer
- Starting the Veritas Web-based installer
- Obtaining a security exception on Mozilla Firefox
- Performing a pre-installation check with the Veritas Web-based installer
- Installing DMP with the Web-based installer

About the Web-based installer

Use the Web-based installer's 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 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 the files for auditing, debugging, and for 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 36.

See "Starting the Veritas Web-based installer" on page 37.

Features not supported with Web-based installer

In this release, the following features that can be performed using the script installer are not available in the Web-based installer:

- Configuring server-based I/O fencing
- Configuring non-SCSI3 I/O fencing in virtual environments where SCSI3 is not supported

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 5.1SP1.
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.

Table 7-1 Web-based installer requirements *(continued)*

System	Function	Requirements
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

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.

2 On the administrative server, start the Web browser.

3 Navigate to the URL that the script displayed.

4 The browser may display the following message:

```
Secure Connection Failed
```

Obtain a security exception for your browser.

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

Obtaining a security exception on Mozilla Firefox

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

To obtain a security exception

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

2 Click **Add Exception** button.

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 37.

2 On the Select a task and a product page, select **Perform a Pre-installation Check** from the **Task** drop-down list.

3 Select the product 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 **Validate**.

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 38.

2 Start the Web-based installer.

See "Starting the Veritas Web-based installer" on page 37.

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 depots. Click **Next**.

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

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 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**.

12 After the product is registered, the installer prompts you to reboot the system.

13 After the systems come up after reboot, start the Veritas Dynamic Multi-Pathing processes.

See "Starting and stopping processes for the Veritas products " on page 44.

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

Section 3

Verification of the installation

- Chapter 8. Verifying the Veritas Dynamic Multi-Pathing installation

Chapter 8

Verifying the Veritas Dynamic Multi-Pathing installation

This chapter includes the following topics:

- Verifying that the products were installed
- Installation log files
- Starting and stopping processes for the Veritas products

Verifying that the products were installed

Verify that the DMP products are installed.

You can use the `swlist` command to check which depots have been installed:

```
# swlist -l product | grep VRTS
```

See "Veritas Dynamic Multi-Pathing installation depots" on page 73.

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 depots, and the status (success or failure) of each depot. The summary also indicates which processes were stopped or restarted during the installation. After installation, refer to the summary file to determine whether any processes need to be started.

Starting and stopping processes for the Veritas products

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

To stop the processes

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

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

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

To start the processes

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

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

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

Section 4

Uninstallation of Veritas Dynamic Multi-Pathing

- Chapter 9. Uninstalling Veritas Dynamic Multi-Pathing

Chapter 9

Uninstalling Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- Uninstalling DMP with the Veritas Web-based installer
- Uninstalling Veritas Dynamic Multi-Pathing
- Removing license files (Optional)

Uninstalling DMP with the Veritas Web-based installer

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

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 37.
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 **Validate**.
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**.

The Web-based installer prompts you to reboot the system.

The Web-based installer prompts you for another task.

Uninstalling Veritas Dynamic Multi-Pathing

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 67.

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

3 Run the `uninstalldmp` command.

```
# ./uninstalldmp
```

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 depots 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.

Removing license files (Optional)

Optionally, you can remove the license files.

To remove the VERITAS license files

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

   ```
   # /sbin/vxlicrep
   ```

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

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

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

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

Section 5

Installation reference

- Appendix A. Installation scripts
- Appendix B. Response files
- Appendix C. Configuring the secure shell or the remote shell for communications
- Appendix D. Veritas Dynamic Multi-Pathing components
- Appendix E. Troubleshooting installation issues

Appendix A

Installation scripts

This appendix includes the following topics:

- Command options for the installation script
- Command options for uninstall script

Command options for the installation script

The `installdmp` command usage takes the following form:

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

 [ -keyfile ssh_key_file ]

[ -patchpath patch_path ]
 [ -pkgpath pkg_path ]

