Veritas™ Dynamic Multi-Pathing Installation Guide

Solaris

6.0
Technical Support

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

Symantec’s support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

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

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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
Section 1  Installation overview and planning  

Chapter 1  Introducing Veritas Dynamic Multi-Pathing  
About Veritas Dynamic Multi-Pathing  

Chapter 2  Planning to install Veritas Dynamic Multi-Pathing  
About planning for DMP installation  
About installation and configuration methods  

Chapter 3  System requirements  
Release notes  
Hardware compatibility list (HCL)  
Supported operating systems  
Disk space requirements  
Discovering product versions and various requirement information  

Chapter 4  Licensing Veritas products  
About Veritas product licensing  
Setting or changing the product level for keyless licensing  
Installing Veritas product license keys  
Section 2 Installation of Veritas Dynamic Multi-Pathing ........................................................... 27

Chapter 5 Preparing to install Veritas Dynamic Multi-Pathing ................................................................. 29
Installation preparation overview ................................................................................................. 29
Setting environment variables ....................................................................................................... 30
About using ssh or rsh with the Veritas installer ......................................................................... 30
Creating the /opt directory .......................................................................................................... 31
Mounting the product disc ............................................................................................................. 31
Assessing the system for installation readiness ............................................................................ 32
Symantec Operations Readiness Tools ......................................................................................... 32
Prechecking your systems using the Veritas installer ................................................................. 33

Chapter 6 Installing Veritas Dynamic Multi-Pathing using the script-based installer ......................... 35
About the Veritas installer .............................................................................................................. 35
Installing Veritas Dynamic Multi-Pathing .................................................................................... 36
Installing language packages ......................................................................................................... 38
Performing a postcheck on a node ................................................................................................. 38

Chapter 7 Installing Veritas Dynamic Multi-Pathing using the web-based installer ......................... 39
About the Web-based installer ....................................................................................................... 39
Before using the Veritas Web-based installer .............................................................................. 40
Starting the Veritas Web-based installer ....................................................................................... 40
Obtaining a security exception on Mozilla Firefox ...................................................................... 41
Performing a pre-installation check with the Veritas Web-based installer ................................. 42
Installing DMP with the Web-based installer ............................................................................... 42

Chapter 8 Installing Veritas Dynamic Multi-Pathing using other methods ........................................ 45
Installing using JumpStart ............................................................................................................ 45
Overview of JumpStart installation tasks ...................................................................................... 45
Generating the finish scripts ......................................................................................................... 46
Preparing installation resources ..................................................................................................... 47
Adding language pack information to the finish file .................................................................... 48
Chapter 12  Upgrading with Live Upgrade ........................................... 75
  About Live Upgrade ....................................................................... 75
  Supported upgrade paths for Live Upgrade .................................... 76
  Before you upgrade DMP using Solaris Live Upgrade ..................... 77
  Upgrading DMP and Solaris using Live Upgrade ......................... 78
    Creating a new boot environment on the alternate boot disk .......... 79
    Upgrading DMP using the installer for a Live Upgrade ................. 79
    Upgrading DMP manually ....................................................... 80
    Completing the Live Upgrade ................................................. 81
    Verifying Live Upgrade of DMP ............................................. 81
  Upgrading Solaris using Live Upgrade ......................................... 82
    Removing and reinstalling DMP using the installer ...................... 82
  Upgrading DMP using Live Upgrade ........................................... 83
  Administering boot environments .............................................. 84
    Reverting to the primary boot environment ................................ 84
    Switching the boot environment for Solaris SPARC .................. 84
    Switching the boot environment for Solaris x86-64 ................. 86

Chapter 13  Performing post-upgrade tasks .................................... 89
  Updating variables ....................................................................... 89
  Upgrading the Array Support Library ......................................... 89
    Adding JBOD support for storage arrays for which there is not an ASL available ......................................................... 89
    Uns suppressing DMP for EMC PowerPath disks .................. 90
  Verifying the Veritas Dynamic Multi-Pathing upgrade ................. 99

Section 5  Uninstallation of Veritas Dynamic Multi-Pathing ............... 101

Chapter 14  Uninstalling Veritas Dynamic Multi-Pathing .................. 103
  About removing Veritas Dynamic Multi-Pathing ......................... 103
  Preparing to uninstall ................................................................ 103
    Remote uninstallation ......................................................... 104
  Uninstalling Veritas Dynamic Multi-Pathing .............................. 104
  Uninstalling DMP with the Veritas Web-based installer ................. 105
  Uninstalling Veritas Dynamic Multi-Pathing using the pkgrm command ............................................................... 106
  Uninstalling the language packages using the pkgrm command ............................................................... 107
Section 6  Installation reference ................................................................. 109
Appendix A  Installation scripts .................................................................. 111
  Command options for the installation script ........................................ 111
  Command options for uninstall script ............................................... 117
Appendix B  Response files ........................................................................ 121
  About response files ........................................................................ 121
  Installing DMP using response files .............................................. 122
  Upgrading DMP using response files ............................................. 122
  Uninstalling DMP using response files .......................................... 123
  Syntax in the response file ................................................................ 123
  Response file variable definitions .................................................. 124
Appendix C  Tunable files for installation .................................................. 127
  About setting tunable parameters using the installer or a response file ........................................................................ 127
  Setting tunables for an installation, configuration, or upgrade ........ 128
  Setting tunables with no other installer-related operations ............ 129
  Setting tunables with an un-integrated response file .................... 130
  Preparing the tunables file ............................................................. 131
  Setting parameters for the tunables file .......................................... 131
  Tunables value parameter definitions .......................................... 132
Appendix D  Configuring the secure shell or the remote shell for communications ........................................................................ 137
  About configuring secure shell or remote shell communication modes before installing products ................................................. 137
  Manually configuring and passwordless ssh .................................. 138
  Restarting the ssh session ............................................................... 142
  Enabling and disabling rsh for Solaris .......................................... 143
Appendix E  Veritas Dynamic Multi-Pathing components .......................... 145
  Veritas Dynamic Multi-Pathing installation packages ..................... 145
Appendix F  Troubleshooting installation issues ....................................... 147
  Restarting the installer after a failed connection ............................ 147
  What to do if you see a licensing reminder ................................... 147
  Troubleshooting information ......................................................... 148
Incorrect permissions for root on remote system ............................................... 148
Inaccessible system ......................................................................................... 149

Appendix G Compatability issues when installing DMP with other products ................................................................................................................. 151

Installing, uninstalling, or upgrading Storage Foundation products
when other Veritas products are present ......................................................... 151
Installing, uninstalling, or upgrading Storage Foundation products
when VOM is already present ........................................................................ 152
Installing, uninstalling, or upgrading Storage Foundation products
when NetBackup is already present ................................................................. 152

Index ..................................................................................................................... 153
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 ZFS. You can create ZFS pools on DMP metadevices. DMP supports only non-root ZFS file systems.

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

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

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

About Veritas Dynamic Multi-Pathing
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: 6.0.2.

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 39.

■ 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 121.

■ JumpStart
  You can use the Veritas product installer or the product-specific installation script to generate a Jumpstart script file. Use the generated script to install Veritas packages from your JumpStart server.
System requirements

This chapter includes the following topics:
- Release notes
- Hardware compatibility list (HCL)
- Supported operating systems
- Disk space requirements
- 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
```

## Discovering product versions and various requirement information

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

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

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

- The installed version of all released Storage Foundation and High Availability Suite of products
- The required packages or patches (if applicable) that are missing
- The available updates (including patches or hotfixes) from Symantec Operations Readiness Tools (SORT) for the installed products
To run the version checker

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

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

Discovering product versions and various requirement information
Licensing Veritas products

This chapter includes the following topics:

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

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

- Install a license key for the product and features that you want to install.
  When you purchase a Symantec product, you receive a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased.

- Continue to install without a license key.
  The installer prompts for the product modes and options that you want to install, and then sets the required product level.
Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled or continue with keyless licensing by managing the server or cluster with a management server, 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 upgrade to this release from a prior release of the Veritas software, the product installer does not change the license keys that are already installed. The existing license keys may not activate new features in this release.

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

- Run the vxkeyless command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See “Setting or changing the product level for keyless licensing” on page 24.
  See the vxkeyless(1m) manual page.

- Use the vxlicinst command to install a valid product license key for the products you have purchased.
  See “Installing Veritas product license keys” on page 26.
  See the vxlicinst(1m) manual page.

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

---

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

---

### Setting or changing the product level for keyless licensing

The keyless licensing method uses product levels to determine the Veritas products and functionality that are licensed. In order to use keyless licensing, you must set up a Management Server to manage your systems.
For more information and to download the management server, see the following URL:

http://go.symantec.com/vom

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

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

**To set or change the product level**

1. 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 product license keys

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

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

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

To install a new license

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

   ```
   # cd /opt/VRTS/bin
   
