Veritas™ Dynamic Multi-Pathing Installation Guide

Solaris

6.0 Platform Release 1

March 2012

Veritas Dynamic Multi-Pathing Installation Guide

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

Product version: 6.0 PR1

Document version: 6.0PR1.0

Legal Notice

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

Contents

Section 1

Installation overview and planning

Chapter 1

Introducing Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

About Veritas Dynamic Multi-Pathing

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.

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: 6.0PR1.0.

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

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

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

About installation and configuration methods

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.
  See "About the Veritas installer" on page 33.
- 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.
- 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 61.

Chapter 3

System requirements

This chapter includes the following topics:

Release notes

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

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

https://sort.symantec.com/documents

Hardware compatibility list (HCL)

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

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

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

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

Supported operating systems

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

Disk space requirements

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

Use the script-based installer `-precheck` option to determine if there is sufficient space.

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

If you have downloaded DMP, 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
   ```

Chapter 4

Licensing Veritas products

This chapter includes the following topics:

About Veritas product licensing

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

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

www.symantec.com/techsupp/

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

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

Within 60 days of choosing this option, you must install a valid license key corresponding to the license level entitled 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 22.
  See the `vxkeyless(1m)` manual page.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
  See "Installing Veritas product license keys" on page 24.
  See the `vxlicinst(1m)` manual page.

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

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

Setting or changing the 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
```

Section 2

Installation of Veritas Dynamic Multi-Pathing

Preparing to install Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

Installation preparation overview

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

Table 5-1 Installation overview

Installation task	Section
Obtain product licenses.	See "About Veritas product licensing" on page 21.
Download the software, or insert the product DVD.	See "Mounting the product disc" on page 30.
Create root user.	See "Creating root user" on page 28.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Set environment variables.	See "Setting environment variables" on page 29.
Create the `/opt` directory, if it does not exist.	See "Creating the /opt directory" on page 30.
Configure the secure shell (ssh) on all nodes.	See "About configuring secure shell or remote shell communication modes before installing products" on page 77.
Verify that hardware, software, and operating system requirements are met.	See "Release notes" on page 17.
Check that sufficient disk space is available.	See "Disk space requirements" on page 18.
Use the installer to install the products.	See "About the Veritas installer" on page 33.

Creating root user

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

To change root role into a user

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

```
% su  - root
```

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

```
# roles admin

root

# usermod -R " " admin
```

3 Change the root role into a user.

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

4 Verify the change.

- `# getent user_attr root`

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

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

- `# userattr type root`

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

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

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

See "Changing root user into root role" on page 37.

Setting environment variables

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

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

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

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

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

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

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

About using ssh or rsh with the Veritas installer

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

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

- When you 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 77.

Creating the /opt directory

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

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

Mounting the product disc

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

To mount the product disc

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

   The systems must be in the same subnet.

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

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

   Where c0t6d0s2 is the default address for the disc drive.

Assessing the system for installation readiness

Symantec provides the following tool for assessing your system, to ensure that the system meets the requirements for installing Veritas Dynamic Multi-Pathing 6.0 PR1.

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 31.

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

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

This chapter includes the following topics:

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.
- Use `q` to quit the installer.
- Use `?` to display help information.
- Use the Enter button to accept a default response.

Installing Veritas Dynamic Multi-Pathing

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

The following sample procedure installs DMP on a single system.

To install DMP

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

2 Load and mount the software disc.

See "Mounting the product disc" on page 30.

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

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

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

```
# ./installer
```

5 Enter `I` to install and press the Return key.

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

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

8 Select one of the following installation options:

- A minimal installation installs packages for minimal functionality for the selected product.
- A recommended installation installs the recommended DMP packages that provide complete functionality of the product.

Note that this option is the default.

- The display selection displays all packages and provides information about them. Note that the recommended installation installs the minimum and the recommended packages.

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

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

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

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

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

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

To install through keyless licensing, select 2.

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

For more information, go to the following Web site:

http://go.symantec.com/sfhakeyless

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

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

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

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

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

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

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

Installing language packages

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

To install the language packages on the server

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

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

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

Performing a postcheck on a node

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

Note: This command option requires downtime for the system.

