

Veritas™ Dynamic Multi-Pathing Installation Guide

AIX

6.0

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

Document version: 6.0.3

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our website 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.

<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

Technical Support	4
Section 1 Installation overview and planning	13
Chapter 1 Introducing Veritas Dynamic Multi-Pathing	14
About Veritas Dynamic Multi-Pathing	14
Chapter 2 Planning to install Veritas Dynamic Multi-Pathing	16
About planning for DMP installation	16
About installation and configuration methods	17
Chapter 3 System requirements	18
Release notes	18
Hardware compatibility list (HCL)	18
Supported operating systems	19
Disk space requirements	19
Virtual I/O Server (VIOS) requirements for DMP support	19
Discovering product versions and various requirement information	19
Chapter 4 Licensing Veritas products	21
About Veritas SFHA Solutions product licensing	21
Setting or changing the Veritas SFHA Solutions product level for keyless licensing	22
Installing Veritas SFHA Solutions product license keys	24

Section 2	Installation of Veritas Dynamic Multi-Pathing	25
Chapter 5	Preparing to install Veritas Dynamic Multi-Pathing	26
	Installation preparation overview	26
	Setting environment variables	27
	About using ssh or rsh with the Veritas installer	27
	Mounting the product disc	28
	Assessing the system for installation readiness	29
	Symantec Operations Readiness Tools	30
	Prechecking your systems using the Veritas installer	30
Chapter 6	Installing Veritas Dynamic Multi-Pathing using the script-based installer	32
	32
	Installing Veritas Dynamic Multi-Pathing	33
	Performing a postcheck on a node	35
Chapter 7	Installing Veritas Dynamic Multi-Pathing using the web-based installer	36
	About the Web-based installer	36
	Before using the Veritas Web-based installer	37
	Starting the Veritas Web-based installer	37
	Obtaining a security exception on Mozilla Firefox	38
	Performing a pre-installation check with the Veritas Web-based installer	39
	Installing DMP with the Web-based installer	39
Chapter 8	Installing Veritas Dynamic Multi-Pathing using other methods	41
	Installing DMP using NIM and the installer	41
	Preparing the installation bundle on the NIM server	41
	Installing DMP on the NIM client using SMIT on the NIM server	42
	Installing DMP and the operating system on the NIM client using SMIT	43
	Installing Veritas Dynamic Multi-Pathing using the mksysb utility	44
	Creating the mksysb backup image	44

	Installing mksysb image on alternate disk	45
	Verifying the installation	46
Section 3	Verification of the installation	47
Chapter 9	Verifying the Veritas Dynamic Multi-Pathing installation	48
	Verifying that the products were installed	48
	Installation log files	49
	Starting and stopping processes for the Veritas products	49
Section 4	Upgrading Veritas Dynamic Multi-Pathing	51
Chapter 10	Preparing to upgrade	52
	About upgrading	52
	52
	Supported upgrade paths for DMP	53
	Preparing to upgrade	54
	Getting ready for the upgrade	54
	Preparing for an upgrade of Veritas Dynamic Multi-Pathing	55
	Creating backups	55
	Upgrading the array support	56
Chapter 11	Upgrading Veritas Dynamic Multi-Pathing	57
	Upgrading Veritas Dynamic Multi-Pathing with the product installer	57
	Upgrading Veritas Dynamic Multi-Pathing using the Veritas Web-based installer	58
	Upgrade Veritas Dynamic Multi-Pathing and AIX on a DMP-enabled rootvg	59
	Upgrading from DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.0 on a DMP-enabled rootvg	59
	Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.0 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg	60
	Upgrading DMP on Virtual I/O Server from 5.1SP1 or later to 6.0	61
	Upgrading the AIX operating system	62

Chapter 12	Upgrading using an alternate disk	63
	About upgrading DMP using an alternate disk	63
	Supported upgrade scenarios	64
	Supported upgrade paths	64
	Preparing to upgrade DMP on an alternate disk	64
	Upgrading DMP on an alternate disk	66
	Upgrading DMP and AIX on a DMP-enabled alternate rootvg	66
	Verifying the upgrade	66
Chapter 13	Upgrading DMP using Network Install Manager Alternate Disk Migration	68
	Supported upgrade paths	68
	Preparing to upgrade DMP and the operating system using the nimadm utility	69
	Preparing the installation bundle on the NIM server	69
	Upgrading DMP and the operating system using the nimadm utility	70
	Verifying the upgrade	72
Chapter 14	Performing post-upgrade tasks	73
	Updating variables	73
	Verifying the Veritas Dynamic Multi-Pathing upgrade	73
Section 5	Uninstallation of Veritas Dynamic Multi-Pathing	74
Chapter 15	Uninstalling Veritas Dynamic Multi-Pathing	75
	Uninstalling Veritas Dynamic Multi-Pathing	75
	Uninstalling DMP with the Veritas Web-based installer	76
	Removing Storage Foundation products using SMIT	77
Section 6	Installation reference	79
Appendix A	Installation scripts	80
	Command options for the installation script	80
	Command options for uninstall script	85

Appendix B	Response files	89
	About response files	89
	Installing DMP using response files	90
	Upgrading DMP using response files	90
	Uninstalling DMP using response files	91
	Syntax in the response file	91
	Response file variable definitions	92
Appendix C	Tunable files for installation	95
	About setting tunable parameters using the installer or a response file	95
	Setting tunables for an installation, configuration, or upgrade	96
	Setting tunables with no other installer-related operations	97
	Setting tunables with an un-integrated response file	98
	Preparing the tunables file	99
	Setting parameters for the tunables file	99
	Tunables value parameter definitions	100
Appendix D	Configuring the secure shell or the remote shell for communications	103
	About configuring secure shell or remote shell communication modes before installing products	103
	Manually configuring and passwordless ssh	104
	Restarting the ssh session	108
	Enabling rsh for AIX	108
Appendix E	Veritas Dynamic Multi-Pathing components	110
	Veritas Dynamic Multi-Pathing installation filesets	110
Appendix F	Troubleshooting installation issues	112
	Restarting the installer after a failed connection	112
	What to do if you see a licensing reminder	112
	Troubleshooting an installation on AIX	113
	Incorrect permissions for root on remote system	113
	Resource temporarily unavailable	114
	Inaccessible system	115

Appendix G	Compatibility issues when installing DMP with other products	116
	Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present	116
	Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present	117
	Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present	117
Index		118

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](#)

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.

DMP is available as a component of Storage Foundation. DMP supports Veritas Volume Manager (VxVM) volumes on DMP metadevices, and Veritas File System (VxFS) file systems on those volumes.

DMP is also available as a stand-alone product, which extends DMP metadevices to support the OS native logical volume manager (LVM). You can create LVM volumes and volume groups on DMP metadevices.

DMP supports LVM volume devices that are used as the paging devices.

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 Enterprise license, SF HA Enterprise license, and Standard license.

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.

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 Symantec Operations Readiness Tools (SORT) website.

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

Document version: 6.0.3.

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

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 36.
- 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 89.
- Network Installation Manager (NIM)
You can use the Veritas product installer or the product-specific installation script to generate a NIM configuration file. Use the generated script to install Veritas filesets from your NIM server.

System requirements

This chapter includes the following topics:

- [Release notes](#)
- [Hardware compatibility list \(HCL\)](#)
- [Supported operating systems](#)
- [Disk space requirements](#)
- [Virtual I/O Server \(VIOS\) requirements for DMP support](#)
- [Discovering product versions and various requirement information](#)

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

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

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

```
# ./installdmp -precheck
```

Virtual I/O Server (VIOS) requirements for DMP support

To run DMP in VIOS, the minimum VIOS level that is required is 2.1.3 10-FP-23 or later.

