Symantec™ Dynamic Multi-Pathing Installation Guide

AIX

6.2

August 2014

Symantec

Symantec™ 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: 6.2

Document version: 6.2 Rev 0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on

page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Support agreement resources

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

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

Contents

Technical Support 4

Section 1 Installation overview and planning 13

Chapter 1 Introducing Symantec Dynamic Multi-Pathing 14

About Symantec Dynamic Multi-Pathing (DMP) 14
About Veritas Operations Manager 15
About Symantec Operations Readiness Tools 15

Chapter 2 System requirements 18

Release notes 18
Important preinstallation information for DMP 18
Supported operating systems 19
Disk space requirements 19
Virtual I/O Server (VIOS) requirements 19
Checking installed product versions and downloading maintenance releases and patches 20
Obtaining installer patches 21
Disabling external network connection attempts 22

Chapter 3 Planning to install DMP 23

About planning for DMP installation 23
About installation and configuration methods 23

Chapter 4 Licensing DMP 26

About Symantec product licensing 26
Setting or changing the product level for keyless licensing 27
Installing Symantec product license keys 29

Section 2 Installation of DMP 31

Chapter 5 Preparing to install DMP 32

Installation preparation overview 32
Setting environment variables 33
About using ssh or rsh with the installer 33
Mounting the product disc 34
Assessing the system for installation readiness 35
Prechecking your systems using the installer 36

Chapter 6 Installing DMP using the script-based installer 37

About the script-based installer 37
Installing DMP using the script-based installer 39
Performing a postcheck on a node 42

Chapter 7 Installing DMP using the web-based installer 43

About the web-based installer 43
Before using the web-based installer 44
Starting the web-based installer 44
Obtaining a security exception on Mozilla Firefox 45
Performing a preinstallation check with the web-based installer 46
Installing DMP with the web-based installer 46

Chapter 8 Automated installation using response files 49

About response files 49
Installing DMP using response files 50
Upgrading DMP using response files 50
Uninstalling DMP using response files 51
Syntax in the response file 51
Response file variable definitions 52

Chapter 9 Installing DMP using operating system-specific methods 55

About installing DMP using operating system-specific methods 55
Installing DMP using NIM and the installer 56
Preparing the installation bundle on the NIM server 56
Installing DMP on the NIM client using SMIT on the NIM server 57

Installing DMP and the operating system on the NIM client using SMIT 58
Installing Symantec Dynamic Multi-Pathing using the mksysb utility 58
Creating the mksysb backup image 59
Installing mksysb image on alternate disk 60
Verifying the installation 62

Section 3 Managing your Symantec deployments 63

Chapter 10 Performing centralized installations using the Deployment Server 64

About the Deployment Server 65
Deployment Server overview 66
Installing the Deployment Server 67
Setting up a Deployment Server 68
Setting deployment preferences 71
Specifying a non-default repository location 73
Downloading the most recent release information 73
Loading release information and patches on to your Deployment Server 74
Viewing or downloading available release images 75
Viewing or removing repository images stored in your repository 79
Deploying Symantec product updates to your environment 82
Finding out which releases you have installed, and which upgrades or updates you may need 83
Defining Install Bundles 84
Creating Install Templates 90
Deploying Symantec releases 92
Connecting the Deployment Server to SORT using a proxy server 95

Section 4 Post-installation tasks 97

Chapter 11 Verifying the DMP installation 98

Verifying that the products were installed 98
Installation log files 99
Starting and stopping processes for the Symantec products 99

Section 5 Upgrade of DMP 101

Chapter 12 Planning to upgrade DMP 102

Upgrade methods for DMP 102
Supported upgrade paths for DMP 103
Preparing to upgrade DMP 104
Getting ready for the upgrade 104
Preparing for an upgrade of Symantec Dynamic Multi-Pathing 105
Creating backups 106
Upgrading the array support 106
Using Install Bundles to simultaneously install or upgrade base releases, maintenance releases, and patches 107

Chapter 13 Upgrading DMP 110

Upgrading Symantec Dynamic Multi-Pathing with the product installer 110
Upgrading DMP using the web-based installer 111
Upgrade Symantec Dynamic Multi-Pathing and AIX on a DMP-enabled rootvg 113
Upgrading from DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.2 on a DMP-enabled rootvg 113
Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.2 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg 114
Upgrading DMP on a Virtual I/O server (VIOS) from 5.1SP1 or later to 6.2 115
Upgrading the AIX operating system 116