   # ./vxlicinst -k 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
- Creating the /opt directory
- 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>
<thead>
<tr>
<th>Installation task</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain product licenses.</td>
<td>See “About Veritas product licensing” on page 23.</td>
</tr>
<tr>
<td>Download the software, or insert the product DVD.</td>
<td>See “Mounting the product disc” on page 31.</td>
</tr>
<tr>
<td>Set environment variables.</td>
<td>See “Setting environment variables” on page 30.</td>
</tr>
<tr>
<td>Create the /opt directory, if it does not exist.</td>
<td>See “Creating the /opt directory” on page 31.</td>
</tr>
</tbody>
</table>
### 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:

  ```bash
  $ 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:

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

### About using ssh or rsh with the Veritas installer

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

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

- When you 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 137.

## Creating the `/opt` directory

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

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

## Mounting the product disc

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

**To mount the product disc**

1. Log in as superuser on a system where you want to install DMP. The systems must be in the same subnet.

2. Insert the product disc into a DVD drive that is connected to your system.

3. If Solaris volume management software is running on your system, the software disc automatically mounts as `/cdrom/cdrom0`.

4. If Solaris volume management software is not available to mount the DVD, you must mount it manually. After you insert the software disc, enter:

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

Where `c0t6d0s2` is the default address for the disc drive.
Assessing the system for installation readiness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Veritas Dynamic Multi-Pathing 6.0.

**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 32.

**Prechecking your systems using the installer**

Perform 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 33.

---

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.
Preparing to install Veritas Dynamic Multi-Pathing

Assessing the system for installation readiness
Installing Veritas Dynamic Multi-Pathing using the script-based installer

This chapter includes the following topics:

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

About the Veritas installer

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.
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 137.

2. Load and mount the software disc.

   See “Mounting the product disc” on page 31.

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

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

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

   
   ```
   # ./installer
   ```

5. Enter 1 to install and press the Return key.

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

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

8. Select one of the following installation options:

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

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

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

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

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

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

If you have a valid license key, select 1 and enter the license key at the prompt. To install through keyless licensing, select 2.

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

For more information, go to the following Web site:

http://go.symantec.com/sfhakeyless

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

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

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

Installing language packages

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

To install the language packages on the server

1. Insert the "Language" disc into the DVD-ROM or CD-ROM drive. With Solaris volume management software, the disc is automatically mounted as /cdrom/cdrom0.

2. Install the language packages using the `install_lp` command.

   ```bash
   cd /cdrom/cdrom0
   ./.install_lp
   ```

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.

  ```bash
  ./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 40.

See “Starting the Veritas Web-based installer” on page 40.

### Before using the Veritas Web-based installer

The Veritas Web-based installer requires the following configuration.

<table>
<thead>
<tr>
<th>System</th>
<th>Function</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target system</td>
<td>The systems where you plan to install the Veritas products.</td>
<td>Must be a supported platform for Veritas Dynamic Multi-Pathing 6.0.</td>
</tr>
<tr>
<td>Installation server</td>
<td>The server where you start the installation. The installation media is accessible from the installation server.</td>
<td>Must use the same operating system as the target systems and must be at one of the supported operating system update levels.</td>
</tr>
<tr>
<td>Administrative system</td>
<td>The system where you run the Web browser to perform the installation.</td>
<td>Must have a Web browser. Supported browsers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Internet Explorer 6, 7, and 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Firefox 3.x and later</td>
</tr>
</tbody>
</table>

### Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.
To start the Web-based installer

1. Start the Veritas XPortal Server process `xprtlwid`, on the installation server:
   
   ```bash
   # ./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 40.
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 42.
2. Start the Web-based installer.
   See “Starting the Veritas Web-based installer” on page 40.
3. Select **Install a Product** from the **Task** drop-down list.
4. Select **Veritas Dynamic Multi-Pathing** from the Product drop-down list, and click Next.
5. On the License agreement page, read the End User License Agreement (EULA). To continue, select **Yes, I agree** and click **Next**.
6. Choose minimal or recommended packages. Click **Next**.
7. Indicate the systems where you want to install. Separate multiple system names with spaces. Click **Next**.
8 If you have not yet configured a communication mode among systems, you have the option to let the installer configure ssh or rsh. If you choose to allow this configuration, select the communication mode and provide the superuser passwords for the systems.

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

10 After the installation completes, you must choose your licensing method. On the license page, select one of the following tabs:

- **Keyless licensing**

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

  For more information, go to the following website:

  [http://go.symantec.com/sfhakeyless](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.
Installing Veritas Dynamic Multi-Pathing using other methods

This chapter includes the following topics:

- Installing using JumpStart
- Installing DMP using the pkgadd command

Installing using JumpStart

These JumpStart instructions assume a working knowledge of JumpStart. See the JumpStart documentation that came with your operating system for details on using JumpStart.

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

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

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

See “Using a Flash archive to install DMP and the operating system” on page 49.

Overview of JumpStart installation tasks

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

1. Add a client (register to the JumpStart server). See the JumpStart documentation that came with your operating system for details.

2. Read the JumpStart installation instructions.

3. Generate the finish scripts.
   See “Generating the finish scripts” on page 46.

4. Prepare shared storage installation resources.
   See “Preparing installation resources” on page 47.

5. Modify the rules file for JumpStart.
   See the JumpStart documentation that came with your operating system for details.

6. Install the operating system using the JumpStart server.

7. When the system is up and running, run the installer command from the installation media to configure the Veritas software.

   # /opt/VRTS/install/installer -configure

Generating the finish scripts

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

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

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

   Or

   ```
   ./installprod -jumpstart directory_to_generate_script
   ```

   Where `prod` is the product's installation command, and
   `directory_to_generate_script` is where you want to put the product's script.

   For example:

   ```
   # ./installldmp -jumpstart /js_scripts
   ```

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

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

Preparing installation resources

Prepare resources for the JumpStart installation.
To prepare the resources

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

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

2. Generate the response file with the list of packages.

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

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

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

Adding language pack information to the finish file

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

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

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

If you downloaded the language pack:

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

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

3. The finish script resembles:

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

Using a Flash archive to install DMP and the operating system

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

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

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

- If you plan to start flar (flash archive) creation from bare metal, perform step 1 through step 10.

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

**Flash archive creation overview**

1. Ensure that you have installed Solaris 10 on the master system.
2. Use JumpStart to create a clone of a system.
3. Reboot the cloned system.
4. Install the Veritas products on the master system.
   Perform one of the installation procedures from this guide.
5. If you have configured the product on the master system, create the vrts_deployment.sh file and the vrts_deployment.cf file and copy them to the master system.
   See “Creating the Veritas post-deployment scripts” on page 50.
6. Use the `flarcreate` command to create the Flash archive on the master system.
7. Copy the archive back to the JumpStart server.
8. Use JumpStart to install the Flash archive to the selected systems.
9. Configure the Veritas product on all nodes in the cluster. Start configuration with the following command:
   ```
   # /opt/VRTS/install/installdmp -configure
   ```

**Creating the Veritas post-deployment scripts**

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

To create the post-deployment scripts

1. Mount the product disc.
2. From the prompt, run the `--flash_archive` option for the installer. Specify a directory where you want to create the files.
   ```
   # ./installer --flash_archive /tmp
   ```
3 Copy the vrts_postedeployment.sh file and the vrts_postedeployment.cf file to the golden system.

4 On the golden system perform the following:
   ■ Put the vrts_postdeployment.sh file in the /etc/flash/postdeployment directory.
   ■ Put the vrts_postdeployment.cf file in the /etc/vx directory.

5 Make sure that the two files have the following ownership and permissions:

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

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

### Installing DMP using the pkgadd command

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

To install DMP using the pkgadd command

1 Mount the software disc.
   
   See “Mounting the product disc” on page 31.

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

   # cp /cdrom/cdrom0/pkgs/VRTS* /tmp/pkgs
3 Create the admin file in the current directory. Specify the `--adminfile` option when you use the `pkgadd` command:

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

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

- `minpkgs`
- `recpkgs`
- `allpkgs`

5 Install the packages listed in step 4.

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

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

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

- `minpkgs`
- `recpkgs`
- `allpkgs`

7 Verify that the packages are installed:

```plaintext
# pkginfo -1 packagename
```

8 Start the processes.
Verification of the installation

- Chapter 9. Verifying the Veritas Dynamic Multi-Pathing installation
Verifying that the products were installed

Verify that the DMP products are installed.
Use the pkginfo command to check which packages have been installed.

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

See “Veritas Dynamic Multi-Pathing installation packages” on page 145.
You can verify the version of the installed product. Use the following command:

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

Use the following sections to further verify the product installation.

Installation log files

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

The log files include the following types of text files:

- **Installation log file**: The installation log file contains all commands executed during the procedure, their output, and errors generated by the commands. This file is for debugging installation problems and can be used for analysis by Veritas Support.

- **Response file**: The response file contains the configuration information that you entered during the procedure. You can use the response file for future installation procedures by invoking an installation script with the `responsefile` option. The response file passes arguments to the script to automate the installation of that product. You can edit the file to automate installation and configuration of additional systems.

- **Summary file**: The summary file contains the results of the installation by the common product installer or product installation scripts. The summary includes the list of the packages, and the status (success or failure) of each package. The summary also indicates which processes were stopped or restarted during the installation. After installation, refer to the summary file to determine whether any processes need to be started.

### Starting and stopping processes for the Veritas products

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

**To stop the processes**

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

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

  ```bash
  # ./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:
  
  ```bash
  # ./installer -start
  ```
Verifying the Veritas Dynamic Multi-Pathing installation

Starting and stopping processes for the Veritas products
Upgrading Veritas Dynamic Multi-Pathing

- Chapter 10. Preparing to upgrade
- Chapter 11. Upgrading Veritas Dynamic Multi-Pathing
- Chapter 12. Upgrading with Live Upgrade
- Chapter 13. Performing post-upgrade tasks
Preparing to upgrade

This chapter includes the following topics:

■ About upgrading
■ About the different ways that you can upgrade
■ 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 “About the different ways that you can upgrade” on page 61.