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 filesets 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
```

Licensing Veritas products

This chapter includes the following topics:

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

About Veritas SFHA Solutions 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.

www.symantec.com/techsupp/

During the installation, you can choose to either:

- 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, such as Veritas Operations Manager (VOM). 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 encounter problems while licensing this product, visit the Symantec licensing support website.

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:

See [About Veritas Storage Foundation and High Availability Solutions 6.0](#)

- 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 Veritas SFHA Solutions product level for keyless licensing”](#) on page 22.

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 SFHA Solutions product license keys”](#) on page 24.

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 Veritas SFHA Solutions 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 Show your current working directory:

```
# pwd
```

Output resembles:

```
/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 SFHA Solutions product license keys

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

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

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

To install a new license

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

```
# cd /opt/VRTS/bin
```

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

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 8. Installing Veritas Dynamic Multi-Pathing using other methods](#)

Preparing to install Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

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

Installation preparation overview

[Table 5-1](#) provides an overview of an installation using the product installer.

Table 5-1 Installation overview

Installation task	Section
Obtain product licenses.	See “About Veritas SFHA Solutions product licensing” on page 21.
Download the software, or insert the product DVD.	See “Mounting the product disc” on page 28.
Set environment variables.	See “Setting environment variables” on page 27.
Configure the secure shell (ssh) on all nodes.	See “About using ssh or rsh with the Veritas installer” on page 27.

Table 5-1 Installation overview (*continued*)

Installation task	Section
Verify that hardware, software, and operating system requirements are met.	See “Release notes” on page 18.
Check that sufficient disk space is available.	See “Disk space requirements” on page 19.
Use the installer to install the products.	See “” on page 32.

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
```

The `nroff` versions of the online manual pages are not readable using the `man` command if the `bos.txt.tfs` fileset is not installed; however, the `VRTSvxvm` and `VRTSvxfs` filesets install ASCII versions in the `/opt/VRTS/man/cat*` and `/opt/VRTS/man/man*` directories that are readable without the `bos.txt.tfs` fileset.

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 add new nodes to an existing cluster.
- When the nodes are in a subcluster 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 103.

Mounting the product disc

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 Determine the device access name of the disc drive. For example, enter:

```
# lsdev -C -c cdrom
```

The output resembles:

```
cd0 Available 1G-19-00 IDE DVD-ROM Drive
```

In this example, `cd0` is the disc's device access name.

- 3 Make sure the /cdrom file system is created:

```
# cat /etc/filesystems
```

If the /cdrom file system exists, the output contains a listing that resembles:

```
.
.
/cdrom:
dev = /dev/cd0
vfs = cdrfs
mount = false
options = ro
account = false
.
.
```

- 4 If the /cdrom file system does not exist, create it:

```
# crfs -v cdrfs -p ro -d cd0 -m /cdrom
```

- 5 Insert the product disc with the DMP software into a drive that is connected to the system.
- 6 Mount the disc:

```
# mount /cdrom
# cd /cdrom
```

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.

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 30.

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.

See “Prechecking your systems using the Veritas installer” on page 30.

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.
- 2 Select the precheck option:
 - From the Web-based installer, select the **Perform a Pre-Installation Check** from the Task pull-down menu.

- In the script-based installer, from root on the system where you want to perform the check, start the installer.

```
# ./installer
```

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

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

Installing Veritas Dynamic Multi-Pathing using the script-based installer

This chapter includes the following topics:

-
- [Installing Veritas Dynamic Multi-Pathing](#)
- [Performing a postcheck on a node](#)

The installer enables you to install and 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.

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 103.

- 2 Load and mount the software disc.

See [“Mounting the product disc”](#) on page 28.

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

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

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

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 filesets 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-****
```

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.

Installing Veritas Dynamic Multi-Pathing using the web-based installer

This chapter includes the following topics:

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

About the Web-based installer

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

You use the `webinstaller` script to start and stop the Veritas XPortal Server `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 37.

See [“Starting the Veritas Web-based installer”](#) on page 37.

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.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must use the same operating system as the target systems and must be at one of the supported operating system update levels.
Administrative system	The system where you run the Web browser to perform the installation.	Must have a Web browser. Supported browsers: <ul style="list-style-type: none">■ 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 `xprt1wid`, on the installation server:

```
# ./webinstaller start
```

The webinstaller script displays a URL. Note this URL.

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

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

- 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 **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 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 39.
- 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 filesets. 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 prompts you for another task.
 - 13 Reboot the systems if the installer prompts for a reboot to enable DMP native support.

Installing Veritas Dynamic Multi-Pathing using other methods

This chapter includes the following topics:

- [Installing DMP using NIM and the installer](#)
- [Installing Veritas Dynamic Multi-Pathing using the mksysb utility](#)

Installing DMP using NIM and the installer

You can use the product installer in concert with NIM to install the Veritas product, or to install the operating system and the Veritas product.

The instructions in this section assume a working knowledge of the Network Installation Management process. See the operating system documentation for detailed information on Network Installation Management.

In the following samples, the LPP resource uses LPP-6100-up2date and its relevant SPOT resource is spot-6100-up2date.

Preparing the installation bundle on the NIM server

You need to prepare the installation bundle on the NIM server before using NIM to install DMP filesets. The following actions are executed on the NIM server.

Note: Make sure that a NIM LPP_SOURCE is present on the NIM server.

To prepare the installation bundle

- 1 Insert and mount the installation media.
- 2 Choose an LPP source:

```
# lsnim |grep -i lpp_source  
LPP-6100-up2date resources lpp_source
```

- 3 Navigate to the product directory on the installation media and run the `installdmp` command to prepare the bundle resource:

```
# ./installdmp -nim LPP-6100-up2date
```

The installation program copies the necessary filesets and patches to the LPP resource directory.

- 4 Enter a name for the bundle, for example *DMP60*.
- 5 Run the `lsnim -l` command to check that the `installp_bundle` resource is created successfully.

```
# lsnim -l DMP60  
DMP60:  
class = resources  
type = installp_bundle  
Rstate = ready for use  
prev_state = unavailable for use  
location = /opt/VRTS/nim/DMP60.bnd  
alloc_count = 0  
server = master
```

Installing DMP on the NIM client using SMIT on the NIM server

You can install DMP on the NIM client using the SMIT tool on the NIM server. Perform these steps on each node to have DMP installed in a cluster.

To install DMP

- 1 On the NIM server, start SMIT.

```
# smit nim
```

- 2 In the menu, select **Perform NIM Software Installation and Maintenance Tasks**.
- 3 In the menu, select **Install and Update Software**.

- 4 In the menu, select **Install Software Bundle**.
- 5 Select the systems from the list on which to install the software bundle.
- 6 In the menu, select the LPP_SOURCE. In this example, specify **LPP-6100-up2date**.
- 7 In the menu, select the bundle, for example, **DMP60**.
- 8 For the installp flags, specify that the ACCEPT new license agreements flag has a **yes** value.
- 9 Press the Enter key to start the installation. Note that it may take some time to finish.

Installing DMP and the operating system on the NIM client using SMIT

You can install VCS and the operating system on the NIM client using the SMIT tool.

Perform these steps on each node to have DMP and AIX installed in a cluster.

To install DMP and the operating system

- 1 On the NIM server, start smitty for a NIM and operating system installation.

```
# smitty nim_bosinst
```
- 2 In the menu, select the stand-alone target.
- 3 In the menu, select **spot - Install a copy of a SPOT resource**.
- 4 In the menu, select the spot resource **spot-6100-up2date**.
- 5 In the menu, select the LPP_SOURCE. In this example, select **LPP-6100-up2date**.
- 6 In the menu, select the following options:
 - For the ACCEPT new license agreements option, specify **yes**.
 - For the Additional Bundles to Install option, specify **DMP60**.
- 7 For the installp flags, specify that the ACCEPT new license agreements flag has a **yes** value.

Installing Veritas Dynamic Multi-Pathing using the `mksysb` utility

On AIX, one can use the `mksysb` utility to back up the system image. This image can be installed on another host. For example, you can use this utility to set up a disaster recovery site. Veritas Dynamic Multi-Pathing can be installed through `mksysb` image.

You can install the `mksysb` image on the same machine or on any NIM client through a NIM server. This procedure assumes working knowledge of `mksysb`. See your operating system installation guide for more details about `mksysb`.