Chapter 14 Upgrading DMP using an alternate disk 117

About upgrading DMP using an alternate disk 117
Supported upgrade scenarios 118
Supported upgrade paths for DMP using alternate disks 118
Preparing to upgrade DMP on an alternate disk 118
Upgrading DMP on an alternate disk 120
Verifying the upgrade 121

Chapter 15 Upgrading DMP using Network Install Manager Alternate Disk Migration 123

Supported upgrade paths for DMP using NIM ADM 123
Preparing to upgrade DMP and the operating system using the `nimadm` utility 124
Preparing the installation bundle on the NIM server 124
Upgrading DMP and the operating system using the `nimadm` utility 125
Verifying the upgrade performed using the NIM ADM utility 127

Chapter 16 Performing post-upgrade tasks 129

Updating variables 129
Verifying the Symantec Dynamic Multi-Pathing upgrade 129

Section 6 Uninstallation of DMP 130

Chapter 17 Uninstalling DMP 131

Uninstalling DMP 131
Uninstalling DMP with the web-based installer 132
Removing Storage Foundation products using SMIT 133

Section 7 Installation reference 136

Appendix A Installation scripts 137

Command options for the installation script 137
Command options for uninstall script 142

Appendix B Tunable files for installation 146

About setting tunable parameters using the installer or a response file 146
Setting tunables for an installation, configuration, or upgrade 147
Setting tunables with no other installer-related operations 148
Setting tunables with an un-integrated response file 149
Preparing the tunables file 150
Setting parameters for the tunables file 150
Tunables value parameter definitions 151

Appendix C Configuring the secure shell or the remote shell for communications 155

About configuring secure shell or remote shell communication modes before installing products 155
Manually configuring and passwordless ssh 156
Restarting the ssh session 160
Enabling rsh for AIX 160

Appendix D DMP components 162

Symantec Dynamic Multi-Pathing installation filesets 162

Appendix E Troubleshooting installation issues 164

Restarting the installer after a failed connection 164
What to do if you see a licensing reminder 164
Troubleshooting an installation on AIX 165
Incorrect permissions for root on remote system 165
Resource temporarily unavailable 166
Inaccessible system 167

Appendix F Compatibility issues when installing DMP with other products 168

Installing, uninstalling, or upgrading Storage Foundation products when other Symantec products are present 168
Installing, uninstalling, or upgrading Storage Foundation products when VOM is already present 169
Installing, uninstalling, or upgrading Storage Foundation products when NetBackup is already present 169

Index 170

Section 1

Installation overview and planning

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

Chapter 1

Introducing Symantec Dynamic Multi-Pathing

This chapter includes the following topics:

- About Symantec Dynamic Multi-Pathing (DMP)
- About Veritas Operations Manager
- About Symantec Operations Readiness Tools

About Symantec Dynamic Multi-Pathing (DMP)

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

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

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

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

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

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

About Veritas Operations Manager

Veritas Operations Manager provides a centralized management console for Symantec Storage Foundation and High Availability products. You can use Veritas Operations Manager to monitor, visualize, and manage storage resources and generate reports.

Symantec recommends using Veritas Operations Manager (VOM) to manage Storage Foundation and Cluster Server environments.

You can download Veritas Operations Manager from http://go.symantec.com/vom.

Refer to the Veritas Operations Manager documentation for installation, upgrade, and configuration instructions.

The Veritas Enterprise Administrator (VEA) console is no longer packaged with Storage Foundation products. If you want to continue using VEA, a software version is available for download from http://www.symantec.com/operations-manager/support. Symantec Storage Foundation Management Server is deprecated.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a website that automates and simplifies some of the most time-consuming administrative tasks. It helps you identify risks in your datacenters and improve operational efficiency, enabling you to manage the complexity that is associated with datacenter architectures and scale

Table 1-1 lists three major datacenter tasks and the SORT tools that can help you accomplish them.

Table 1-1 Datacenter tasks and the SORT tools

Task	SORT tools
Prepare for installations and upgrades	■ Installation and Upgrade checklists Display system requirements including memory, disk space, and architecture. ■ Installation and Upgrade custom reports Create reports that determine if you're ready to install or upgrade a Symantec enterprise product. ■ Array-specific Module Finder List the latest Array Support Libraries (ASLs) and Array Policy Modules (APMs) for UNIX servers, and Device Driver Installers (DDIs) and Device Discovery Layers (DDLs) for Windows servers. ■ High Availability Agents table Find and download the agents for applications, databases, replication, and Symantec partners.
Identify risks and get server-specific recommendations	■ Patch notifications Receive automatic email notifications about patch updates. (Sign in required.) ■ Risk Assessment check lists Display configuration recommendations based on your Symantec product and platform. ■ Risk Assessment custom reports Create reports that analyze your system and give you recommendations about system availability, storage use, performance, and best practices. ■ Error code descriptions and solutions Display detailed information on thousands of Symantec error codes.