To run the postcheck command on a node

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

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

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

Changing root user into root role

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

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

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

   ```
   # getent user_attr root
   ```

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

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

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

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

Section 3

Verification of the installation

Chapter 7

Verifying the Veritas Dynamic Multi-Pathing installation

This chapter includes the following topics:

Verifying that the products were installed

Verify that the DMP products are installed.

Use the pkg info command to check which packages have been installed.

```
# pkg info -l VRTSvlic package_name package_name ...
```

See “Veritas Dynamic Multi-Pathing installation packages” on page 85.

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:

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

To start the processes

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

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

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

Section 4

Uninstallation of Veritas Dynamic Multi-Pathing

Chapter 8

Uninstalling Veritas Dynamic Multi-Pathing

This chapter includes the following topics:

About removing Veritas Dynamic Multi-Pathing

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

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

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

Preparing to uninstall

Review the following removing the Veritas software.

Remote uninstallation

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

The following prerequisites are required for remote uninstallation:

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

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.
2. On the system where you plan to remove DMP, move to the /opt/VRTS/install directory.
3. Run the `uninstalldmp` command.

   ```
   # ./uninstalldmp
   ```

4. When the installer prompts you, enter the names of each system where you want to uninstall DMP. Separate system names with spaces.
5. The installer program checks the systems. It then asks you if you want to stop DMP processes.

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

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

Section 5

Installation reference

Appendix A

Installation scripts

This appendix includes the following topics:

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

Command options for the installation script

The `installdmp` command usage takes the following form:

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

 [ -jumpstart jumpstart_path ]

 [ -keyfile ssh_key_file ]

 [ -pkgpath pkg_path ]

 [ -rootpath root_path ]

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

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

Table A-1 installdmp options

Option and Syntax	Description
`-allpkgs`	View a list of all DMP packages and patches. The installdmp lists the packages and patches in the correct installation order. You can use the output to create scripts for command-line installation, or for installations over a network. See the -minpkgs and the -recpkgs options.
`-comcleanup`	The `-comcleanup` option removes the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.
`-configure`	Configure DMP after using `-install` option to install DMP.
`-copyinstallscripts`	Use this option when you manually install products and want to use the intallation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./installer -rootpath` *`alt_root_path`* `-copyinstallscripts` The path *alt_root_path* can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the *release_name* is UXRT51SP1.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-hostfile`	Specifies the location of a file that contains the system names for the installer.
`-ignorepatchreqs`	The `-ignorepatchreqs` option is used to allow installation or upgrading even if the prerequisite packages or patches are missed on the system.
`-install`	Install product packages on systems without configuring DMP.
`-installallpkgs`	Selects all the packages for installation. See the `-allpkgs` option.
`-installminpkgs`	Selects the minimum packages for installation. See the `-minpkgs` option.
`-installrecpkgs`	Selects the recommended packages for installation. See the `-recpkgs` option.
`-jumpstart` *`dir_path`*	Use this option to generate the finish scripts that the Solaris JumpStart Server can use for Veritas products. The *dir_path* indicates the path to an existing directory where the installer must store the finish scripts.
`-keyfile` *`ssh_key_file`*	Specifies a key file for SSH. The option passes `-i` *`ssh_key_file`* with each SSH invocation.
`-license`	Register or update product licenses on the specified systems. This option is useful to replace a demo license.
`-listpatches`	The `-listpatches` option displays product patches in correct installation order.
`-logpath` *`log_path`*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where install log files, summary files, and response files are saved.
`-makeresponsefile`	Create a response file. This option only generates a response file and does not install DMP.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-minpkgs`	View a list of the minimal packages and the patches that are required for DMP. The installdmp lists the packages and patches in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -recpkgs options.
`-nolic`	Allows installation of product packages without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
`-osversion`	View the list of packages and patches that apply to the specified Solaris version. Valid values are `sol8`, `sol9`, or `sol10`. Use this option with one of the following options: ■ -allpkgs ■ -minpkgs ■ -recpkgs ■ -jumpstart
`-patchpath` *`patch_path`*	Specifies that *patch_path* contains all patches that the installdmp is about to install on all systems. The *patch_path* is the complete path of a directory. **Note:** You can use this option when you download recent versions of patches.
`-pkg info`	Displays a list of packages in the order of installation in a user-friendly format. Use this option with one of the following options: ■ -allpkgs If you do not specify an option, -allpkgs is used by default. ■ -minpkgs ■ -recpkgs
`-pkgpath` *`pkg_path`*	Specifies that *pkg_path* contains all packages that the installdmp is about to install on all systems. The *pkg_path* is the complete path of a directory, usually NFS mounted.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-pkgset`	Discovers and lists the 6.0 PR1 packages installed on the systems that you specify.
`-pkgtable`	Displays the DMP 6.0 PR1 packages in the correct installation order.
`-postcheck`	Checks that the processes are running and other post-installation checks.
`-precheck`	Verify that systems meet the installation requirements before proceeding with DMP installation. Symantec recommends doing a precheck before you install DMP.
`-recpkgs`	View a list of the recommended packages and the patches that are required for DMP. The installdmp lists the packages and patches in the correct installation order. The list does not include the optional packages. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -minpkgs options.
`-redirect`	Specifies that the installer need not display the progress bar details during the installation.
`-requirements`	View a list of required operating system version, required patches, file system space, and other system requirements to install DMP.
`-responsefile` *`response_file`*	Perform automated DMP installation using the system and the configuration information that is stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. See "Installing DMP using response files" on page 61.
`-rootpath` *`root_path`*	Specifies that root_path is the root location for the installation of all packages. On Solaris, `-rootpath` passes `-R` *`root_path`* to pkgadd command.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-rsh`	Specifies that *rsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *rsh* commands between systems execute without prompting for passwords or confirmations
`-serial`	Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.
`-start`	Starts the daemons and processes for DMP. If the installdmp failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -stop option. See "Starting and stopping processes for the Veritas products " on page 42.
`-stop`	Stops the daemons and processes for DMP. If the installdmp failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -start option. See "Starting and stopping processes for the Veritas products " on page 42.
`-tmppath` *`tmp_path`*	Specifies that *tmp_path* is the working directory for installdmp. This path is different from the /var/tmp path. This destination is where the installdmp performs the initial logging and where the installdmp copies the packages on remote systems before installation.
`-upgrade`	Upgrades the installed packages on the systems that you specify.
`-uninstall`	Uninstalls DMP from the systems that you specify.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-version`	Checks and reports the installed products and their versions. Identifies the installed and missing packages and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing packages and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.