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

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

Table A-1 installdmp options

Option and Syntax	Description
`-allpkgs`	View a list of all DMP depots and patches. The installdmp lists the depots 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.
`-copyinstallscripts`	Use this option when you manually install products and want to use the intallation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./installer -rootpath` *`alt_root_path`* `-copyinstallscripts` The path *alt_root_path* can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the *release_name* is UXRT51SP1.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-hostfile`	Specifies the location of a file that contains the system names for the installer.
`-ignorepatchreqs`	The `-ignorepatchreqs` option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
`-install`	Install product depots on systems without configuring DMP.
`-installallpkgs`	Selects all the depots for installation. See the `-allpkgs` option.
`-installminpkgs`	Selects the minimum depots for installation. See the `-minpkgs` option.
`-installrecpkgs`	Selects the recommended depots for installation. See the `-recpkgs` option.
`-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.
`-listpatches`	The `-listpatches` option displays product patches in correct installation order.
`-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.
`-minpkgs`	View a list of the minimal depots and the patches that are required for DMP. The installdmp lists the depots and patches in the correct installation order. The list does not include the optional depots. 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.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-nolic`	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
`-patchpath` *`patch_path`*	Specifies that *patch_path* contains all patches that the installdmp is about to install on all systems. The *patch_path* is the complete path of a directory. **Note:** You can use this option when you download recent versions of patches.
`-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
`-pkgpath` *`pkg_path`*	Specifies that *pkg_path* contains all depots 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 5.1SP1 depots installed on the systems that you specify.
`-pkgtable`	Displays the DMP 5.1SP1 depots 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.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-recpkgs`	View a list of the recommended depots and the patches that are required for DMP. The installdmp lists the depots and patches in the correct installation order. The list does not include the optional depots. 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.
`-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 61.
`-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.
`-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 44.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-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 44.
`-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 depots on remote systems before installation.
`-upgrade`	Upgrades the installed depots on the systems that you specify.
`-uninstall`	Uninstalls DMP from the systems that you specify.
`-version`	Checks and reports the installed products and their versions. Identifies the installed and missing depots and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing depots and patches where applicable.

Command options for uninstall script

The `uninstalldmp program` command usage takes the following form:

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

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

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

Table A-2 uninstalldmp program 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.
`-copyinstallscripts`	Use this option when you manually install products and want to use the intallation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./installer -rootpath` *`alt_root_path`* `-copyinstallscripts` The path *alt_root_path* can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the *release_name* is UXRT51SP1.
`-hostfile`	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 program log files, summary file, and response file are saved.

Table A-2 uninstalldmp program options *(continued)*

Option and Syntax	Description
`-makeresponsefile`	Use this option to create a response file or to verify that your system configuration is ready for uninstalling DMP.
`-nolic`	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
`-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 62.
`-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.
`-tmppath` *`tmp_path`*	Specifies that *tmp_path* is the working directory for uninstalldmp program. This path is different from the /var/tmp path. This destination is where the uninstalldmp program performs the initial logging and where the installdmp copies the depots on remote systems before installation.
`-version`	Checks and reports the installed products and their versions. Identifies the installed and missing depots and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing depots and patches where applicable.

Appendix B

Response files

This appendix includes the following topics:

- About response files
- Installing DMP using response files
- Uninstalling DMP using response files
- Syntax in the response file
- Response file variable definitions

About response files

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

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

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

Installing DMP using response files

Typically, you can use the response file that the installer generates after you perform DMP installation on one cluster to install DMP on other clusters. 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 one of the cluster systems 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 -responsefile /tmp/response_file
   ```

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

Uninstalling DMP using response files

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

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 -responsefile /tmp/response_file
   ```

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

Syntax in the response file

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

For example, in the case of a string value:

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

or, in the case of an integer value:

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

or, in the case of a list:

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

Response file 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 depots. 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

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

Variable	Description
CFG{prod}	Defines the product to be installed, uninstalled, or configured. List or scalar: scalar Optional or required: required
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{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 depots. 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 depots that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{rsh}	Defines that *rsh* must be used instead of ssh as the communication method between systems. List or scalar: scalar Optional or required: optional
CFG{donotinstall} {depot}	Instructs the installation to not install the optional depots in the list. List or scalar: list Optional or required: optional