Table 1-1 Datacenter tasks and the SORT tools *(continued)*

Task	SORT tools
Improve efficiency	■ Patch Finder List and download patches for your Symantec enterprise products. ■ License/Deployment custom reports Create custom reports that list your installed Symantec products and license keys. Display licenses by product, platform, server tier, and system. ■ Symantec Performance Value Unit (SPVU) Calculator Use the calculator to assist you with the pricing meter transition. ■ Documentation List and download Symantec product documentation, including manual pages, product guides, and support articles. ■ Related links Display links to Symantec product support, forums, customer care, and vendor information on a single page.

SORT is available at no additional charge.

To access SORT, go to:

https://sort.symantec.com

Chapter 2

System requirements

This chapter includes the following topics:

- Release notes
- Important preinstallation information for DMP
- Supported operating systems
- Disk space requirements
- Virtual I/O Server (VIOS) requirements
- Checking installed product versions and downloading maintenance releases and patches
- Obtaining installer patches
- Disabling external network connection attempts

Release notes

The *Release Notes* for each Symantec 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

Important preinstallation information for DMP

Before you install DMP, make sure that you have reviewed the following information:

- Preinstallation checklist for your configuration. Go to the SORT installation checklist tool. From the drop-down lists, select the information for the Symantec product you want to install, and click **Generate Checklist**.
- Hardware compatibility list for information about supported hardware: http://www.symantec.com/docs/TECH211575
- For important updates regarding this release, review the Late-Breaking News Technote on the Symantec Technical Support website: http://www.symantec.com/docs/TECH211540

Supported operating systems

For information on supported operating systems for various components of DMP, see the *Symantec 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 to determine whether there is sufficient space.

Or, go to the installation directory and run the installer with the `-precheck` option.

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

See "About the script-based installer" on page 37.

Virtual I/O Server (VIOS) requirements

To run DMP in VIOS, the minimum VIOS level that is required is 2.1.3.10-FP-23 or later.

Before installing DMP on VIOS, confirm the following:

If any path to the target disk has `SCSI reserve ODM` attribute set, then change the attributes to release the SCSI reservation from the paths, on a restart.

- If a path has the `reserve_policy` attribute set, change the`reserve_policy` attribute to `no_reserve` for all the paths.

  # lsattr -E1 hdisk557 | grep res

  ```
  reserve_policy single_path
  Reserve Policy True
  ```

```
# chdev -l hdisk557 -a reserve_policy=no_reserve -P
hdisk557 changed
```

- If a path has the `reserve_lock` attribute set, change the `reserve_lock`attribute to `no`.

```
# lsattr -E1 hdisk558 | grep reserve_lock
reserve_lock yes
Reserve Device on open True
# chdev -l hdisk558 -a reserve_lock=no -P
hdisk558 changed
```

Checking installed product versions and downloading maintenance releases and patches

Symantec provides a means to check the Symantec filesets you have installed, and download any needed maintenance releases and patches.

Use the `installer` command with the `-version` option to determine what is installed on your system, and download any needed maintenance releases or patches. After you have installed the current version of the product, you can use the `showversion` script in the `/opt/VRTS/install` directory to find product information.

The `version` option or the `showversion` script checks the specified systems and discovers the following:

- DMP product versions that are installed on the system
- All the required filesets and the optional Symantec filesets installed on the system
- Any required or optional filesets (if applicable) that are not present
- Installed patches
- Available base releases (major or minor)
- Available maintenance releases
- Available patch releases

To check your systems and download maintenance releases and patches

1. Mount the media, or navigate to the installation directory.
2. Start the installer with the `-version` option.

   ```
   # ./installer -version sys1 sys2
   ```

   For each system, the installer lists all of the installed base releases, maintenance releases, and patches, followed by the lists of available downloads.

3 If you have Internet access, follow the prompts to download the available maintenance releases and patches to the local system.