The installation process involves the following steps:

- Creating the `mksysb` image.
- Installing the DMP stack through `mksysb` image on a machine.
- Verifying the installation.

Creating the `mksysb` backup image

You can create the `mksysb` backup image with the SMIT interface or with manual steps.

Before you begin, make sure that the DMP installation media is available.

To create an `mksysb` image using SMIT interface

- 1 Check maximum file size limit with `ulimit`. It should be sufficient for creating backup image
- 2 Check that all the required filesets are installed for a particular product stack. You can obtain the list of filesets from the the installer.

The recommended approach is to install all of the filesets but do not configure product stack before taking `mksysb` image if the image is to be installed on a different machine.

- 3 Enter fast path `smitty mksysb` and enter the required values.
- 4 Press enter to start the backup image creation.

To create an `mksysb` image using commands manually

- 1 Check maximum file size limit with `ulimit`. It should be sufficient for creating backup image
- 2 Check that all the required file sets are installed for a particular product stack. You can obtain the list of filesets from the installer.

The recommended approach is to install all of the filesets but do not configure product stack before taking `mksysb` image if the image is to be installed on a different machine.

- 3 Enter command

```
# /usr/bin/mksysb -i -X backup file name
```

Installing `mksysb` image on alternate disk

You can install the `mksysb` image on the same system or on any NIM client through a NIM server.

To install DMP with `mksysb` on an alternate disk of the same system using SMIT

- 1 Type `smitty` and then select Software Installation and Maintenance -> Alternate Disk Installation -> Install `mksysb` on an Alternate Disk
- 2 Select target disks
- 3 Select `mksysb` image to be installed
- 4 Select appropriate values for remaining options
- 5 Press enter to start the `mksysb` image installation.
- 6 After installation is complete reboot from the alternate disk.
- 7 If DMP was not configured in the `mksysb` image then run `installdmp -configure` after reboot.

To install DMP with `mksysb` on an alternate disk of the same system using commands manually

- ◆ To install DMP with `mksysb` on an alternate disk of the same system using commands manually

```
# /usr/sbin/alt_disk_mksysb -m mksysb_image -P "all" -d "disk_name"
```

To install DMP with mksysb on an alternate disk of the NIM client using SMIT

- 1 Create an `mksysb` resource from the `mksysb` image created above on NIM server.
- 2 Set up the system on which you want to install DMP as NIM client.
- 3 Type `smitty nim` then select Perform NIM Software Installation and Maintenance Tasks -> Alternate Disk Installation -> Install `mksysb` on an Alternate Disk
- 4 Select target system.
- 5 Select target disks.
- 6 Select `mksysb` image to be installed.
- 7 Select appropriate values for remaining options.
- 8 Press enter to start the `mksysb` image installation.
- 9 If DMP was not configured in the `mksysb` image then run `installdmp -configure` after rebooting NIM client.

To install DMP with mksysb on an alternate disk of a NIM client using commands manually

- 1 Create an `mksysb` resource from the `mksysb` image created above on NIM server.
- 2 Set up the system on which you want to install DMP as NIM client.
- 3 To install DMP with `mksysb` on an alternate disk of a NIM client using commands manually:

```
# /usr/sbin/nim -o alt_disk_install \  
-a source=mksysb -a mksysb=mksysb_resource -a \  
disk=hdisk_name system_name
```

- 4 If DMP was not configured in the `mksysb` image then run `installdmp -configure` after rebooting NIM client.

Verifying the installation

After the installation is finished, verify the installation using the following command:

```
# ls1pp -l|grep -i vrts
```

All the filesets should be installed properly.

See [“Discovering product versions and various requirement information”](#) on page 19.

Verification of the installation

- [Chapter 9. Verifying the Veritas Dynamic Multi-Pathing installation](#)

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.

Use the `ls1pp` command to check which filesets have been installed:

```
# ls1pp -L | grep VRTS
```

The filesets should be in the COMMITTED state.

See [“Veritas Dynamic Multi-Pathing installation filesets”](#) on page 110.

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

```
# /opt/VRTS/install/installdmp program -version
```

Use the following sections to further verify the product installation.

Installation log files

The Veritas product installer or product installation script `installmp` program 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 <code>responsefile</code> 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 filesets, and the status (success or failure) of each fileset. 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
```

Upgrading Veritas Dynamic Multi-Pathing

- [Chapter 10. Preparing to upgrade](#)
- [Chapter 11. Upgrading Veritas Dynamic Multi-Pathing](#)
- [Chapter 12. Upgrading using an alternate disk](#)
- [Chapter 13. Upgrading DMP using Network Install Manager Alternate Disk Migration](#)
- [Chapter 14. Performing post-upgrade tasks](#)

Preparing to upgrade

This chapter includes the following topics:

- [About upgrading](#)
-
- [Supported upgrade paths for DMP](#)
- [Preparing to upgrade](#)

About upgrading

There are many types of upgrades available. Before you start to upgrade, review the types of upgrades for the Veritas products.

See [“”](#) on page 52.

Review the supported upgrade paths that are available for the different methods of upgrading.

After you determine the type of upgrade that you want to perform and its upgrade paths, review the steps to prepare for the upgrade.

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 10-1 Review this table to determine how you want to perform the upgrade

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

Supported upgrade paths for DMP

The following tables describe upgrading to 6.0.

Table 10-2 AIX upgrades using the script- or Web-based installer

Veritas software version	5.3	6.1	7.1
<p>5.1 SP1</p> <p>5.1 SP1 RPx</p>	<p>Upgrade the operating system to 6.1 TL5 or later—do not upgrade to 7.1. Use the installer to upgrade your Veritas product to 6.0.</p> <p>Then, upgrade the operating system to 7.1 if you want to use your Veritas product on AIX 7.1.</p>	<p>Upgrade the operating system to 6.1 TL5 or later—do not upgrade to 7.1. Use the installer to upgrade your Veritas product to 6.0.</p> <p>Then, upgrade the operating system to 7.1 if you want to use your Veritas product on AIX 7.1.</p>	<p>N/A</p>
<p>5.1 SP1 PR1</p>	<p>N/A</p>	<p>N/A</p>	<p>Use the installer to upgrade to the 6.0 version of your Veritas Product.</p>

Table 10-2 AIX upgrades using the script- or Web-based installer (*continued*)

Veritas software version	5.3	6.1	7.1
New installation	N/A	Upgrade the operating system to 6.1 TL5 or later. Use the 6.0 version of your Veritas Product. Then, upgrade the operating system to 7.1 if you want to use your Veritas product on AIX 7.1.	Use the installer to install the 6.0 version of your Veritas Product.

Preparing to upgrade

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/>
- 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.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the filesets, 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 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.

- For any startup scripts in `/etc/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 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.
- Make sure the file systems are clean before upgrading.
- Upgrade arrays (if required).
- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a fallback point.

Preparing for an upgrade of Veritas Dynamic Multi-Pathing

Before you upgrade, perform the following procedure.

To prepare for an upgrade of Veritas Dynamic Multi-Pathing

- 1 Log in as `root`.
- 2 Stop activity to all file systems and raw volumes, for example by unmounting any file systems that have been created on volumes.

`# umount mnt_point`
- 3 Stop all the volumes by entering the following command for each disk group:

`# vxvol -g diskgroup stopall`
- 4 Stop the VEA backend service by entering the following command if VRTSob is installed:

`# /opt/VRTS/bin/vxsvcctrl stop`
- 5 Upgrade AIX on your system to the required levels if applicable.

Creating backups

Save relevant system information before the upgrade.

To create backups

- 1 Log in as superuser.
- 2 Before the upgrade, ensure that you have made backups of all data that you want to preserve.
- 3 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 release includes all array support in a single fileset, `VRTSaslapm`. The array support fileset includes the array support previously included in the `VRTSvxvm` fileset. The array support fileset also includes support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

See the 6.0 Hardware Compatibility List for information about supported arrays.

See [“Hardware compatibility list \(HCL\)”](#) on page 18.

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` fileset exits with an error if external ASLs or APMs are detected.

After you have installed Storage Foundation 6.0, Symantec provides support for new disk arrays through updates to the `VRTSaslapm` fileset.

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

Upgrading Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- [Upgrading Veritas Dynamic Multi-Pathing with the product installer](#)
- [Upgrading Veritas Dynamic Multi-Pathing using the Veritas Web-based installer](#)
- [Upgrade Veritas Dynamic Multi-Pathing and AIX on a DMP-enabled rootvg](#)
- [Upgrading DMP on Virtual I/O Server from 5.1SP1 or later to 6.0](#)
- [Upgrading the AIX operating system](#)

Upgrading Veritas Dynamic Multi-Pathing with the product installer

This section describes upgrading from Veritas Dynamic Multi-Pathing products to 6.0.

Use this procedure to upgrade Veritas Dynamic Multi-Pathing.

To upgrade Veritas Dynamic Multi-Pathing

- 1 Log in as superuser.
- 2 Load and mount the disc. If you downloaded the software, navigate to the top level of the download directory.

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

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

- 4 Enter `c` to upgrade and select the **Full Upgrade**.
- 5 You are prompted to enter the system names (in the following example, "host1") on which the software is to be installed. Enter the system name or names and then press Return.

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

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

- 6 The installer asks if you agree with the terms of the End User License Agreement. Press `y` to agree and continue.
- 7 The installer lists the filesets and any patches to install or to update. You are prompted to confirm that you are ready to upgrade.
- 8 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.

- 9 The installer stops, uninstalls, reinstalls, and starts specified filesets.
- 10 The Veritas Dynamic Multi-Pathing software is verified and configured.
- 11 The installer prompts you to provide feedback, and provides the log location for the upgrade.
- 12 Reboot the systems if the installer prompts reboot to enable DMP native support.

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 37.
- 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.

Upgrade Veritas Dynamic Multi-Pathing and AIX on a DMP-enabled rootvg

The following upgrade paths are supported to upgrade DMP and AIX on a DMP-enabled rootvg

Table 11-1 Upgrade paths for DMP on a DMP-enabled rootvg

Upgrade path	Procedure
DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.0	See “Upgrading from DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.0 on a DMP-enabled rootvg” on page 59.
DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.0 on AIX 6.1 or AIX 7.1	See “Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.0 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg” on page 60.

Upgrading from DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.0 on a DMP-enabled rootvg

When you upgrade from a prior version of DMP on a DMP-enabled rootvg to DMP 6.0, you must disable DMP root support before performing the upgrade. Enable the DMP root support after the upgrade. If the AIX version is less than 6.1, an operating system upgrade is required.

See [“Upgrading from DMP 5.1SP1 \(or later\) on AIX 5.3 to DMP 6.0 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg”](#) on page 60.

To upgrade from DMP 5.1SP1 or later to DMP 6.0 on a DMP-enabled rootvg

- 1 Disable DMP support for the rootvg:

```
# vxddmpadm native disable vname=rootvg
```

Please reboot the system to disable DMP support for LVM bootability

- 2 Reboot the system.
- 3 Upgrade DMP to 6.0.

Run the installer command on the disc, and enter G for the upgrade task.

See [“Upgrading Veritas Dynamic Multi-Pathing with the product installer”](#) on page 57.

- 4 Reboot the system.
- 5 Enable DMP for rootvg.

```
# vxddmpadm native enable vname=rootvg
```

Please reboot the system to enable DMP support for LVM bootability

- 6 Reboot the system. After the reboot, the system has DMP root support enabled.

Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.0 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg

DMP 6.0 requires at least AIX 6.1. When you upgrade DMP from a prior version on a system that uses AIX 5.3, you must also upgrade the AIX operating system. If the rootvg is enabled for DMP, follow these steps.

To upgrade from DMP 5.1SP1 or later to SF 6.0 on a DMP-enabled rootvg

- 1 Disable DMP support for the rootvg:

```
# vxddmpadm native disable vname=rootvg
```

Please reboot the system to disable DMP support for LVM bootability

- 2 Upgrade the AIX operating system from 5.3 to 6.1 before rebooting.
- 3 Reboot the system.

- 4 Upgrade DMP to 6.0.

See [“Upgrading Veritas Dynamic Multi-Pathing with the product installer”](#) on page 57.

Restart the system if the installer prompts for restart during upgrade.

If `vxconfigd` cannot be started after the upgrade, restart the system.

- 5 Reboot the system. After the reboot, the system has DMP root support enabled.

Upgrading DMP on Virtual I/O Server from 5.1SP1 or later to 6.0

This section provides the instructions to upgrade DMP on Virtual I/O Server (VIOS) from 5.1SP1 or later to 6.0.

To upgrade DMP on VIOS

- 1 Shut down all Virtual I/O clients not having a failover capability, and only dependent on the Virtual I/O server being upgraded.
- 2 Log in to the VIO Server partition.

Use the following command to access the non-restricted root shell.

```
$ oem_setup_env
```

Note: In this procedure, invoke all subsequent commands from the non-restricted shell.

Symantec recommends that you take a backup, in case you want to revert back to the earlier version.

- 3 Unconfigure all virtual devices from all virtual adapters.

```
# rmdev -p vhost0
vtscsi0 Defined
..
```

- 4 Follow the procedure to upgrade DMP on Virtual I/O Server.

See [“Upgrading Veritas Dynamic Multi-Pathing with the product installer”](#) on page 57.

- 5 If required, reconfigure all the virtual target devices from all the virtual adapters.

```
# cfgmgr -p vhost0
```

- 6 For all the Virtual I/O Servers, repeat the steps 1 through 5.
- 7 Restart all the Virtual I/O clients you had shut down, and verify the configuration.

Upgrading the AIX operating system

Use this procedure to upgrade the AIX operating system if DMP 6.0 is installed. You must upgrade to a version that DMP 6.0 supports.

To upgrade the AIX operating system

- 1 If DMP root support is enabled, run the `vxdmpadm native release` command to give back pvids to OS device paths.

```
# vxdmpadm native release
```

- 2 Upgrade the AIX operating system. See the operating system documentation for more information.
- 3 Apply the necessary APARs.
- 4 Reboot the system.

```
# shutdown -Fr
```

Upgrading using an alternate disk

This chapter includes the following topics:

- [About upgrading DMP using an alternate disk](#)
- [Supported upgrade scenarios](#)
- [Supported upgrade paths](#)
- [Preparing to upgrade DMP on an alternate disk](#)
- [Upgrading DMP on an alternate disk](#)
- [Upgrading DMP and AIX on a DMP-enabled alternate rootvg](#)
- [Verifying the upgrade](#)

About upgrading DMP using an alternate disk

Use the alternate disk installation process to upgrade the operating system and DMP on a production server while the server runs. Perform the upgrade on an alternate or inactive boot environment. After the upgrade, restart the system on the alternate disk to use the updated environment. The instructions in this section assume a working knowledge of the alternate disk installation process. See the operating system documentation for detailed information on alternate disk installations.

Note: Only Technology Level (TL) and Service Pack (SP) releases of the operating system can be upgraded using this procedure.

Upgrading DMP on an alternate disk has the following advantages:

- The server remains active during the time the new boot environment is created and upgraded on the alternate boot device.
- The actual downtime for the upgrade is reduced to the period of time required for a single reboot.
- The original boot environment is still available for use if the updated environment fails to become active.

Supported upgrade scenarios

The following upgrade scenarios are supported on an alternate disk:

- Upgrading only DMP
See “[Upgrading DMP on an alternate disk](#)” on page 66.
- Upgrading only the operating system (Technology Level (TL) and Service Pack (SP) releases)

Note: For instructions, see the operating system documentation. No additional steps are required for DMP after the operating system upgrade.

- Upgrading the operating system (Technology Level (TL) and Service Pack (SP) releases) and DMP
See “[Upgrading DMP on an alternate disk](#)” on page 66.

Supported upgrade paths

You can upgrade the operating system and DMP using an alternate disk from the following versions:

AIX version	Technology Level and Service Pack releases of AIX 5.3 and later
DMP version	5.1 and later

Preparing to upgrade DMP on an alternate disk

Complete the preparatory steps in the following procedure before you upgrade DMP on an alternate disk.

To prepare to upgrade DMP on an alternate disk

- 1 Make sure that the DMP installation media is available.
- 2 Check the status of the physical disks on your system.

Note: The alternate disk must have a physical identifier and must not contain any mounted volume groups.