Command options for uninstall script

The `uninstalldmp 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

Option and Syntax	Description
`-comcleanup`	The `-comcleanup` option removes the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.

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

Option and Syntax	Description
`-copyinstallscripts`	Use this option when you manually install products and want to use the intallation scripts that are stored on the system to perform product configuration, uninstallation, and licensing tasks without the product media. Use this option to copy the installation scripts to an alternate rootpath when you use it with the `-rootpath` option. The following examples demonstrate the usage for this option: ■ `./installer -copyinstallscripts` Copies the installation and uninstallation scripts for all products in the release to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./install`*`product_name`* `-copyinstallscripts` Copies the installation and uninstallation scripts for the specified product and any subset products for the product to /opt/VRTS/install. It also copies the installation Perl libraries to /opt/VRTSperl/lib/site_perl/*release_name* . ■ `./installer -rootpath` *`alt_root_path`* `-copyinstallscripts` The path *alt_root_path* can be a directory like /rdisk2. In that case, this command copies installation and uninstallation scripts for all the products in the release to /rdisk2/opt/VRTS/install. CPI perl libraries are copied at /rdisk2/opt/VRTSperl/lib/site_perl/release_name. For example, for the 5.1 SP1 the *release_name* is UXRT51SP1.
`-hostfile`	Specifies the location of a file that contains the system names for the installer.
`-keyfile` *`ssh_key_file`*	Specifies a key file for SSH. The option passes `-i` *`ssh_key_file`* with each SSH invocation.
`-logpath` *`log_path`*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where uninstalldmp program log files, summary file, and response file are saved.
`-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 uninstalldmp program options *(continued)*

Option and Syntax	Description
`-redirect`	Displays progress details without showing progress bar.
`-responsefile` *`response_file`*	Perform automated DMP uninstallation using the system and the configuration information that is stored in a specified file instead of prompting for information. The *response_file* must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file. See "Uninstalling DMP using response files" on page 62.
`-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 uninstalldmp program. This path is different from the /var/tmp path. This destination is where the uninstalldmp program performs the initial logging and where the installdmp copies the 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.