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.

About the different ways that you can 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.
### Supported upgrade paths for DMP

The following tables describe upgrading to 6.0.

#### Table 10-2   Solaris SPARC upgrades using the script- or Web-based installer

<table>
<thead>
<tr>
<th>Veritas software versions</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 SP1</td>
<td>Upgrade the OS to at least Solaris 10, then use the installer to upgrade to 6.0.</td>
<td>Use the installer to upgrade to 6.0.</td>
</tr>
<tr>
<td>5.1 SP1 RPx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New installation</td>
<td>N/A</td>
<td>Use the installer to install 6.0.</td>
</tr>
</tbody>
</table>

#### Table 10-3   Solaris x64 upgrades using the script- or Web-based installer

<table>
<thead>
<tr>
<th>Veritas software versions</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 SP1*</td>
<td>Use the installer to upgrade to 6.0.</td>
</tr>
<tr>
<td>5.1 SP1 RPx</td>
<td></td>
</tr>
<tr>
<td>New installation</td>
<td>Use the installer to upgrade to 6.0.</td>
</tr>
</tbody>
</table>

*When you upgrade to 6.0 from 5.1 SP1 using the Web-based installer, you must first upgrade to 5.1 SP1 RP1 if you want the installer to create a backup of the
boot disk. You can upgrade directly to 6.0 from 5.1 SP1 if you do not want the installer to create a backup of the boot disk.

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/
- For Solaris 10, make sure that all non-global zones are booted and in the running state before you use the Veritas product installer to upgrade the Storage Foundation products in the global zone. If the non-global zones are not mounted and running at the time of the upgrade, you must upgrade each package in each non-global zone manually.
  For Live Upgrade, if the alternative root environment also has a zone, you cannot install VRTSodm. You must remove the VRTSodm package first then install the Storage Foundation product. After you reboot the alternative root, you can install VRTSodm.
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.
- Make sure that all users are logged off and that all major user applications are properly shut down.
- Make sure that you have created a valid backup.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the packages, for example /packages/Veritas when the root file system has enough space or /var/tmp/packages if the /var file system has enough space.
  Do not put the files under /tmp, which is erased during a system reboot. Do not put the files on a file system that is inaccessible prior to running the upgrade script.
  You can use a Veritas-supplied disc for the upgrade as long as modifications to the upgrade script are not required. If /usr/local was originally created as a slice, modifications are required.
- For any startup scripts in /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.

- Any swap partitions not in rootdg must be commented out of /etc/vfstab. If possible, swap partitions other than those on the root disk should be commented out of /etc/vfstab and not mounted during the upgrade. Active swap partitions that are not in rootdg cause upgrade_start to fail.

- Make sure the file systems are clean before upgrading.

- Symantec recommends that you upgrade VxFS disk layouts to a supported version prior to installing VxFS 6.0. Unsupported disk layout versions 4, 5, and 6 can be mounted for the purpose of online upgrading in VxFS 6.0. You can upgrade unsupported layout versions online before installing VxFS 6.0.

- Upgrade arrays (if required).

- Make sure that you have worked out all terminal emulation issues. Make sure that the terminal you use is fully functional for OpenBoot prompts and single-user and multi-user run levels.

- To reliably save information on a mirrored disk, shut down the system and physically remove the mirrored disk. Removing the disk in this manner offers a failback point.

Creating backups

Save relevant system information before the upgrade.

To create backups

1. Log in as superuser.

2. Before the upgrade, ensure that you have made backups of all data that you want to preserve.

   Back up the /etc/system file.

3. 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 package, VRTSaslapm. The array support package includes the array support previously
included in the VRTSvxvm package. The array support package also includes support previously packaged as external array support libraries (ASLs) and array policy modules (APMs).

See the 6.0 Hardware Compatibility List for information about supported arrays. See “Hardware compatibility list (HCL)” on page 19.

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

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

For more information about array support, see the Veritas Storage Foundation Administrator's Guide.
Upgrading Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- Upgrading Veritas Dynamic Multi-Pathing with the product installer when OS upgrade is not required
- Upgrading Veritas Dynamic Multi-Pathing to 6.0 using the product installer or manual steps
- Upgrading Veritas Dynamic Multi-Pathing using the Veritas Web-based installer
- Upgrading the Solaris operating system
- Upgrading language packages

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

This section describes upgrading to the current Veritas Dynamic Multi-Pathing if the root disk is unencapsulated, and you do not intend to upgrade your Solaris version. Only use this procedure if you are already running a version of Solaris that is supported with 6.0.

Use this procedure to upgrade Veritas Dynamic Multi-Pathing.

To upgrade Veritas Dynamic Multi-Pathing

1. Log in as superuser.
2. If your system has separate \texttt{/opt} and \texttt{/var} file systems, make sure they are mounted before proceeding with installation.
3 Load and mount the disc. If you downloaded the software, navigate to the top level of the download directory.

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

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

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

6 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.

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

8 The installer lists the packages and any patches to install or to update. You are prompted to confirm that you are ready to upgrade.

9 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.

10 The installer stops, uninstalls, reinstalla, and starts specified packages.

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

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

13 Reboot the systems if the installer prompts reboot to enable DMP native support.
Upgrading Veritas Dynamic Multi-Pathing to 6.0 using the product installer or manual steps

This section describes upgrading DMP from a prior release to 6.0. Symantec recommends that you perform this upgrade from single-user mode.

Upgrading Veritas Dynamic Multi-Pathing using manual steps

This section describes upgrading from a previous version of Veritas Dynamic Multi-Pathing to the current Veritas Dynamic Multi-Pathing (6.0) when you do not intend to upgrade your Solaris version. Only use this procedure if you are already running a version of Solaris that is supported with 6.0.

To upgrade Veritas Dynamic Multi-Pathing

1 Unmount any mounted VxFS file systems.

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

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

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

   To remove the package, use the `pkg rm` command as follows:

   ```
   # pkg rm VRTSfsnbl
   ```

   Respond to any system messages as needed.

   The libraries contained in this package are included in the VRTSvxfs package in 6.0.

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

4 Load and mount the software disc.

   See “Mounting the product disc” on page 31.

5 Change to the directory containing the DMP packages.

   ```
   # cd /dvd_mount
   ```
6 Remove the Veritas packages from your existing installation.
   Refer to the Veritas Dynamic Multi-Pathing Installation Guide for the previous release to obtain the list of packages to remove.

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

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

8 Use the `pkgadd` and `patchadd` commands to install the packages from the previous steps.

   ```
   # pkgadd -d . package_name.pkg
   # patchadd patch_id
   ```

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

---

**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 40.

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.
Upgrading the Solaris operating system

If you are running Veritas Dynamic Multi-Pathing 6.0 with an earlier release of the Solaris operating system, you can upgrade the Solaris operating system using the following procedure.

**Warning:** You should only use this procedure to upgrade the Solaris operating system if you are running Veritas Dynamic Multi-Pathing 6.0.

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

**To upgrade the Solaris operating system only**

1. Bring the system down to single-user mode using the following command:
   ```
   # init S
   ```
   You must mount `/opt` manually if `/opt` is on its own partition.

2. Load and mount the software disc from the currently installed version of Veritas Dynamic Multi-Pathing.
   See “Mounting the product disc” on page 31.

3. Change directory:
   ```
   # cd /mount_point/scripts
   ```

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

5. Run the `upgrade_start` script so that the system can come up with partitions. The `upgrade_start` script searches for volumes containing file systems, and if any are found, converts them to partitions:
   ```
   # ./upgrade_start
   ```
6 Bring the system down to run level 0.
   # init 0

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

8 After installing the Solaris operating system, install any Solaris patches
   required by Veritas Dynamic Multi-Pathing 6.0.
   See the Veritas Dynamic Multi-Pathing Release Notes.

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

10 Ensure that /opt is mounted.

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

12 If you upgraded to Solaris 10, you must reinstall certain Veritas Dynamic
   Multi-Pathing packages in order to support Solaris 10 functionality.
   To reinstall the required packages, follow the steps below:

   ■ Remove the existing packages in the reverse order of their installation.
     For example, if you chose the installation of all packages and patches then
     uninstall those in the following order.

   ■ Run the following commands.
     To obtain a list of recommended packages to install:
     
     # ./installdmp -recpkgs

     Or
     To obtain a list of all packages to install:
     
     # ./installdmp -allpkgs

   ■ Change to the directory containing the appropriate packages.
     
     # cd /mount_point/pkgs
Use the `pkgadd` command to install the packages from the list you generated.

- Reboot the system.

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

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

### Upgrading language packages

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

Install the language packages as for an initial installation.