```
# lspv
```

Output similar to the following displays:

```
hdisk0          0009710fa9c79877    rootvg    active
hdisk1          0009710f0b90db93    None
```

If the alternate disk does not have a physical identifier, set the physical identifier for the disk:

```
# chdev -l hdisk1 -a pv=yes
```

- 3 Make sure that the following filesets are installed on the primary disk:
`bos.alt_disk_install.boot_images`, `bos.alt_disk_install.rte`
- 4 Mount the DMP installation media.

Determine the filesets you want to install on the alternate disk.

```
# ./installdmp -install_option
```

where `install_option` is one of the following:

- installminpkgs: For installing the minimum set of filesets
- installrecpkgs: For installing the recommended filesets
- installallpkgs: For installing all filesets

Copy the required filesets from the `pkgs` directory on the installation media to a directory on the primary boot disk, for example `/tmp/prod_name`

If you are upgrading the operating system along with DMP, copy the necessary operating system filesets and the DMP filesets to a directory on the primary disk, for example `/tmp/prod_name`.

See the operating system documentation to determine the operating system filesets.

Upgrading DMP on an alternate disk

This section provides instructions to clone the primary boot environment to the alternate disk, upgrade DMP on the alternate disk, and reboot the system to start from the alternate disk. You may perform the steps manually or using the SMIT interface.

In the procedure examples, the primary or current boot environment resides on `hdisk0` and the alternate or inactive boot environment resides on `hdisk1`.

Upgrading DMP and AIX on a DMP-enabled alternate rootvg

To upgrade DMP and AIX on an alternate rootvg that is enabled for DMP on an LVM root disk, perform the following procedure.

To upgrade DMP on `altinst_rootvg` on a DMP-enabled rootvg

- 1 Clone the currently running system to the alternate disk. For example:

```
# alt_disk_install -C -P all hdisk##
```

- 2 Boot from the alternate disk.
- 3 Upgrade AIX and DMP according to the instructions for alternate root upgrade. See [“Upgrading DMP on an alternate disk”](#) on page 66.
- 4 Enable DMP on the root disk.

Verifying the upgrade

To ensure that alternate disk installation has completed successfully, verify that the system has booted from the alternate boot environment.

To verify the upgrade

- 1 Verify that the alternate boot environment is active:

```
# lspv |grep rootvg
hdisk0          0009710fa9c79877    old_rootvg
hdisk1          0009710f0b90db93    rootvg             active
```

- 2 Verify that the version of the upgraded filesets on the alternate boot disk is 6.0.0.0.

If you upgraded the operating system (TL or SP):

```
# oslevel -s
```

Upgrading DMP using Network Install Manager Alternate Disk Migration

This chapter includes the following topics:

- [Supported upgrade paths](#)
- [Preparing to upgrade DMP and the operating system using the nimadm utility](#)
- [Preparing the installation bundle on the NIM server](#)
- [Upgrading DMP and the operating system using the nimadm utility](#)
- [Verifying the upgrade](#)

Supported upgrade paths

You can perform an upgrade of the product and the operating system using Network Install Manager Alternate Disk Migration (NIM ADM).

The supported upgrade paths are as follows:

AIX version	AIX 5.3 and later
DMP version	5.1 SP1 and later

Preparing to upgrade DMP and the operating system using the nimadm utility

Complete the preparatory steps in the following procedure before you upgrade DMP and the operating system.

To prepare to upgrade DMP and the operating system using the nimadm utility

- 1 Make sure that the DMP installation media is available.
- 2 Check the status of the physical disks on your system.

Note: The alternate disk must have a physical identifier and must not contain any mounted volume groups.

```
# lspv
```

Output similar to the following displays:

```
hdisk0          0009710fa9c79877  rootvg  active
hdisk1          0009710f0b90db93  None
```

If the alternate disk does not have a physical identifier, set the physical identifier for the disk:

```
# chdev -l hdisk1 -a pv=yes
```

- 3 Make sure that the following filesets are installed on the NIM server and the client: `bos.alt_disk_install.boot_images`, `bos.alt_disk_install.rte`

Preparing the installation bundle on the NIM server

You need to prepare the installation bundle `installp` on the NIM server before using `nimadm` to upgrade DMP filesets. The following actions are executed on the NIM server.

Note: Make sure that a NIM LPP_SOURCE is present on the NIM server.

To prepare the installation bundle

- 1 Insert and mount the installation media.
- 2 Choose an LPP source:

```
# lsnim |grep -i lpp_source
LPP-6100-up2date resources lpp_source
```

- 3 Navigate to the product directory on the installation media and run the `installdmp` command to prepare the bundle resource:

```
# ./installdmp -nim LPP-6100-up2date
```

The installation program copies the necessary filesets and patches to the LPP resource directory.

- 4 Enter a name for the bundle, for example *DMP60*.
- 5 Run the `lsnim -l` command to check that the `installp_bundle` resource is created successfully.

```
# lsnim -l DMP60
DMP60:
class = resources
type = installp_bundle
Rstate = ready for use
prev_state = unavailable for use
location = /opt/VRTS/nim/DMP60.bnd
alloc_count = 0
server = master
```

Upgrading DMP and the operating system using the nimadm utility

This section provides instructions to upgrade DMP and the operating system using the `nimadm` utility. You may perform the steps manually or using the SMIT interface.

In the procedure examples, the primary or current boot environment is indicated by `hdisk0` and the alternate or inactive boot environment is indicated by `hdisk1`.

To upgrade DMP and the operating system using the `nimadm` utility

- 1 Clone the primary boot disk `rootvg` to an alternate disk using one of the following methods:

Manual

Upgrade DMP and the operating system by running the following command on the NIM server:

```
# nimadm -l lpp_source -c nim_client \  
-s spot_name -b bundle_name \  
-d nimclient_altdisk_name -Y
```

For example:

```
# nimadm -l LPP-6100-up2date -c node1 \  
-s spot-6100-up2date -b dmp60 \  
-d hdisk1 -Y
```

Where:

- -l: Specifies the LPP_SOURCE
- -c: Specifies the NIM client
- -s: Specifies the SPOT resource
- -b: Specifies DMP bundle
- -d: Specifies the alternate disk on which the installation is performed
- -Y: Specifies acceptance of all licenses

Using SMIT interface

Start the SMIT menu:

```
# smit nimadm
```

Select the option **Perform NIM Alternate Disk Migration**.

Enter the required information at the prompts:

- Target NIM Client: **system1**
- NIM LPP_SOURCE resource: **LPP-6100-up2date**
- NIM SPOT resource: **SPOT-6100-up2date**
- Target disk(s) to install: **hdisk1**
- Phase to execute: **all**
- Set Client bootlist to alternate disk? **yes**
- ACCEPT new license agreements? **yes**

Press **Enter** to start the upgrade on the alternate disk. The upgrade process takes some time.

2 Verify that the alternate disk is created:

```
# lspv | grep rootvg  
hdisk0          0009710fa9c79877    rootvg  
hdisk1          0009710f0b90db93    altinst_rootvg
```

- 3 Verify that the normal boot list includes the name of the alternate boot disk. By default, the alternate disk installation process changes the boot list to enable the system to boot from the alternate disk.

```
# bootlist -m normal -o  
hdisk1
```

- 4 Restart the system. The boot environment on the alternate disk is activated when you restart the system.