Appendix B

Response files

This appendix includes the following topics:

About response files

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

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

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

Installing DMP using response files

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

To install DMP using response files

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

2. Make sure the preinstallation tasks are completed.

3. Copy the response file to the system where you want to install DMP.

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

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

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

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

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

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

Uninstalling DMP using response files

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

To perform an automated uninstallation

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

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

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

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

   ```
   # /opt/VRTS/install/uninstalldmp -responsefile /tmp/response_file
   ```

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

Syntax in the response file

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

For example, in the case of a string value:

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

or, in the case of an integer value:

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

or, in the case of a list:

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

Response file variable definitions

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

Table B-1 Response file variables

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

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

Variable	Description
CFG{prod}	Defines the product to be installed, uninstalled, or configured. List or scalar: scalar Optional or required: required
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{patchpath}	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{pkgpath}	Defines a location, typically an NFS mount, from which all remote systems can install product packages. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the packages that are needed during the install. The default location is /var/tmp. List or scalar: scalar Optional or required: optional
CFG{opt}{rsh}	Defines that *rsh* must be used instead of ssh as the communication method between systems. List or scalar: scalar Optional or required: optional
CFG{donotinstall} {package}	Instructs the installation to not install the optional packages in the list. List or scalar: list Optional or required: optional

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

Variable	Description
CFG{donotremove} {package}	Instructs the uninstallation to not remove the optional packages in the list. List or scalar: list Optional or required: optional
$CFG{vm_restore_cfg}{system1}	Indicates whether a previous VM configuration should be restored. 0: indicates do not restore 1: indicates do restore. List or scalar: Scalar Optional or required: optional
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

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 68.

- 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 69.

- 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 70.

See “About response files” on page 61.

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

See “Tunables value parameter definitions” on page 72.

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 72.

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 71.

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

3. Complete any preinstallation tasks.

4. Copy the tunables file to one of the systems where you want to install, configure, or upgrade the product.

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

6. Start the installer for the installation, configuration, or upgrade. For example:

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

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

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

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

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

Setting tunables with no other installer-related operations

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

See "Tunables value parameter definitions" on page 72.

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 71.

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 72.

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 71.

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

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

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

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

Where *response_file_name* is the full path name for the response file and *tunables_file_name* is the full path name for the tunables file.

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

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

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

Preparing the tunables file

A tunables file is a Perl module and consists of an opening and closing statement, with the tunables defined between. Use the hash symbol at the beginning of the line to comment out the line. The tunables file opens with the line "our %TUN;" and ends with the return true "1;" line. The final return true line only needs to appear once at the end of the file. Define each tunable parameter on its own line.

Format the tunable parameter as follows:

```
$TUN{"tunable_name"}{"system_name"|"*"}=value_of_tunable;
```

For the *system_name*, use the name of the system, its IP address, or a wildcard symbol. The *value_of_tunable* depends on the type of tunable you are setting. End the line with a semicolon.

The following is an example of a tunables file.

```
#
# Tunable Parameter Values:
#
our %TUN;

$TUN{"tunable1"}{"*"}=1024;
$TUN{"tunable3"}{"sys123"}="SHA256";

1;
```

Setting parameters for the tunables file

Each tunables file defines different tunable parameters. The values that you can use are listed in the description of each parameter. Select the tunables that you want to add to the tunables file and then configure each parameter.

See "Tunables value parameter definitions" on page 72.

Each line for the parameter value starts with $TUN. The name of the tunable is in curly brackets and double-quotes. The system name is enclosed in curly brackets and double-quotes. Finally define the value and end the line with a semicolon, for example:

```
$TUN{"dmp_daemon_count"}{"node123"}=16;
```

In this example, you are changing the dmp_daemon_count value from its default of 10 to 16. You can use the wildcard symbol "*" for all systems. For example:

```
$TUN{"dmp_daemon_count"}{"*"}=16;
```

Tunables value parameter definitions

When you create a tunables file for the installer you can only use the parameters in the following list.

Prior to making any updates to the tunables, refer to the *Veritas Storage Foundation and High Availability Solutions Tuning Guide* for detailed information on product tunable ranges and recommendations .

Table C-1 describes the supported tunable parameters that can be specified in a tunables file.