See “Installing language packages” on page 38.
Upgrading language packages
Upgrading with Live Upgrade

This chapter includes the following topics:

■ About Live Upgrade
■ Supported upgrade paths for Live Upgrade
■ Before you upgrade DMP using Solaris Live Upgrade
■ Upgrading DMP and Solaris using Live Upgrade
■ Upgrading Solaris using Live Upgrade
■ Upgrading DMP using Live Upgrade
■ Administering boot environments

About Live Upgrade

You can use Live Upgrade to perform the following types of upgrade:

■ Upgrade the operating system and DMP.
  See “Upgrading DMP and Solaris using Live Upgrade” on page 78.
■ Upgrade the operating system.
  See “Upgrading Solaris using Live Upgrade” on page 82.
■ Upgrade DMP.
  See “Upgrading DMP using Live Upgrade” on page 83.

Figure 12-1 illustrates an example of an upgrade of Veritas products from 5.1 SP1 to 6.0, and the operating system from Solaris 9 to Solaris 10.
Some service groups (failover and parallel) may be online in this cluster and they are not affected by the Live Upgrade process. The only downtime experienced is when the server is rebooted to boot into the alternate boot disk.

### Supported upgrade paths for Live Upgrade

The systems where you plan to use Live Upgrade must run Solaris 9 or Solaris 10. You can upgrade from systems that run Solaris 9, but DMP 6.0 is not supported on Solaris 9.

DMP version must be at least 5.1 SP1.

You can use Live Upgrade in the following virtualized environments:

<table>
<thead>
<tr>
<th>Environment</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris native zones</td>
<td>Perform Live Upgrade to upgrade both global and local zones. See “Upgrading DMP and Solaris using Live Upgrade” on page 78.</td>
</tr>
</tbody>
</table>
Table 12-1  Live Upgrade support in virtualized environments (continued)

<table>
<thead>
<tr>
<th>Environment</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris branded zones (BrandZ)</td>
<td>Perform Live Upgrade to upgrade the global zone.</td>
</tr>
<tr>
<td></td>
<td>See “Upgrading DMP and Solaris using Live Upgrade” on page 78.</td>
</tr>
<tr>
<td></td>
<td>Manually upgrade the branded zone separately.</td>
</tr>
<tr>
<td></td>
<td>Note that while you can perform a Live Upgrade in the presence of branded zones, the branded zones are not upgraded.</td>
</tr>
<tr>
<td>Oracle VM Server for SPARC</td>
<td>Perform Live Upgrade on the Control domain only.</td>
</tr>
<tr>
<td></td>
<td>Perform Live Upgrade on the Guest domain only.</td>
</tr>
<tr>
<td></td>
<td>Use the standard Live Upgrade procedure for both types of logical domains.</td>
</tr>
<tr>
<td></td>
<td>See “Upgrading DMP and Solaris using Live Upgrade” on page 78.</td>
</tr>
</tbody>
</table>

Before you upgrade DMP using Solaris Live Upgrade

Before you upgrade, perform the following procedure.

To prepare for the Live Upgrade

1  Make sure that the DMP installation media and the operating system installation images are available and on hand.

2  On the nodes to be upgraded, select an alternate boot disk that is at least the same size as the root partition of the primary boot disk.

3  On the primary boot disk, patch the operating system for Live Upgrade. Patch 137477-01 is required. Verify that this patch is installed.

4  The version of the Live Upgrade packages must match the version of the operating system to which you want to upgrade on the alternate boot disk. If you are upgrading the Solaris operating system, do the following steps:
   - Remove the installed Live Upgrade packages for the current operating system version:
     - All Solaris versions: SUNWluu, SUNWlur packages.
     - Solaris 10 update 7 or later also requires: SUNWlucfg package.
   - From the new Solaris installation image, install the new versions of the following Live Upgrade packages:
All Solaris versions: SUNWluu, SUNWlur, and SUNWlucfg packages.

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

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

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

In the procedure examples, the primary or current boot environment resides on Disk0 (c0t0d0) and the alternate or inactive boot environment resides on Disk1 (c0t1d0).

## Upgrading DMP and Solaris using Live Upgrade

Upgrading DMP using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See “Before you upgrade DMP using Solaris Live Upgrade” on page 77.

- Create a new boot environment on the alternate boot disk.
  See “Creating a new boot environment on the alternate boot disk” on page 79.

- Upgrade to Veritas Dynamic Multi-Pathing 6.0 on the alternate boot environment manually or using the installer.
  To upgrade DMP manually, refer to the following procedure:
    - See “Upgrading DMP manually” on page 80.
  To upgrade DMP using the installer, refer to the following procedure:
    - See “Upgrading DMP using the installer for a Live Upgrade” on page 79.

- Switch the alternate boot environment to be the new primary.
  See “Completing the Live Upgrade” on page 81.

- Verify Live Upgrade of DMP.
  See “Verifying Live Upgrade of DMP” on page 81.
Creating a new boot environment on the alternate boot disk

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

At the end of the process:

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

To create a new boot environment on the alternate boot disk

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

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

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

Upgrading DMP using the installer for a Live Upgrade

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

At the end of the process the following occurs:

- Veritas Dynamic Multi-Pathing 6.0 is installed on the alternate boot disk.

To perform Live Upgrade of DMP using the installer

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

2. Run the installer script specifying the root path as the alternate boot disk, enter the following:
3 Enter the names of the nodes that you want to upgrade to Veritas Dynamic Multi-Pathing 6.0.

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

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

5 Verify that the version of the Veritas packages on the alternate boot disk is 6.0.

   # pkginfo -R /altroot.5.10 -l VRTSpkname

   For example:

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

**Upgrading DMP manually**

At the end of the process the following occurs:

- Veritas Dynamic Multi-Pathing 6.0 is installed on the alternate boot disk.

To perform **Live Upgrade of DMP manually**

1 Remove the DMP packages on the alternate boot disk in the following order:
   - For Dynamic Multi-Pathing (DMP):

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

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

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

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

     For example:

     # pkgadd -R /altroot.5.10 -d package_name.pkg
Where you replace `package_name.pkg` with a package's name, for example `VRTSperl.pkg`.

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

3. Verify that the version of the Veritas packages on the alternate boot disk is 6.0.

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

For example:

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

### Completing the Live Upgrade

At the end of the process:

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

To **complete the Live Upgrade**

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

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

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

### Verifying Live Upgrade of DMP

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

1. Verify that the alternate boot environment is active.
   ```
   # lустatus
   ```
   If the alternate boot environment is not active, you can revert to the primary boot environment.
   See “Reverting to the primary boot environment” on page 84.

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

Upgrading Solaris using Live Upgrade

Upgrading Solaris using Live Upgrade involves the following steps:

- Preparing to upgrade using Solaris Live Upgrade.
  See “Before you upgrade DMP using Solaris Live Upgrade” on page 77.

- Creating a new boot environment on the alternate boot disk
  See “Creating a new boot environment on the alternate boot disk” on page 79.

- Removing and reinstalling Veritas Dynamic Multi-Pathing 6.0 on the alternate boot environment:
  See “Removing and reinstalling DMP using the installer” on page 82.

  **Note:** Do NOT configure the Veritas Dynamic Multi-Pathing 6.0.

- Switching the alternate boot environment to be the new primary
  See “Completing the Live Upgrade” on page 81.

- Verifying Live Upgrade of DMP.
  See “Verifying Live Upgrade of DMP” on page 81.

Removing and reinstalling DMP using the installer

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

At the end of the process the following occurs:

- Veritas Dynamic Multi-Pathing 6.0 is installed on the alternate boot disk, with the correct binaries for the new operating system version.
To remove and reinstall DMP using the installer

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

   ```
   # /opt/VRTS/install/uninstallmp -rootpath altrootpath
   ```

2. Enter the names of the nodes that you want to uninstall.
   The installer displays the list of packages that will be uninstalled.

3. Press `Return` to continue.

4. DMP is uninstalled from the alt disk.

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

6. Run the `installmp` command specifying the rootpath, for example:

   ```
   # installmp -rootpath altrootpath
   ```

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

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

Upgrading DMP using Live Upgrade

Perform the Live Upgrade manually or use the installer. The nodes will not form a cluster until all of the nodes are upgraded to Veritas Dynamic Multi-Pathing 6.0. At the end of the Live Upgrade of the last node, all the nodes must boot from the alternate boot environment and join the cluster.

Upgrading DMP using Live Upgrade involves the following steps:

- Prepare to upgrade using Solaris Live Upgrade.
  See “Before you upgrade DMP using Solaris Live Upgrade” on page 77.

- Create a new boot environment on the alternate boot disk.
  See “Creating a new boot environment on the alternate boot disk” on page 79.

- Upgrade to Veritas Dynamic Multi-Pathing 6.0 on the alternate boot environment manually or using the installer. Refer to one of the following:
  - To upgrade DMP manually:
    - See “Upgrading DMP manually” on page 80.
  - To upgrade DMP using the installer:
    - See “Upgrading DMP using the installer for a Live Upgrade” on page 79.
Switch the alternate boot environment to be the new primary. See “Completing the Live Upgrade” on page 81.


Administering boot environments

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

Reverting to the primary boot environment

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

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

Switching the boot environment for Solaris SPARC

You do not have to perform the following procedures to switch the boot environment when you use the vxlufinish scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

Two different procedures exist to switch the boot environment, choose one of the following procedures based on the encapsulation of the root disk:

- See “To switch the boot environment if the root disk is not encapsulated” on page 85.