```
# shutdown -r
```

- 5 Verify the upgrade.

See [“Verifying the upgrade”](#) on page 66.

Verifying the upgrade

To ensure that alternate disk installation has completed successfully, verify that all the nodes have booted from the alternate boot environment and joined the cluster.

To verify the upgrade

- 1 Verify that the alternate boot environment is active:

```
# lspv | grep rootvg  
hdisk0          0009710fa9c79877    old_rootvg  
hdisk1          0009710f0b90db93    rootvg             active
```

- 2 Verify that the version of the upgraded filesets on the alternate boot disk is 6.0.0.0.

If you upgraded the operating system:

```
# oslevel -s
```

Performing post-upgrade tasks

This chapter includes the following topics:

- [Updating variables](#)
- [Verifying the Veritas Dynamic Multi-Pathing upgrade](#)

Updating variables

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

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

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 48.

Uninstallation of Veritas Dynamic Multi-Pathing

- [Chapter 15. Uninstalling Veritas Dynamic Multi-Pathing](#)

Uninstalling Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- [Uninstalling Veritas Dynamic Multi-Pathing](#)
- [Uninstalling DMP with the Veritas Web-based installer](#)
- [Removing Storage Foundation products using SMIT](#)

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 103.

- 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 filesets are uninstalled.

- 6 Reboot the systems if the DMP native support is on and the systems need a reboot to disable the DMP native support. Re-run the uninstall task after reboot.
- 7 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.

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 with 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 Disable DMP native support, if it is enabled. Run the following command to disable DMP native support

```
# vxdmppadm settune dmp_native_support=off
# reboot
```
- 3 Start the Web-based installer.
See [“Starting the Veritas Web-based installer”](#) on page 37.
- 4 On the Select a task and a product page, select **Uninstall a Product** from the Task drop-down list.
- 5 Select **Veritas Dynamic Multi-Pathing** from the Product drop-down list, and click **Next**.
- 6 Indicate the systems on which to uninstall. Enter one or more system names, separated by spaces. Click **Next**.
- 7 After the validation completes successfully, click **Next** to uninstall DMP on the selected system.

- 8 Reboot the systems if DMP native support is on and the systems need a reboot to disable DMP native support. Re-run the uninstallation after the reboot.
- 9 If there are any processes running on the target system, the installer stops the processes. Click **Next**.
- 10 After the installer stops the processes, the installer removes the products from the specified system.
Click **Next**.
- 11 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.
- 12 Click **Finish**.

You see a prompt recommending that you reboot the system, and then return to the Web page to complete additional tasks.

Removing Storage Foundation products using SMIT

Use the following procedure to remove Storage Foundation products using SMIT.

To remove the filesets using SMIT

- 1 Disable DMP native support, if it is enabled. Run the following command to disable DMP native support

```
# vxddmpadm settune dmp_native_support=off
# reboot
```
- 2 Enter this command to invoke SMIT:

```
# smit
```
- 3 In SMIT, select **Software Installation and Maintenance > Software Maintenance and Utilities > Remove Installed Software**.
- 4 Under the "SOFTWARE name" menu, press F4 or Esc-4 to list all software installed on the system.
- 5 Enter "/" for Find, type "VRTS" to find all Veritas filesets, and select the filesets that you want to remove.

- 6 Reboot the system after removing all Storage Foundation filesets.

Note: Reboot is required only if the root device is under DMP control.

- 7 Depending on the choices that were made when Storage Foundation was originally installed, you may find that not all of the listed Storage Foundation filesets are installed on the system. You may also choose to remove the `VRTSvlic` licensing fileset unless this is required by other Veritas software.

Installation reference

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

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 ]

[ -nim LLT_SOURCE ]

[ -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` program command options.

Table A-1 installdmp program options

Option and Syntax	Description
<code>-allpkgs</code>	<p>View a list of all DMP filesets and patches. The <code>installdmp</code> program lists the filesets and patches in the correct installation order.</p> <p>You can use the output to create scripts for command-line installation, or for installations over a network.</p> <p>See the <code>-minpkgs</code> and the <code>-recpkgs</code> options.</p>
<code>-comcleanup</code>	<p>The <code>-comcleanup</code> 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.</p>
<code>-configure</code>	<p>Configure DMP after using <code>-install</code> option to install DMP.</p>
<code>-copyinstallscripts</code>	<p>Use this option when you manually install products and want to use the installation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media.</p> <p>Use this option to copy the installation scripts to an alternate rootpath when you use it with the <code>-rootpath</code> option.</p> <p>The following examples demonstrate the usage for this option:</p> <ul style="list-style-type: none"> ■ <code>./installer -copyinstallscripts</code> Copies the installation and uninstallation scripts for all products in the release to <code>/opt/VRTS/install</code>. It also copies the installation Perl libraries to <code>/opt/VRTSperl/lib/site_perl/release_name</code>. ■ <code>./installproduct_name -copyinstallscripts</code> Copies the installation and uninstallation scripts for the specified product and any subset products for the product to <code>/opt/VRTS/install</code>. It also copies the installation Perl libraries to <code>/opt/VRTSperl/lib/site_perl/release_name</code>. ■ <code>./installer -rootpath alt_root_path -copyinstallscripts</code> The path <code>alt_root_path</code> can be a directory like <code>/rdisk2</code>. In that case, this command copies installation and uninstallation scripts for all the products in the release to <code>/rdisk2/opt/VRTS/install</code>. CPI perl libraries are copied at <code>/rdisk2/opt/VRTSperl/lib/site_perl/release_name</code>. For example, for the 5.1 SP1 the <code>release_name</code> is <code>UXRT51SP1</code>.

Table A-1 `installdmp` program options (*continued*)

Option and Syntax	Description
<code>-hostfile</code>	Specifies the location of a file that contains the system names for the installer.
<code>-ignorepatchreqs</code>	The <code>-ignorepatchreqs</code> option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
<code>-install</code>	Install product filesets on systems without configuring DMP.
<code>-installallpkgs</code>	Selects all the filesets for installation. See the <code>-allpkgs</code> option.
<code>-installminpkgs</code>	Selects the minimum filesets for installation. See the <code>-minpkgs</code> option.
<code>-installrecpkgs</code>	Selects the recommended filesets for installation. See the <code>-recpkgs</code> option.
<code>-keyfile</code> <code>ssh_key_file</code>	Specifies a key file for SSH. The option passes <code>-i ssh_key_file</code> with each SSH invocation.
<code>-license</code>	Register or update product licenses on the specified systems. This option is useful to replace a demo license.
<code>-listpatches</code>	The <code>-listpatches</code> option displays product patches in correct installation order.
<code>-logpath log_path</code>	Specifies that <code>log_path</code> , not <code>/opt/VRTS/install/logs</code> , is the location where install log files, summary files, and response files are saved.
<code>-makeresponsefile</code>	Create a response file. This option only generates a response file and does not install DMP.
<code>-minpkgs</code>	View a list of the minimal filesets and the patches that are required for DMP. The <code>installdmp</code> program lists the filesets and patches in the correct installation order. The list does not include the optional filesets. You can use the output to create scripts for command-line installation, or for installations over a network. See the <code>-allpkgs</code> and the <code>-recpkgs</code> options.

Table A-1 `installdmp` program options (*continued*)

Option and Syntax	Description
<code>-nim LLT_SOURCE</code>	Generates an <code>installp_bundle</code> for the NIM Server to install DMP. You must specify a valid <code>LLT_SOURCE</code> location.
<code>-nolic</code>	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
<code>-patchpath patch_path</code>	Specifies that <code>patch_path</code> contains all patches that the <code>installdmp</code> program is about to install on all systems. The <code>patch_path</code> is the complete path of a directory. Note: You can use this option when you download recent versions of patches.
<code>-pkginfo</code>	Displays a list of packages in the order of installation in a user-friendly format. Use this option with one of the following options: <ul style="list-style-type: none"> ■ <code>-allpkgs</code> If you do not specify an option, <code>-allpkgs</code> is used by default. ■ <code>-minpkgs</code> ■ <code>-recpkgs</code>
<code>-pkgpath pkg_path</code>	Specifies that <code>pkg_path</code> contains all filesets that the <code>installdmp</code> program is about to install on all systems. The <code>pkg_path</code> is the complete path of a directory, usually NFS mounted.
<code>-pkgset</code>	Discovers and lists the 6.0 filesets installed on the systems that you specify.
<code>-pkgtable</code>	Displays the DMP 6.0 filesets in the correct installation order.
<code>-postcheck</code>	Checks that the processes are running and other post-installation checks.
<code>-precheck</code>	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` program options (*continued*)

Option and Syntax	Description
<code>-recpkgs</code>	<p>View a list of the recommended filesets and the patches that are required for DMP. The <code>installdmp</code> program lists the filesets and patches in the correct installation order. The list does not include the optional filesets.</p> <p>You can use the output to create scripts for command-line installation, or for installations over a network.</p> <p>See the <code>-allpkgs</code> and the <code>-minpkgs</code> options.</p>
<code>-redirect</code>	<p>Specifies that the installer need not display the progress bar details during the installation.</p>
<code>-requirements</code>	<p>View a list of required operating system version, required patches, file system space, and other system requirements to install DMP.</p>
<code>-responsefile</code> <code>response_file</code>	<p>Perform automated DMP installation using the system and the configuration information that is stored in a specified file instead of prompting for information.</p> <p>The <code>response_file</code> 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.</p> <p>See “Installing DMP using response files” on page 90.</p> <p>See “Upgrading DMP using response files” on page 90.</p>
<code>-rsh</code>	<p>Specifies that <code>rsh</code> and <code>rcp</code> are to be used for communication between systems instead of <code>ssh</code> and <code>scp</code>. This option requires that systems be preconfigured such that <code>rsh</code> commands between systems execute without prompting for passwords or confirmations</p>
<code>-serial</code>	<p>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.</p>

Table A-1 `installdmp` program options (*continued*)

Option and Syntax	Description
<code>-start</code>	<p>Starts the daemons and processes for DMP.</p> <p>If the <code>installdmp</code> program failed to start up all the DMP processes, you can use the <code>-stop</code> option to stop all the processes and then use the <code>-start</code> option to start the processes.</p> <p>See the <code>-stop</code> option.</p> <p>See “Starting and stopping processes for the Veritas products” on page 49.</p>
<code>-stop</code>	<p>Stops the daemons and processes for DMP.</p> <p>If the <code>installdmp</code> program failed to start up all the DMP processes, you can use the <code>-stop</code> option to stop all the processes and then use the <code>-start</code> option to start the processes.</p> <p>See the <code>-start</code> option.</p> <p>See “Starting and stopping processes for the Veritas products” on page 49.</p>
<code>-tmppath <i>tmp_path</i></code>	<p>Specifies that <i>tmp_path</i> is the working directory for <code>installdmp</code> program. This path is different from the <code>/var/tmp</code> path. This destination is where the <code>installdmp</code> program performs the initial logging and where the <code>installdmp</code> program copies the filesets on remote systems before installation.</p>
<code>-upgrade</code>	<p>Upgrades the installed filesets on the systems that you specify.</p>
<code>-uninstall</code>	<p>Uninstalls DMP from the systems that you specify.</p>
<code>-version</code>	<p>Checks and reports the installed products and their versions. Identifies the installed and missing filesets and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing filesets and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.</p>

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
<code>-comcleanup</code>	The <code>-comcleanup</code> 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.
<code>-copyinstallscripts</code>	<p>Use this option when you manually install products and want to use the installation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media.</p> <p>Use this option to copy the installation scripts to an alternate rootpath when you use it with the <code>-rootpath</code> option.</p> <p>The following examples demonstrate the usage for this option:</p> <ul style="list-style-type: none"> ■ <code>./installer -copyinstallscripts</code> Copies the installation and uninstallation scripts for all products in the release to <code>/opt/VRTS/install</code>. It also copies the installation Perl libraries to <code>/opt/VRTSperl/lib/site_perl/release_name</code>. ■ <code>./installproduct_name -copyinstallscripts</code> Copies the installation and uninstallation scripts for the specified product and any subset products for the product to <code>/opt/VRTS/install</code>. It also copies the installation Perl libraries to <code>/opt/VRTSperl/lib/site_perl/release_name</code>. ■ <code>./installer -rootpath alt_root_path -copyinstallscripts</code> The path <code>alt_root_path</code> can be a directory like <code>/rdisk2</code>. In that case, this command copies installation and uninstallation scripts for all the products in the release to <code>/rdisk2/opt/VRTS/install</code>. CPI perl libraries are copied at <code>/rdisk2/opt/VRTSperl/lib/site_perl/release_name</code>. For example, for the 5.1 SP1 the <code>release_name</code> is <code>UXRT51SP1</code>.

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

Option and Syntax	Description
<code>-hostfile</code>	Specifies the location of a file that contains the system names for the installer.
<code>-keyfile</code> <code>ssh_key_file</code>	Specifies a key file for SSH. The option passes <code>-i ssh_key_file</code> with each SSH invocation.
<code>-logpath log_path</code>	Specifies that <code>log_path</code> , not <code>/opt/VRTS/install/logs</code> , is the location where <code>uninstalldmp</code> program log files, summary file, and response file are saved.
<code>-makeresponsefile</code>	Use this option to create a response file or to verify that your system configuration is ready for uninstalling DMP.
<code>-nolic</code>	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
<code>-redirect</code>	Displays progress details without showing progress bar.
<code>-responsefile</code> <code>response_file</code>	<p>Perform automated DMP uninstallation using the system and the configuration information that is stored in a specified file instead of prompting for information.</p> <p>The <i>response_file</i> must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.</p> <p>See “Uninstalling DMP using response files” on page 91.</p>
<code>-rsh</code>	Specifies that <code>rsh</code> and <code>rscp</code> are to be used for communication between systems instead of <code>ssh</code> and <code>scp</code> . This option requires that systems be preconfigured such that <code>rsh</code> commands between systems execute without prompting for passwords or confirmations
<code>-serial</code>	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.
<code>-tmppath tmp_path</code>	Specifies that <code>tmp_path</code> is the working directory for <code>uninstalldmp</code> program. This path is different from the <code>/var/tmp</code> path. This destination is where the <code>uninstalldmp</code> program performs the initial logging and where the <code>installdmp</code> program copies the filesets on remote systems before installation.

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

Option and Syntax	Description
<code>-version</code>	Checks and reports the installed products and their versions. Identifies the installed and missing filesets and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing filesets and patches where applicable.

Response files

This appendix includes the following topics:

- [About response files](#)
- [Installing DMP using response files](#)
- [Upgrading 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 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 -responsefile /tmp/response_file
```

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

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 -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 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 -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 filesets. Configuration can be performed at a later time using the <code>-configure</code> 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 or 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
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional

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

Variable	Description
CFG{opt}{patchpath}	<p>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.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{pkgpath}	<p>Defines a location, typically an NFS mount, from which all remote systems can install product filesets. The location must be accessible from all target systems.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{tmppath}	<p>Defines the location where a working directory is created to store temporary files and the filesets that are needed during the install. The default location is /var/tmp.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{opt}{rsh}	<p>Defines that <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>
CFG{donotinstall} {fileset}	<p>Instructs the installation to not install the optional filesets in the list.</p> <p>List or scalar: list</p> <p>Optional or required: optional</p>
CFG{donotremove} {fileset}	<p>Instructs the uninstallation to not remove the optional filesets in the list.</p> <p>List or scalar: list</p> <p>Optional or required: optional</p>
CFG{opt}{logpath}	<p>Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.</p> <p>List or scalar: scalar</p> <p>Optional or required: optional</p>

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

Variable	Description
CFG{opt}{configure}	Performs the configuration after the filesets are installed using the <code>-install</code> option. List or scalar: scalar Optional or required: optional
CFG{opt}{upgrade}	Upgrades all filesets installed, without configuration. List or scalar: list Optional or required: optional
CFG{opt}{uninstall}	Uninstalls DMP filesets. List or scalar: scalar Optional or required: optional

Tunable files for installation

This appendix includes the following topics:

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

About setting tunable parameters using the installer or a response file

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

- When you install, configure, or upgrade systems.