Table C-1 Supported tunable parameters

Tunable	Description
dmp_cache_open	(Veritas Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_daemon_count	(Veritas Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_delayq_interval	(Veritas Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_fast_recovery	(Veritas Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_health_time	(Veritas Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_log_level	(Veritas Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

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

Tunable	Description
dmp_low_impact_probe	(Veritas Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_lun_retry_timeout	(Veritas Dynamic Multi-Pathing) The retry period for handling transient errors. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_fabric	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Veritas Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_monitor_ownership	(Veritas Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_multipathing	(Veritas Dynamic Multi-Pathing) Whether DMP will intercept the I/Os directly on the raw OS paths or not. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_native_support	(Veritas Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_path_age	(Veritas Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_pathswitch_blks_shift	(Veritas Dynamic Multi-Pathing) The default number of contiguous I/O blocks sent along a DMP path to an array before switching to the next available path. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

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

Tunable	Description
dmp_probe_idle_lun	(Veritas Dynamic Multi-Pathing) Whether the path restoration kernel thread probes idle LUNs. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_probe_threshold	(Veritas Dynamic Multi-Pathing) The number of paths will be probed by the restore daemon. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_cycles	(Veritas Dynamic Multi-Pathing) The number of cycles between running the check_all policy when the restore policy is check_periodic. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_interval	(Veritas Dynamic Multi-Pathing) The time interval in seconds the restore daemon analyzes the condition of paths. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_policy	(Veritas Dynamic Multi-Pathing) The policy used by DMP path restoration thread. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_restore_state	(Veritas Dynamic Multi-Pathing) Whether kernel thread for DMP path restoration is started. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_retry_count	(Veritas Dynamic Multi-Pathing) The number of times a path reports a path busy error consecutively before DMP marks the path as failed. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_scsi_timeout	(Veritas Dynamic Multi-Pathing) The timeout value for any SCSI command sent via DMP. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_sfg_threshold	(Veritas Dynamic Multi-Pathing) The status of the subpaths failover group (SFG) feature. This tunable must be set after Veritas Dynamic Multi-Pathing is started.
dmp_stat_interval	(Veritas Dynamic Multi-Pathing) The time interval between gathering DMP statistics. This tunable must be set after Veritas Dynamic Multi-Pathing is started.

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

Tunable	Description
vx_era_nthreads	(Veritas File System) Maximum number of threads VxFS will detect read_ahead patterns on. This tunable requires system reboot to take effect.
vx_bc_bufhwm	(Veritas File System) VxFS metadata buffer cache high water mark. This tunable requires system reboot to take effect.

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

About configuring secure shell or remote shell communication modes before installing products

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.

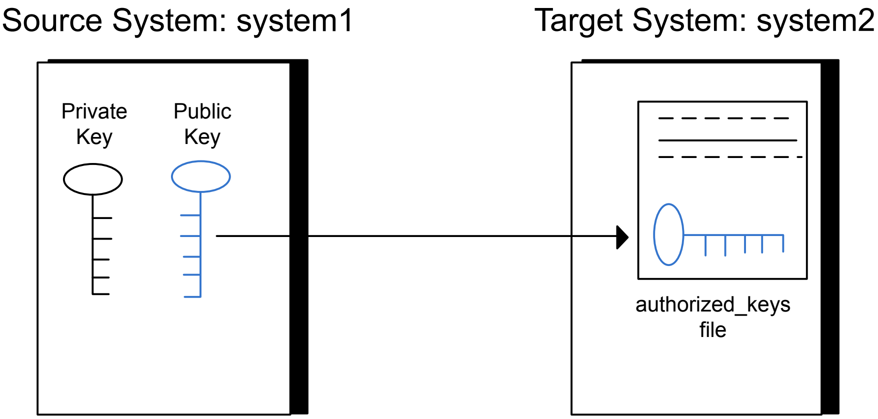
Manually configuring and passwordless ssh

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

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

Figure D-1 illustrates this procedure.

Figure D-1 Creating the DSA key pair and appending it to target systems



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

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

To create the DSA key pair

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

   ```
   system1 # cd /
   ```

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

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

   System output similar to the following is displayed:

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

3. Press Enter to accept the default location of `/.ssh/id_dsa`.
4. When the program asks you to enter the passphrase, press the Enter key twice.

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

   Do not enter a passphrase. Press Enter.