- See “To switch the boot environment if the root disk is encapsulated” on page 86.

The switching procedures for Solaris SPARC vary, depending on whether VxVM encapsulates the root disk.
To switch the boot environment if the root disk is not encapsulated

1. Display the status of Live Upgrade boot environments.

```bash
# lustatus
```

<table>
<thead>
<tr>
<th>Boot Environment</th>
<th>Is Complete</th>
<th>Is Active</th>
<th>Can Copy Now</th>
<th>On Reboot</th>
<th>Delete Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>source.2657</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>dest.2657</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>-</td>
</tr>
</tbody>
</table>

In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657)

2. Unmount any file systems that are mounted on the alternate root disk (dest.2657).

```bash
# lufslist dest.2657
```

```
boot environment name: dest.2657

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>fstype</th>
<th>device</th>
<th>size</th>
<th>Mounted on</th>
<th>Mount Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/dsk/c0t0d0s1</td>
<td>swap</td>
<td>4298342400</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s0</td>
<td>ufs</td>
<td>15729328128</td>
<td>/</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s5</td>
<td>ufs</td>
<td>8591474688</td>
<td>/var</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s3</td>
<td>ufs</td>
<td>5371625472</td>
<td>/vxfs</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
```

```bash
# luumount dest.2657
```

3. Activate the Live Upgrade boot environment.

```bash
# luactivate dest.2657
```

4. Reboot the system.

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

The system automatically selects the boot environment entry that was activated.
To switch the boot environment if the root disk is encapsulated

1 Display the current boot disk device and device aliases

   # eeprom
   boot-device=vx-rootdg vx-int_disk
   use-nvramrc?=true
   nvramrc=devalias vx-int_disk /pci@1c,600000/scsi@2/disk@0,0:a
   devalias vx-rootdg01 /pci@1c,600000/scsi@2/disk@1,0:a

2 Set the device from which to boot using the eeprom command. This example shows booting from the primary root disk.

   # eeprom boot-device=vx-rootdg01

3 Reboot the system.

   # shutdown -g0 -i6 -y

Switching the boot environment for Solaris x86-64

You do not have to perform the following procedures to switch the boot environment when you use the vxlufinish scripts to process Live Upgrade. You must perform the following procedures when you perform a manual Live Upgrade.

Two different procedures exist to switch the boot environment, choose one of the following procedures based on the encapsulation of the root disk:

- See “To switch the boot environment if root disk is not encapsulated” on page 87.
- See “To switch the boot environment if root disk is encapsulated” on page 88.
To switch the boot environment if root disk is not encapsulated

1. Display the status of Live Upgrade boot environments.

```bash
# lustatus
```

<table>
<thead>
<tr>
<th>Boot Environment Name</th>
<th>Complete</th>
<th>Active Now</th>
<th>Active On Reboot</th>
<th>Can Delete</th>
<th>Copy Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>source.2657</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>-</td>
</tr>
<tr>
<td>dest.2657</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>-</td>
</tr>
</tbody>
</table>

In this example, the primary boot disk is currently (source.2657). You want to activate the alternate boot disk (dest.2657).

2. Unmount any file systems that are mounted on the alternate root disk (dest.2657).

```bash
# lufslist dest.2657
```

```
boot environment name: dest.2657

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>fstype</th>
<th>device size</th>
<th>Mounted on</th>
<th>Mount Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/dsk/c0t0d0s1</td>
<td>swap</td>
<td>4298342400</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s0</td>
<td>ufs</td>
<td>15729328128</td>
<td>/</td>
<td>-</td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s5</td>
<td>ufs</td>
<td>8591474688</td>
<td>/var</td>
<td>-</td>
</tr>
<tr>
<td>/dev/dsk/c0t0d0s3</td>
<td>ufs</td>
<td>5371625472</td>
<td>/vxfs</td>
<td>-</td>
</tr>
</tbody>
</table>
```

```bash
# luumount dest.2657
```

3. Activate the Live Upgrade boot environment.

```bash
# luactivate dest.2657
```

4. Reboot the system.

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

When the system boots up, the GRUB menu displays the following entries for the Live Upgrade boot environments:

source.2657
dest.2657

The system automatically selects the boot environment entry that was activated.
To switch the boot environment if root disk is encapsulated

◆ If the root disk is encapsulated, for releases before Solaris 10 update 6 (2.10u6), you can use the `luactivate` method. For Solaris 10 update 6 and subsequent Solaris 10 updates, do one of the following:

■ Select the GRUB entry for the source boot environment or destination boot environment when the system is booted. You can also use the following procedure to manually set the default GRUB menu.lst entry to the source (PBE) or destination (ABE) grub entry:

■ If the system is booted from the alternate boot environment, perform the following steps to switch to the primary boot environment:

```
# mkdir /priroot
# mount rootpath /priroot
# bootadm list-menu -R /priroot
# bootadm list-menu
# bootadm set-menu -R /priroot default=PBE_menu_entry
# bootadm set-menu default=PBE_menu_entry
# shutdown -g0 -i6 -y
```

Where:
- `rootpath` is the path to the root device, such as
  `/dev/vx/dsk/rootdg/rootvol`
- `priroot` is the primary root device
- `PBE_menu_entry` is the number of the primary boot environment in the GRUB menu.

■ If the system is booted from the primary boot environment, perform the following steps to switch to the alternate boot environment:

```
# bootadm list-menu
# bootadm set-menu default=ABE_menu_entry
```

ABE booting
Performing post-upgrade tasks

This chapter includes the following topics:

■ Updating variables
■ Upgrading the Array Support Library
■ 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.

Upgrading the Array Support Library

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

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

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

1. Stop all applications, such as databases, from accessing VxVM volumes that are configured on the array, and unmount all VxFS file systems and checkpoints that are configured on the array.

2. Add the array as a JBOD of type A/P:

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

3. If you have not already done so, upgrade the Storage Foundation or VxVM software to 6.0. Device discovery will be performed during the upgrade, and the array will be claimed as a JBOD of appropriate type.

   If you have already upgraded your system to 6.0, run the following command to perform device discovery:

   ```bash
   # vxdctl enable
   ```

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

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

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

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

### Unsuppressing DMP for EMC PowerPath disks

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

In releases of VxVM before 4.1, a combination of DMP subpaths and the controllers of DMP subpaths were usually suppressed to prevent interference between DMP and the EMC PowerPath multi-pathing driver. Suppression has the effect of hiding these subpaths and their controllers from DMP, and as a result the disks on these subpaths and controllers cannot be seen by VxVM.
VxVM 4.1 and later releases have the ability to discover EMCpower disks, and configure them as autodiscovered disks that DMP recognizes are under the control of a separate multi-pathing driver. This has the benefit of allowing such disks to reconfigured in cluster-shareable disk groups. Before upgrading to VxVM 6.0, you must remove the suppression of the subpaths and controllers so that DMP can determine the association between EMCpower metadevices and disk devices.

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

■ Converting a foreign disk
  See “Converting a foreign disk to auto:simple” on page 91.

■ Converting a defined disk
  See “Converting a defined disk to auto:simple” on page 94.

■ Converting a powervxvm disk
  See “Converting a powervxvm disk to auto:simple” on page 97.

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

```bash
# powervxvm remove
```

Converting a foreign disk to auto:simple

Release 4.0 of VxVM provided the `vxddladm addforeign` command to configure foreign disks with default disk offsets for the private and public regions, and to define them as simple disks. A foreign disk must be manually converted to auto:simple format before upgrading to VxVM 6.0.

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

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

```bash
# vxdisk list

DEVICE      TYPE       DISK     GROUP  STATUS
    c6t0d12s2  auto:sliced       -   -   online
  emcpower10c    simple     fdisk    fdg   online

```

The `vxprint` command is used to display information about the disk group, `fdg`:
To convert a foreign disk to auto:simple format

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

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

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

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

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

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

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

   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/vtoc /dev/rdsk/emcpower10c
   ```
4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

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

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

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

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

5 Upgrade to VxVM 6.0 using the appropriate upgrade procedure.
6  After upgrading VxVM, use the `vxdisk list` command to validate the conversion to `auto:simple` format:

```bash
# vxdisk list

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>TYPE</th>
<th>DISK</th>
<th>GROUP</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>c6t0d12s2</td>
<td>auto:sliced</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>emcpower10s2</td>
<td>auto:simple</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>
...
```

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

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

7  Import the disk group and start the volumes:

```bash
# vxsg import fdg
# vxvol -g fdg startall
```

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

```bash
# vxdisk list

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>TYPE</th>
<th>DISK</th>
<th>GROUP</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>c6t0d12s2</td>
<td>auto:sliced</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>emcpower10s2</td>
<td>auto:simple</td>
<td>fdisk</td>
<td>fdg</td>
<td>online</td>
</tr>
</tbody>
</table>
```

### Converting a defined disk to `auto:simple`

In VxVM 4.0, and particularly in prior releases, EMCpower disks could be defined by a persistent disk access record (`darec`), and identified as simple disks. If an EMCpower disk is defined with a persistent `darec`, it must be manually converted to `auto:simple` format before upgrading to VxVM 6.0.

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

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