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

See [“Setting tunables for an installation, configuration, or upgrade”](#) on page 96.

- 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 97.

- 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 98.

See [“About response files”](#) on page 89.

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

See [“Tunables value parameter definitions”](#) on page 100.

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 100.

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 99.
- 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 100.

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 99.
- 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 `-setttunables` option.

```
# ./installer -tunablesfile tunables_file_name -setttunables [
sys123 sys234 ...]
```

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

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

Setting tunables with an un-integrated response file

You can use the installer to set tunable parameters with an un-integrated response file. You must use the parameters described in this guide. Note that many of the parameters are product-specific. You must select the tunables that you want to use from this guide.

See [“Tunables value parameter definitions”](#) on page 100.

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 99.
- 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 -responsefile response_file_name -tunablesfile  
tunables_file_name -settunables
```

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 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.

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.

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 100.

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.
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.

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

Tunable	Description
dmp_low_impact_probe	(Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_lun_retry_timeout	(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_fabric	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_ownership	(Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_support	(Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
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.

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

Tunable	Description
dmp_probe_threshold	(Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_cycles	(Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_interval	(Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_policy	(Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_state	(Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_retry_count	(Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
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.
vx_bc_bufhwm	(Veritas File System) VxFS metadata buffer cache high water mark. This tunable requires system reboot to take effect.

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

- [About configuring secure shell or remote shell communication modes before installing products](#)
- [Manually configuring and passwordless ssh](#)
- [Restarting the ssh session](#)
- [Enabling rsh for AIX](#)

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 password less communication for you.

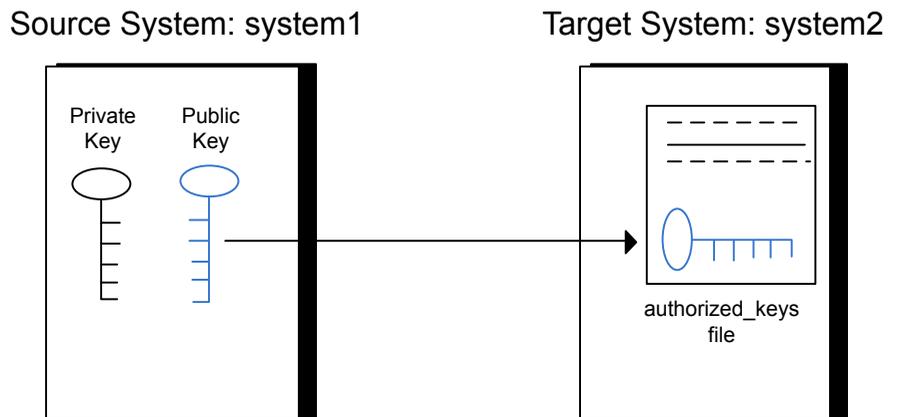
Manually configuring and passwordless ssh

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

Use the secure file transfer program.

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

Use the following command for secure file transfer:

```
system1 # sftp system2
```

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

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

- 2 Enter `yes`.

Output similar to the following is displayed:

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

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

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

The following output is displayed:

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

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

```
sftp> quit
```

- 6 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:
```

- 7 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
```

- 8 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
```

- 9 To log out of the `ssh` session, enter the following command:

```
system2 # exit
```

- 10 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
```

- 11 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 rsh for AIX

To enable `rsh`, create a `/.rhosts` file on each target system. Then add a line to the file specifying the full domain name of the source system. For example, add the line:

```
sysname.domainname.com root
```

Change permissions on the `/.rhosts` file to 600 by typing the following command:

```
# chmod 600 /.rhosts
```

After you complete an installation procedure, delete the `.rhosts` file from each target system to ensure security:

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

Veritas Dynamic Multi-Pathing components

This appendix includes the following topics:

- [Veritas Dynamic Multi-Pathing installation filesets](#)

Veritas Dynamic Multi-Pathing installation filesets

[Table E-1](#) shows the fileset name and contents for each English language fileset for Veritas Dynamic Multi-Pathing. The table also gives you guidelines for which filesets to install based whether you want the minimum, recommended, or advanced configuration.

Table E-1 Veritas Dynamic Multi-Pathing filesets

filesets	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
VRTSveki	Veritas Kernel Interface Contains a common set of modules that other Veritas drivers use.	Minimum

Table E-1 Veritas Dynamic Multi-Pathing filesets (*continued*)

filesets	Contents	Configuration
VRTSvlic	<p>Veritas License Utilities</p> <p>Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.</p>	Minimum
VRTSvxvm	Veritas Volume Manager binaries	Minimum
VRTSsfcp160	<p>Veritas Storage Foundation Common Product Installer</p> <p>The Storage Foundation Common Product installer fileset contains the scripts that perform the following:</p> <ul style="list-style-type: none">■ installation■ configuration■ upgrade■ uninstallation■ adding nodes■ removing nodes■ etc. <p>You can use this script to simplify the native operating system installations, configurations, and upgrades.</p>	Minimum
VRTSsfmh	<p>Veritas Storage Foundation Managed Host</p> <p>Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at:</p> <p>http://www.symantec.com/business/storage-foundation-manager</p>	Recommended
VRTSspt	Veritas Software Support Tools	Recommended

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](#)
- [Troubleshooting an installation on AIX](#)
- [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:

```
# /opt/VRTS/bin/vxkeyless
```

- 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>

Troubleshooting an installation on AIX

Save a copy of `/var/adm/ras/errtmpl` and `/etc/trcfmt` files before you install the product. If the filesets fail to install due to the `template` file is corrupted error message, replace `/var/adm/ras/errtmpl` file and `/etc/trcfmt` file with the ones that you had saved, uninstall all the filesets installed.

Then reinstall.

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 103.

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 maximum number of processes allowed per user may not be large enough. This kernel attribute is a tunable and can be changed on any node of the cluster.

To determine the current value of "Maximum number of PROCESSES allowed per user", enter:

```
# lsattr -H -E -l sys0 -a maxuproc
```

To see the default value of this tunable and its valid range of values, enter:

```
# odmget -q "attribute=maxuproc" PdAt
```

If necessary, you can change the value of the tunable using the smitty interface:

```
# smitty chgsys
```

You can also directly change the CuAt class using the following command:

```
# chdev -l sys0 -a maxuproc=600
```

Increasing the value of the parameter takes effect immediately; otherwise the change takes effect after a reboot.

See the `smitty` and `chdev` 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.

```
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.

Compatibility 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, uninstalling, or upgrading Storage Foundation products when VOM is already present](#)
- [Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present](#)

Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present

Installing Storage Foundation when other Veritas products are installed can create compatibility issues. For example, installing Storage Foundation products when VOM, ApplicationHA, and NetBackup are present on the systems.

Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present

If you plan to install or upgrade Storage Foundation products on systems where VOM has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where SFM or VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the SFM Central Server and Managed Host filesets as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present

If you plan to install or upgrade Storage Foundation on systems where NetBackup has already been installed, be aware of the following compatibility issues:

- When you install or upgrade Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSspb and VRTSicsco. It does not upgrade VRTSat.
- When you uninstall Storage Foundation products where NetBackup is present, the installer does not uninstall VRTSspb, VRTSicsco, and VRTSat.

Index

C

- configuring
 - rsh 27
 - ssh 27

I

- installer program 33
- Installing
 - DMP with the Web-based installer 39
- installing
 - DMP 33

M

- mounting
 - software disc 28

R

- rsh
 - configuration 27

S

- ssh
 - configuration 27

T

- tunables file
 - about setting parameters 95
 - parameter definitions 100
 - preparing 99
 - setting for configuration 96
 - setting for installation 96
 - setting for upgrade 96
 - setting parameters 99
 - setting with no other operations 97
 - setting with un-integrated response file 98

U

- uninstalldmp command 75

- uninstalling
 - DMP 75

W

- Web-based installer 39