   ```
   Enter same passphrase again:
   ```

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

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

   Change the permissions of this directory, to secure it.

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

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

1 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.

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

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

The following output is displayed:

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

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

```
sftp> quit
```

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

```
system1 # ssh system2
```

Enter the root password of system2 at the prompt:

```
password:
```

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

```
system2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

10 After the `id_dsa.pub` public key file is copied to the target system (system2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, enter the following command on system2:

```
system2 # rm /id_dsa.pub
```

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

```
system2 # exit
```

12 When you install from a source system that is also an installation target, also add the local system `id_dsa.pub` key to the local `authorized_keys` file. The installation can fail if the installation source system is not authenticated.

To add the local system `id_dsa.pub` key to the local `authorized_keys` file, enter the following command:

```
system1 # cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys
```

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

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

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

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

To verify that you can connect to a target system

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

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

where system2 is the name of the target system.

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

3 Repeat this procedure for each target system.

Restarting the ssh session

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

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

To restart ssh

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

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

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

   ```
   system1 # ssh-add
   ```

Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system.

Veritas recommends configuring a secure shell environment for Veritas product installations.

See “Manually configuring and passwordless ssh” on page 78.

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

To enable rsh

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

   ```
   # inetadm | grep -i login
   ```

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

   ```
   enabled online svc:/network/login:rlogin
   ```

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

   ```
   disabled disabled svc:/network/login:rlogin
   ```

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

   ```
   # inetadm -e rlogin
   ```

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

   ```
   # inetadm -d rlogin
   ```

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

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

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

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

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 E-1 Veritas Dynamic Multi-Pathing packages

packages	Contents	Configuration
VRTSaslapm	Veritas Array Support Library (ASL) and Array Policy Module(APM) binaries Required for the support and compatibility of various storage arrays.	Minimum
VRTSperl	Perl 5.10.0 for Veritas	Minimum
VRTSvlic	Veritas License Utilities Installs the license key layout files required to decode the Storage Foundation license keys. Provides the standard license key utilities vxlicrep, vxlicinst, and vxlictest.	Minimum
VRTSvxvm	Veritas Volume Manager binaries	Minimum

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

packages	Contents	Configuration
VRTSsfcpi60	Veritas Storage Foundation Common Product Installer The Storage Foundation Common Product installer package contains the scripts that perform the following: ■ installation ■ configuration ■ upgrade ■ uninstallation ■ adding nodes ■ removing nodes ■ etc. You can use this script to simplify the native operating system installations, configurations, and upgrades.	Minimum
VRTSsfmh	Veritas Storage Foundation Managed Host Discovers configuration information on a Storage Foundation managed host. This information is stored on a central database, which is not part of this release. You must download the database separately at: http://www.symantec.com/business/storage-foundation-manager	Recommended
VRTSspt	Veritas Software Support Tools	Recommended

Appendix F

Troubleshooting installation issues

This appendix includes the following topics:

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

What to do if you see a licensing reminder

In this release, you can install without a license key. In order to comply with the End User License Agreement, you must either install a license key or make the host managed by a Management Server. If you do not comply with these terms within 60 days, the following warning messages result:

```
WARNING V-365-1-1 This host is not entitled to run Veritas Storage
Foundation/Veritas Cluster Server.As set forth in the End User
```

```
License Agreement (EULA) you must complete one of the two options
set forth below. To comply with this condition of the EULA and
stop logging of this message, you have <nn> days to either:
- make this host managed by a Management Server (see
  http://go.symantec.com/sfhakeyless for details and free download),
  or
- add a valid license key matching the functionality in use on this host
  using the command 'vxlicinst'
```

To comply with the terms of the EULA, and remove these messages, you must do one of the following within 60 days:

- Install a valid license key corresponding to the functionality in use on the host.
  After you install the license key, you must validate the license key using the following command:

  ```
  # /opt/VRTS/bin/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`.

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

Inaccessible system

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

```
 Verifying systems: 12% ....................................
 Estimated time remaining: 0:10 1 of 8
 Checking system communication ............................. Done
System verification did not complete successfully
```

```
The following errors were discovered on the systems:
cannot resolve hostname host1
Enter the  system names separated by spaces: q,? (host1)
```

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

Appendix G

Compatability issues when installing DMP with other products

This appendix includes the following topics:

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