```bash
# ls -l /dev/vx/dmp/emcdisk1
lrwxrwxrwx 1 root other 36 Sep 24 17:59 /dev/vx/dmp/emcdisk1->
/dev/dsk/c6t0d11s5
# ls -l /dev/vx/rdmp/emcdisk1
```
Here the fifth partition of `/dev/vx/rdmp/emcdisk1` is defined as the persistent disk access record `emcdisk1`.

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

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

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

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

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

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

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

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

   ```
   # vxdisk rm emcdisk1
   ```

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

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

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

   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/hdisk /dev/rdsk/c6t0d11s2
   ```
4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

```bash
# /etc/vx/bin/vxedvtoc -f /tmp/hdisk /dev/rdsk/c6t0d1s2

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

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

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

5 Upgrade to VxVM 6.0 using the appropriate upgrade procedure.
6 After upgrading VxVM, use the `vxdisk list` command to validate the conversion to `auto:simple` format:

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

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

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

7 Import the disk group and start the volumes:

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

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

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

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

**Converting a powervxvm disk to auto:simple**

In VxVM 4.0, and particularly in prior releases, EMCpower disks could be defined by a persistent disk access record (darec) using powervxvm script, and identified as simple disks. If an EMCpower disk is used using powervxvm, it must be manually converted to auto:simple format before upgrading to VxVM 6.0.

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

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

Upgrading the Array Support Library

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

```
# vxdisk list
DEVICE   TYPE       DISK GROUP   STATUS
--------- -------- ---------------  -------
c6t0d12s2 auto:sliced   -   -    online
emcpower0c simple      pddsk01 ppdg     online
```

```
# vxprint
Disk group: fdg
TY NAME ASSOC KSTATE LENGTH PLOFFS STATE TUTIL0 PUTIL0
dg pddg  pddg - - - - - - - - -
dm pddsk01 emcpower0c - 2094960 - - - - - - - - -
```

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

1. Stop all the volumes in the disk group, and then deport it:
   ```
   # vxvol -g ppdg stopall
   # vxdg deport ppdg
   ```

2. Use the `vxdisk rm` command to remove all emcpower disks from VxVM:
   ```
   # vxdisk rm emcpower0c
   ```
   If you now run the `vxdisk list` command, the EMCPower disk is no longer displayed:
   ```
   # vxdisk list
   DEVICE   TYPE       DISK GROUP   STATUS
   --------- -------- ---------------  -------
c6t0d12s2 auto:sliced   -   -    online
   ```

3. Use the `vxprtvtoc` command to retrieve the partition table entry for this device:
   ```
   # /etc/vx/bin/vxprtvtoc -f /tmp/vtoc /dev/vx/rdmp/emcpower0c
   ```
4 Use the `vxedvtoc` command to modify the partition tag and update the VTOC:

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

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

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

5 Upgrade to VxVM 6.0 using the appropriate upgrade procedure.

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

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

7 Import the disk group and start the volumes.

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

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

Verifying the Veritas Dynamic Multi-Pathing upgrade

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

See “Verifying that the products were installed” on page 55.
Performing post-upgrade tasks
Verifying the Veritas Dynamic Multi-Pathing upgrade
Uninstallation of Veritas Dynamic Multi-Pathing

- Chapter 14. Uninstalling Veritas Dynamic Multi-Pathing
Uninstalling Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

- About removing Veritas Dynamic Multi-Pathing
- Preparing to uninstall
- Uninstalling Veritas Dynamic Multi-Pathing
- Uninstalling DMP with the Veritas Web-based installer
- Uninstalling Veritas Dynamic Multi-Pathing using the pkgrm command

About removing Veritas Dynamic Multi-Pathing

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

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

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

Preparing to uninstall

Review the following removing the Veritas software.
Remote uninstallation

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

The following prerequisites are required for remote uninstallation:

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

See “About configuring secure shell or remote shell communication modes before installing products” on page 137.

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 137.

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

3. Run the uninstallldmp command.

   # ./uninstallldmp

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

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

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

   If you respond yes, the processes are stopped and the packages are uninstalled.
6 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 a previous version of DMP.

To uninstall DMP

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

2 Start the Web-based installer.

   See “Starting the Veritas Web-based installer” on page 40.

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

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

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

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

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

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

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

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

Uninstalling Veritas Dynamic Multi-Pathing using the pkgrm command

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

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

To uninstall Veritas Dynamic Multi-Pathing

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

# umount /mount_point

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

2 Stop all applications from accessing VxVM volumes, and close all volumes.
3 Stop various daemons, if applicable.

# /opt/VRTS/bin/vxsvcctrl stop

4 Remove the packages in the following order:

For Veritas Dynamic Multi-Pathing:

# pkgrm VRTSsfcpi60 VRTSsfmh VRTSaslapm VRTSvxvm VRTSspt VRTSperl VRTSvlic
Uninstalling the language packages using the `pkgrm` command

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

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

To remove the language packages

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

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

Because the packages do not contain any dependencies, you can remove them in any order.
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 `installldmp` command usage takes the following form:

```
installldmp [ system1 system2... ]
[ -configure | -install | -license | -precheck
  | -requirements | -start | -stop | -uninstall
  | -upgrade | -postcheck ]
[ -logpath log_path ]
[ -responsefile response_file ]
[ -tmppath tmp_path ]
[ -hostfile hostfile_path ]
[ -jumpstart jumpstart_path ]
[ -keyfile ssh_key_file ]
[ -pkgpath pkg_path ]
[ -rootpath root_path ]
[ -rsh | -redirect | -installminpkgs | -installrecpkgs
  | -installallpkgs | -minpkgs | -recpkgs | -allpkgs
  | -listpatches | -pkgset | -copyinstallscripts
  | -pkginfo | -serial | -comcleanup | -makeresponsefile
  | -pkgtable | -ignorepatchreqs | -version | -nolic ]
```
Table A-1 lists the `installdmp` command options.

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--allpkgs</code></td>
<td>View a list of all DMP packages and patches. The installdmp lists the packages and patches in the correct installation order. You can use the output to create scripts for command-line installation, or for installations over a network. See the <code>--minpkgs</code> and the <code>--recpkgs</code> options.</td>
</tr>
<tr>
<td><code>--comcleanup</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>--configure</code></td>
<td>Configure DMP after using <code>--install</code> option to install DMP.</td>
</tr>
</tbody>
</table>
| `--copyinstallscripts` | 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. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `--rootpath` option. The following examples demonstrate the usage for this option:  

<table>
<thead>
<tr>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>./installer -copyinstallscripts</code></td>
<td><code>./install product_name -copyinstallscripts</code></td>
<td><code>./installer -rootpath alt_root_path -copyinstallscripts</code></td>
</tr>
<tr>
<td>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>.</td>
<td>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>.</td>
<td>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 UXRT51SP1.</td>
</tr>
<tr>
<td>Option and Syntax</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>-hostfile</td>
<td>Specifies the location of a file that contains the system names for the installer.</td>
<td></td>
</tr>
<tr>
<td>-ignorepatchreqs</td>
<td>The <code>-ignorepatchreqs</code> option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.</td>
<td></td>
</tr>
<tr>
<td>-install</td>
<td>Install product packages on systems without configuring DMP.</td>
<td></td>
</tr>
<tr>
<td>-installallpkgs</td>
<td>Selects all the packages for installation. See the <code>-allpkgs</code> option.</td>
<td></td>
</tr>
<tr>
<td>-installminpkgs</td>
<td>Selects the minimum packages for installation. See the <code>-minpkgs</code> option.</td>
<td></td>
</tr>
<tr>
<td>-installrecepkg</td>
<td>Selects the recommended packages for installation. See the <code>-recpkg</code> option.</td>
<td></td>
</tr>
<tr>
<td>-jumpstart <code>dir_path</code></td>
<td>Use this option to generate the finish scripts that the Solaris JumpStart Server can use for Veritas products. The <code>dir_path</code> indicates the path to an existing directory where the installer must store the finish scripts.</td>
<td></td>
</tr>
<tr>
<td>-keyfile <code>ssh key_file</code></td>
<td>Specifies a key file for SSH. The option passes <code>-i ssh_key_file</code> with each SSH invocation.</td>
<td></td>
</tr>
<tr>
<td>-license</td>
<td>Register or update product licenses on the specified systems. This option is useful to replace a demo license.</td>
<td></td>
</tr>
<tr>
<td>-listpatches</td>
<td>The <code>-listpatches</code> option displays product patches in correct installation order.</td>
<td></td>
</tr>
<tr>
<td>-logpath <code>log_path</code></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>-makeresponsefile</td>
<td>Create a response file. This option only generates a response file and does not install DMP.</td>
<td></td>
</tr>
</tbody>
</table>
Table A-1  installdmp options *(continued)*

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>-minpkgs</strong></td>
<td>View a list of the minimal packages and the patches that are required for DMP. The installdmp lists the packages and patches in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -recpkgs options.</td>
</tr>
<tr>
<td><strong>-nolic</strong></td>
<td>Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.</td>
</tr>
<tr>
<td><strong>-osversion</strong></td>
<td>View the list of packages and patches that apply to the specified Solaris version. Valid values are sol8, sol9, or sol10. Use this option with one of the following options: -allpkgs -minpkgs -recpkgs -jumpstart</td>
</tr>
<tr>
<td><strong>-patchpath patch_path</strong></td>
<td>Specifies that patch_path contains all patches that the installdmp is about to install on all systems. The patch_path is the complete path of a directory. <strong>Note</strong>: You can use this option when you download recent versions of patches.</td>
</tr>
<tr>
<td><strong>-pkginfo</strong></td>
<td>Displays a list of packages in the order of installation in a user-friendly format. Use this option with one of the following options: -allpkgs -minpkgs -recpkgs</td>
</tr>
<tr>
<td><strong>-pkgpath pkg_path</strong></td>
<td>Specifies that pkg_path contains all packages that the installdmp is about to install on all systems. The pkg_path is the complete path of a directory, usually NFS mounted.</td>
</tr>
<tr>
<td>Option and Syntax</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-pkgset</td>
<td>Discovers and lists the 6.0 packages installed on the systems that you specify.</td>
</tr>
<tr>
<td>-pkgtable</td>
<td>Displays the DMP 6.0 packages in the correct installation order.</td>
</tr>
<tr>
<td>-postcheck</td>
<td>Checks that the processes are running and other post-installation checks.</td>
</tr>
<tr>
<td>-precheck</td>
<td>Verify that systems meet the installation requirements before proceeding with DMP installation. Symantec recommends doing a precheck before you install DMP.</td>
</tr>
<tr>
<td>-recpkgs</td>
<td>View a list of the recommended packages and the patches that are required for DMP. The installdmp lists the packages and patches in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -minpkgs options.</td>
</tr>
<tr>
<td>-redirect</td>
<td>Specifies that the installer need not display the progress bar details during the installation.</td>
</tr>
<tr>
<td>-requirements</td>
<td>View a list of required operating system version, required patches, file system space, and other system requirements to install DMP.</td>
</tr>
<tr>
<td>-responsefile</td>
<td>Perform automated DMP installation using the system and the configuration information that is stored in a specified file instead of prompting for information. The response_file must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. See “Installing DMP using response files” on page 122. See “Upgrading DMP using response files” on page 122.</td>
</tr>
</tbody>
</table>
### Table A-1  
**installdmp options (continued)**

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>-rootpath</strong> root_path</td>
<td>Specifies that root_path is the root location for the installation of all packages. On Solaris, <code>-rootpath</code> passes <code>-R root_path</code> to <code>pkgadd</code> command.</td>
</tr>
<tr>
<td><strong>-rsh</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-serial</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>-start</strong></td>
<td>Starts the daemons and processes for DMP. If the <code>installdmp</code> failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -stop option. See “Starting and stopping processes for the Veritas products” on page 56.</td>
</tr>
<tr>
<td><strong>-stop</strong></td>
<td>Stops the daemons and processes for DMP. If the <code>installdmp</code> failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -start option. See “Starting and stopping processes for the Veritas products” on page 56.</td>
</tr>
<tr>
<td><strong>-tmppath</strong> tmp_path</td>
<td>Specifies that <code>tmp_path</code> is the working directory for <code>installdmp</code>. This path is different from the <code>/var/tmp</code> path. This destination is where the <code>installdmp</code> performs the initial logging and where the <code>installdmp</code> copies the packages on remote systems before installation.</td>
</tr>
<tr>
<td><strong>-upgrade</strong></td>
<td>Upgrades the installed packages on the systems that you specify.</td>
</tr>
</tbody>
</table>
Table A-1  installdmp options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-uninstall</td>
<td>Uninstalls DMP from the systems that you specify.</td>
</tr>
<tr>
<td>-version</td>
<td>Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.</td>
</tr>
</tbody>
</table>

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

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

Table A-2  uninstalldmp program options

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-comcleanup</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table A-2  uninstallldmp program options (continued)

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-copyinstallscripts</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Use this option to copy the installation scripts to an alternate rootpath when you use it with the -rootpath option.</td>
</tr>
<tr>
<td></td>
<td>The following examples demonstrate the usage for this option:</td>
</tr>
</tbody>
</table>
|                             | ■  ./installer -copyinstallscripts
|                             | Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/release_name. |
|                             | ■  ./installproduct_name -copyinstallscripts
|                             | Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/release_name. |
|                             | ■  ./installer -rootpath alt_root_path -copyinstallscripts
|                             | The path alt_root_path can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the release_name is UXRT51SP1. |
| -hostfile                   | Specifies the location of a file that contains the system names for the installer.                                                                                                                        |
| -keyfile ssh_key_file       | Specifies a key file for SSH. The option passes -i ssh_key_file with each SSH invocation.                                                                                                               |
| -logpath log_path           | Specifies that log_path, not /opt/VRTS/install/logs, is the location where uninstallldmp program log files, summary file, and response file are saved.                                                        |
| -makeresponsefile           | Use this option to create a response file or to verify that your system configuration is ready for uninstalling DMP.                                                                                       |
| -nolic                      | Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.                                              |
### Table A-2  uninstallldmp program options *(continued)*

<table>
<thead>
<tr>
<th>Option and Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-redirect</code></td>
<td>Displays progress details without showing progress bar.</td>
</tr>
</tbody>
</table>
| `-responsefile`   | Perform automated DMP uninstallation using the system and the configuration information that is stored in a specified file instead of prompting for information.  
The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.  
See “Uninstalling DMP using response files” on page 123. |
| `-rootpath root_path` | Specifies that *root_path* is the root location for uninstalling all packages.  
On Solaris, `-rootpath` passes `-R root_path` to pkgrm command. |
| `-rsh`            | Specifies that *rsh* and *rcp* are to be used for communication between systems instead of *ssh* and *scp*. This option requires that systems be preconfigured such that *rsh* commands between systems execute without prompting for passwords or confirmations. |
| `-serial`         | Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems. |
| `-tmppath tmp_path` | Specifies that *tmp_path* is the working directory for uninstallldmp program. This path is different from the /var/tmp path. This destination is where the uninstallldmp program performs the initial logging and where the instaldmp copies the packages on remote systems before installation. |
| `-version`        | Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. |
Installation scripts

Command options for uninstall script
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
   # ./installldmp -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/uninstallldmp -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:
Response file variable definitions

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG[opt][install]</td>
<td>Installs DMP packages. Configuration can be performed at a later time using the -configure option.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG[accepteula]</td>
<td>Specifies whether you agree with the EULA.pdf file on the media.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: required</td>
</tr>
<tr>
<td>$CFG[opt][vxkeyless]</td>
<td>Installs the product with keyless license.</td>
</tr>
<tr>
<td></td>
<td>List of scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG[systems]</td>
<td>List of systems on which the product is to be installed, uninstalled, or configured.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: list</td>
</tr>
<tr>
<td></td>
<td>Optional or required: required</td>
</tr>
<tr>
<td>CFG[prod]</td>
<td>Defines the product to be installed, uninstalled, or configured.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: required</td>
</tr>
<tr>
<td>CFG[opt][keyfile]</td>
<td>Defines the location of an ssh keyfile that is used to communicate with all remote systems.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CFG{opt}{patchpath}</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG{opt}{pkgpath}</td>
<td>Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG{opt}{tmppath}</td>
<td>Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG{opt}{rsh}</td>
<td>Defines that rsh must be used instead of ssh as the communication method between systems.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: scalar</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG{donotinstall} {package}</td>
<td>Instructs the installation to not install the optional packages in the list.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: list</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
<tr>
<td>CFG{donotremove} {package}</td>
<td>Instructs the uninstallation to not remove the optional packages in the list.</td>
</tr>
<tr>
<td></td>
<td>List or scalar: list</td>
</tr>
<tr>
<td></td>
<td>Optional or required: optional</td>
</tr>
</tbody>
</table>
### Table B-1  Response file variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| $CFG{vm_restore_cfg}{system1} | Indicates whether a previous VM configuration should be restored.  
0: indicates do not restore  
1: indicates do restore.  
List or scalar: Scalar  
Optional or required: optional |
| CFG[opt]{logpath} | Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.  
List or scalar: scalar  
Optional or required: optional |
| CFG[opt]{configure} | Performs the configuration after the packages are installed using the -install option.  
List or scalar: scalar  
Optional or required: optional |
| CFG[opt]{upgrade} | Upgrades all packages installed, without configuration.  
List or scalar: list  
Optional or required: optional |
| CFG[opt]{uninstall} | Uninstalls DMP packages.  
List or scalar: scalar  
Optional or required: optional |
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 128.

- 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 129.

■ 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 130.

See “About response files” on page 121.

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

See “Tunables value parameter definitions” on page 132.

## 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 132.

---

**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 131.

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.
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.

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 132.

---

**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 131.

2. Make sure the systems where you want to install DMP meet the installation requirements.

3. Complete any preinstallation tasks.

4. Copy the tunables file to one of the systems that you want to tune.

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

6. Start the installer with the `-settunables` option.

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

   Where `/tmp/tunables_file` is the full path name for the tunables file.
7 Proceed with the operation. When prompted, accept the tunable parameters. Certain tunables are only activated after a reboot. Review the output carefully to determine if the system requires a reboot to set the tunable value.

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

Setting tunables with an un-integrated response file

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

See “Tunables value parameter definitions” on page 132.

**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 131.

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.

   ```shell
   # ./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 132.