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

Variable	Description
CFG{donotremove} {depot}	Instructs the uninstallation to not remove the optional depots in the list. List or scalar: list Optional or required: optional
CFG{opt}{logpath}	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. List or scalar: scalar Optional or required: optional
CFG{opt}{configure}	Performs the configuration after the depots are installed using the `-install` option. List or scalar: scalar Optional or required: optional
CFG{opt}{upgrade}	Upgrades all depots installed, without configuration. List or scalar: list Optional or required: optional
CFG{opt}{uninstall}	Uninstalls DMP depots. List or scalar: scalar Optional or required: optional

Appendix C

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
- Configuring and enabling ssh
- Enabling remsh

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 cluster. The node from which the installer is run must have permissions to run `remsh` (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 (remsh). Symantec recommends that you use ssh as it is more secure than remsh.

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

Configuring and enabling ssh

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

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

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

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

To create the DSA key pair

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

   ```
   system1 # cd /
   ```

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

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

   System output similar to the following is displayed:

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

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

4 When the program asks you to enter the passphrase, press the Enter key twice.

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

Do not enter a passphrase. Press Enter.

```
Enter same passphrase again:
```

Press Enter again.

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

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

Change the permissions of this directory, to secure it.

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

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

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

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

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

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

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

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

Use the secure file transfer program.

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

Use the following command for secure file transfer:

```
system1 # sftp system2
```

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

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

4 Enter `yes`.

Output similar to the following is displayed:

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

5 Enter the root password of system2.

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

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

The following output is displayed:

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

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

```
sftp> quit
```

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

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

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

Enabling remsh

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

Typically, the only requirement to enable remote installations is to modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. You must modify this file for each user who remotely accesses the system using `remsh`. Each line of the `.rhosts` file must contain a fully qualified domain name or IP address for each remote system that has access to the local system. For example, if the root user must remotely access `system1` from `system2`, add an entry for `system2.companyname.com` to the `/.rhosts` file on `system1`.

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

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

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

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

Appendix D

Veritas Dynamic Multi-Pathing components

This appendix includes the following topics:

- Veritas Dynamic Multi-Pathing installation depots

Veritas Dynamic Multi-Pathing installation depots

Table D-1 shows the depot name and contents for each English language depot for Veritas Dynamic Multi-Pathing. The table also gives you guidelines for which depots to install based whether you want the minimum, recommended, or advanced configuration.

Table D-1 Veritas Dynamic Multi-Pathing depots

depots	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 5.10.0 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 D-1 Veritas Dynamic Multi-Pathing depots *(continued)*

depots	Contents	Configuration
VRTSsfmh	Veritas Storage Foundation Managed Host Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at: http://www.symantec.com/business/storage-foundation-manager	Recommended
VRTSspt	Veritas Software Support Tools	Recommended

Appendix E

Troubleshooting installation issues

This appendix includes the following topics:

- Restarting the installer after a failed connection
- What to do if you see a licensing reminder
- Incorrect permissions for root on remote system
- Resource temporarily unavailable
- Inaccessible system

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:

  ```
  # vxkeyless display
  ```

- 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

Incorrect permissions for root on remote system

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

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


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 67.

Note: Remove remote shell permissions after completing the DMP installation and configuration.

Resource temporarily unavailable

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

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

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

```
# kctune -q nkthread
```

If necessary, you can change the value of `nkthread` using the SAM (System Administration Manager) interface, or by running the `kctune` command. If you

change the value of nkthread, the kernel must be rebuilt for the new value to take effect. It is easier to change the value using SAM because there is an option to process the new kernel immediately.

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

Inaccessible system

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

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

 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.

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

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

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

Index

C

configuring
    remsh 26
    ssh 26

I

installer program 32
Installing
    DMP with the Web-based installer 38
installing
    DMP 32, 48

K

kctune command 78

M

mounting
    software disc 27

R

remsh
    configuration 26

S

sam command 78
ssh
    configuration 26

U

uninstalldmp command 48

W

Web-based installer 38