4 If you do not have Internet access, you can download any needed maintenance releases and patches from the Symantec Operations Readiness Tools (SORT) Patch Finder page at:

https://sort.symantec.com/patch/finder

You can obtain installer patches automatically or manually.

See "Obtaining installer patches" on page 21.

Downloading maintenance releases and patches requires the installer to make outbound networking calls. You can also disable external network connection attempts.

See "Disabling external network connection attempts" on page 22.

Obtaining installer patches

Symantec occasionally finds issues with the Symantec Dynamic Multi-Pathing installer, and posts public installer patches on the Symantec Operations Readiness Tools (SORT) website's Patch Finder page at:

https://sort.symantec.com/patch/finder

You can access installer patches automatically or manually.

To download installer patches automatically

- Starting with Symantec Dynamic Multi-Pathing version 6.1, installer patches are downloaded automatically. No action is needed on your part.

  If you are running Symantec Dynamic Multi-Pathing version 6.1 or later, and your system has Internet access, the installer automatically imports any needed installer patch, and begins using it.

Automatically downloading installer patches requires the installer to make outbound networking calls. You can also disable external network connection attempts.

See "Disabling external network connection attempts" on page 22.

If your system does not have Internet access, you can download installer patches manually.

To download installer patches manually

1. Go to the Symantec Operations Readiness Tools (SORT) website's Patch Finder page, and save the most current Symantec patch on your local system.
2. Navigate to the directory where you want to unzip the file you downloaded in step 1.
3. Unzip the patch tar file. For example, run the following command:

   ```
   # gunzip cpi-6.1P2-patches.tar.gz
   ```

4. Untar the file. For example, enter the following:

   ```
   # tar -xvf cpi-6.1P2-patches.tar
   patches/
   patches/CPI61P2.pl
   README
   ```

5. Navigate to the installation media or to the installation directory.
6. To start using the patch, run the `installer` command with the `-require` option. For example, enter the following:

   ```
   # ./installer -require /target_directory/patches/CPI61P2.pl
   ```

Disabling external network connection attempts

When you execute the `installer` command, the installer attempts to make an outbound networking call to get information about release updates and installer patches. If you know your systems are behind a firewall, or do not want the installer to make outbound networking calls, you can disable external network connection attempts by the installer.

To disable external network connection attempts

- Disable inter-process communication (IPC).

  To disable IPC, run the installer with the `-noipc` option.

  For example, to disable IPC for system1 (sys1) and system2 (sys2) enter the following:

  ```
  # ./installer -noipc sys1 sys2
  ```

Chapter 3

Planning to install DMP

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 have the current version of this guide. The latest documentation is available on the Symantec Operations Readiness Tools (SORT) website.

https://sort.symantec.com/documents

Document version: 6.2 Rev 0.

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

Follow the preinstallation instructions if you want to install Symantec Dynamic Multi-Pathing.

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

About installation and configuration methods

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

Table 3-1 shows the installation and configuration methods that DMP supports.

Table 3-1 Installation and configuration methods

Method	Description

The script-based installer	Using the script-based installer, you can install Symantec products (version 6.1 and later) from a driver system running a supported platform to target computers running any supported platform.
	
	To install your Symantec product using the installer, choose one of the following:
	
	■ The general product installer:
	`installer`
	The general product installer script provides a menu that simplifies the selection of installation and configuration options. Use the general product installer if you want to install multiple products from a disc.
	
	■ Product-specific installation scripts:
	`installdmp<version>`
	The product-specific installation scripts provide command-line interface options. Installing and configuring with the `installdmp` script is identical to running the general product installer and specifying DMP from the list of products to install.
	Use the product-specific installation scripts to install or configure individual products you download electronically.
	
	See "About the script-based installer" on page 37.

The web-based installer	Using the web-based installer, you can install Symantec products (version 6.1 and later) from a driver system running a supported platform to target computers running any supported platform The web-based installer provides an interface to manage the installation and configuration from a remote site using a standard web browser. `webinstaller` See "About the web-based installer" on page 43.
Deployment Server	Using the Deployment Server, you can store multiple release images in one central location and deploy them to systems of any supported platform. See "About the Deployment Server" on page 65.