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:
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>
<thead>
<tr>
<th>Tunable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dmp_cache_open</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_daemon_count</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_delayq_interval</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_fast_recovery</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_health_time</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_log_level</td>
<td>(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.</td>
</tr>
<tr>
<td>Tunable</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>dmp_low_impact_probe</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_lun_retry_timeout</td>
<td>(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.</td>
</tr>
<tr>
<td>dmp_monitor_fabric</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_monitor_osevent</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_monitor_ownership</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_native_multipathing</td>
<td>(Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started.</td>
</tr>
<tr>
<td>dmp_native_support</td>
<td>(Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started.</td>
</tr>
<tr>
<td>dmp_path_age</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_pathswitch_blks_shift</td>
<td>(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.</td>
</tr>
<tr>
<td>Tunable</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dmp_probe_idle_lun</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_probe_threshold</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_restore_cycles</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_restore_interval</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_restore_policy</td>
<td>(Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.</td>
</tr>
<tr>
<td>dmp_restore_state</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_retry_count</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_scsi_timeout</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_sfg_threshold</td>
<td>(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.</td>
</tr>
<tr>
<td>dmp_stat_interval</td>
<td>(Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.</td>
</tr>
<tr>
<td>Tunable</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vx_era_nthreads</td>
<td>(Veritas File System) Maximum number of threads VxFS will detect read_ahead patterns on. This tunable requires system reboot to take effect.</td>
</tr>
<tr>
<td>vx_bc_bufhwm</td>
<td>(Veritas File System) VxFS metadata buffer cache high water mark. This tunable requires system reboot to take effect.</td>
</tr>
</tbody>
</table>
Tunable files for installation

Tunables value parameter definitions
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 and disabling rsh for Solaris

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.

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

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

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

   system1 # cd /

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

   system1 # ssh-keygen -t dsa

   System output similar to the following is displayed:

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

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

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

   Enter passphrase (empty for no passphrase):

   Do not enter a passphrase. Press Enter.

   Enter same passphrase again:

   Press Enter again.

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

   system2 # mkdir /.ssh

   Change the permissions of this directory, to secure it.

   system2 # chmod go-w /.ssh
To append the public key from the source system to the authorized_keys file on the target system, using secure file transfer

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

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

   PermitRootLogin yes
   Subsystem sftp /usr/lib/ssh/sftp-server

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

   To restart ssh on Solaris 10, type the following command:

   system1 # svcadm restart ssh

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

   Use the secure file transfer program.

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

   Use the following command for secure file transfer:

   system1 # sftp system2

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

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

4. Enter yes.

   Output similar to the following is displayed:

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

5. Enter the root password of system2.
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
```

To quit the SFTP session, type the following command:

```
sftp> quit
```

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:

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
```

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
```

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

```
system2 # exit
```
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
```

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

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

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

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

To verify that you can connect to a target system

1. On the source system (system1), enter the following command:

```
system1 # ssh -l root system2 uname -a
```

where system2 is the name of the target system.

2. The command should execute from the source system (system1) to the target system (system2) without the system requesting a passphrase or password.

3. Repeat this procedure for each target system.

**Restarting the ssh session**

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh
To restart ssh

1. On the source installation system (system1), bring the private key into the shell environment.

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

2. Make the key globally available for the user root.

   system1 # ssh-add

Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system. Veritas recommends configuring a secure shell environment for Veritas product installations.

See "Manually configuring and passwordless ssh" on page 138.

See the operating system documentation for more information on configuring remote shell.

To enable rsh

1. To determine the current status of rsh and rlogin, type the following command:

   # inetadm | grep -i login

   If the service is enabled, the following line is displayed:

   enabled online svc:/network/login:rlogin

   If the service is not enabled, the following line is displayed:

   disabled disabled svc:/network/login:rlogin

2. To enable a disabled rsh/rlogin service, type the following command:

   # inetadm -e rlogin

3. To disable an enabled rsh/rlogin service, type the following command:

   # inetadm -d rlogin
4 Modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. This file must be modified for each user who remotely accesses the system using rsh. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access `system1` from `system2`, you must add an entry for `system2.companyname.com` in the `.rhosts` file on `system1`.

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

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

```bash
# rm -f $HOME/.rhosts
```
Veritas Dynamic Multi-Pathing components

This appendix includes the following topics:

- Veritas Dynamic Multi-Pathing installation packages

Veritas Dynamic Multi-Pathing installation packages

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

<table>
<thead>
<tr>
<th>packages</th>
<th>Contents</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSaslapm</td>
<td>Veritas Array Support Library (ASL) and Array Policy Module (APM) binaries Required for the support and compatibility of various storage arrays.</td>
<td>Minimum</td>
</tr>
<tr>
<td>VRTSperl</td>
<td>Perl 5.10.0 for Veritas</td>
<td>Minimum</td>
</tr>
<tr>
<td>VRTSvlic</td>
<td>Veritas License Utilities Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.</td>
<td>Minimum</td>
</tr>
<tr>
<td>VRTSvxvm</td>
<td>Veritas Volume Manager binaries</td>
<td>Minimum</td>
</tr>
</tbody>
</table>
### Table E-1  Veritas Dynamic Multi-Pathing packages (continued)

<table>
<thead>
<tr>
<th>packages</th>
<th>Contents</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSsfcpip60</td>
<td>Veritas Storage Foundation Common Product Installer</td>
<td>Minimum</td>
</tr>
<tr>
<td></td>
<td>The Storage Foundation Common Product installer package contains the scripts that perform the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ upgrade</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ uninstallation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ adding nodes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ removing nodes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can use this script to simplify the native operating system installations, configurations, and upgrades.</td>
<td></td>
</tr>
<tr>
<td>VRTSsfmh</td>
<td>Veritas Storage Foundation Managed Host</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td>Discovers configuration information on a Storage Foundation managed host.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This information is stored on a central database, which is not part of this release. You must download the database separately at:</td>
<td></td>
</tr>
<tr>
<td>VRTSspt</td>
<td>Veritas Software Support Tools</td>
<td>Recommended</td>
</tr>
</tbody>
</table>
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 information
- Incorrect permissions for root on remote system
- 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),
- 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:

```bash
# /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 Information

The VRTSspt package provides a group of tools for troubleshooting a system and collecting information on its configuration. The tools can gather Veritas File System and Veritas Volume Manager metadata information and establish various benchmarks to measure file system and volume manager performance. Although the tools are not required for the operation of any Veritas product, Symantec recommends installing them should a support case be needed to be opened with Symantec Support. If you are unfamiliar with their use and purpose, use caution when using them or use them in concert with Symantec Support.

Incorrect permissions for root on remote system

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

Failed to setup rsh communication on 10.198.89.241: 'rsh 10.198.89.241 <command>' failed
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied

Failed to login to remote system(s) 10.198.89.241.
Please make sure the password(s) are correct and superuser(root) can login to the remote system(s) with the password(s).
If you want to setup rsh on remote system(s), please make sure rsh with command argument ('rsh <host> <command>') is not denied by remote system(s).

Either ssh or rsh is needed to be setup between the local node and 10.198.89.241 for communication

Would you like the installer to setup ssh/rsh communication automatically between the nodes?
Superuser passwords for the systems will be asked. [y,n,q] (y) n

System verification did not complete successfully

The following errors were discovered on the systems:

The ssh permission denied on 10.198.89.241
rsh exited 1 on 10.198.89.241
either ssh or rsh is needed to be setup between the local node and 10.198.89.241 for communication

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

See “About configuring secure shell or remote shell communication modes before installing products” on page 137.

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

Inaccessible system

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

Verifying systems: 12% ....................................
Estimated time remaining: 0:10 1 of 8
Checking system communication .............................. Done
System verification did not complete successfully
The following errors were discovered on the systems:
cannot resolve hostname host1
Enter the system names separated by spaces: q, ? (host1)

Suggested solution: Verify that you entered the system name correctly; use the ping(1M) command to verify the accessibility of the host.
Compatability issues when installing DMP with other products

This appendix includes the following topics:

- Installing, uninstalling, or upgrading Storage Foundation products when other Veritas products are present
- Installing, 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 packages as is.
- When uninstalling Storage Foundation products where SFM or VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where SFM or VOM Managed Host is present, the installer gives warning messages that it will upgrade VRTSsfmh.

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

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

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

C
configuring
  rsh 30
  ssh 30
creating
  Flash archive 49
  post-deployment scripts 50

F
flarcreate 49
Flash archive 49
  post-deployment scripts 50

I
installer program 36
Installing
  DMP with the Web-based installer 42
installing
  DMP 36, 104
  JumpStart 45

J
JumpStart
  installing 45

L
language packages
  removal 107
Live Upgrade
  preparing 77
  upgrade paths 75
  upgrading Solaris on alternate boot disk 79

M
mounting
  software disc 31

P
post-deployment scripts 50

preparing
  Live Upgrade 77

R
rsh
  configuration 30

S
ssh
  configuration 30

T
tunables file
  about setting parameters 127
  parameter definitions 132
  preparing 131
  setting for configuration 128
  setting for installation 128
  setting for upgrade 128
  setting parameters 131
  setting with no other operations 129
  setting with un-integrated response file 130

U
uninstallldmp command 104
upgrade paths
  Live Upgrade 75
using Live Upgrade 75

W
Web-based installer 42