Table 3-1 Installation and configuration methods *(continued)*

Method	Description
Silent installation using response files	Response files automate installation and configuration by using the information that is stored in a specified file instead of prompting you for information. 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 option to install silently on one or more systems. See "About response files" on page 49.
Install Bundles	Beginning with version 6.1, you can easily install or upgrade your systems directly to a base, maintenance, or patch level in one step using Install Bundles. The installer installs both releases as if they were combined in the same release image. The various scripts, filesets, and patch components are merged, and multiple releases are installed together as if they are one combined release. See "Using Install Bundles to simultaneously install or upgrade base releases, maintenance releases, and patches" on page 107.
Network Installation Manager (NIM)	You can perform many advanced NIM installation tasks using the NIM command interface and the System Management Interface Tool (SMIT). Use the product installer or the product-specific installation script to generate a NIM `installp` bundle. Use the generated `installp` bundle to install Symantec filesets from your NIM server.
mksysb utility	You can use the mksysb utility to back up the system image. This image can be installed on another host.

Chapter 4

Licensing DMP

This chapter includes the following topics:

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

About Symantec product licensing

You have the option to install Symantec 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.

http://www.symantec.com/products-solutions/licensing/activating-software/detail.jsp?detail_id=licensing_portal

The 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 systems with a management server. 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 previous release of the Symantec software, the installer asks whether you want to upgrade the key to the new version. The existing license keys may not activate new features in this release.

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

- Run the `vxkeyless` command to set the product level for the products you have purchased. This option also requires that you manage the server or cluster with a management server.
  See "Setting or changing the product level for keyless licensing" on page 27.
  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 Symantec product license keys" on page 29.
  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: 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 Symantec products and functionality that are licensed.

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

http://go.symantec.com/vom

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

When you upgrade from a previous release, the product installer prompts you to update the `vxkeyless` license product level to the current release level. If you update the `vxkeyless` license product level during the upgrade process, no further action is required. If you do not update the `vxkeyless` license product level, the output you see when you run the `vxkeyless display` command includes the previous release's `vxkeyless` license product level. Each `vxkeyless` license product level name includes the suffix *_previous_release_version*. For example, DMP_6.0, or SFENT_VR_5.1SP1, or VCS_GCO_5.1. If there is no suffix, it is the current release version.

You would see the suffix *_previous_release_version* if you did not update the `vxkeyless` product level when prompted by the product installer. Symantec highly recommends that you always use the current release version of the product levels. To do so, use the `vxkeyless set` command with the desired product levels. If you see SFENT_60, VCS_60, use the `vxkeyless set SFENT,VCS` command to update the product levels to the current release.

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

To set or change the product level

1 Change your current working directory:

```
# export PATH=$PATH:/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 Symantec products until you install a new key or set a new product level.

See "Installing Symantec product license keys" on page 29.

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 Symantec product license keys

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

`vxlicinst`	Installs a license key for a Symantec product
`vxlicrep`	Displays the currently installed licenses
`vxlictest`	Retrieves the features and their descriptions that are 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 or change a license

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

```
# cd /opt/VRTS/bin

# ./vxlicinst -k license key
```

2 Run the following Veritas Volume Manager (VxVM) command to recognize the new license:

```
# vxdctl license init
```

See the `vxdctl(1M)` manual page.

If you have `vxkeyless` licensing, you can view or update the keyless product licensing levels.

See "Setting or changing the product level for keyless licensing" on page 27.

Section 2

Installation of DMP

- Chapter 5. Preparing to install DMP
- Chapter 6. Installing DMP using the script-based installer
- Chapter 7. Installing DMP using the web-based installer
- Chapter 8. Automated installation using response files
- Chapter 9. Installing DMP using operating system-specific methods

Chapter 5

Preparing to install DMP

This chapter includes the following topics:

- Installation preparation overview
- Setting environment variables
- About using ssh or rsh with the installer
- Mounting the product disc
- Assessing the system for installation readiness

Installation preparation overview

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

Table 5-1 Installation overview

Installation task	Section
Obtain product licenses.	See "About Symantec product licensing" on page 26.
Download the software, or insert the product DVD.	See "Mounting the product disc" on page 34.
Set environment variables.	See "Setting environment variables" on page 33.
Configure the Secure Shell (ssh) or Remote Shell (rsh) on all nodes.	See "About using ssh or rsh with the installer" on page 33.
Verify that hardware, software, and operating system requirements are met.	See "Release notes" on page 18.

Table 5-1 Installation overview *(continued)*

Installation task	Section
Check that sufficient disk space is available.	See "Disk space requirements" on page 19.
Use the installer to install the products.	See "About the script-based installer" on page 37.

Setting environment variables

Most of the commands which are used in the installation are present 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 want to use `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 want to use a C shell (`csh` or `tcsh`), enter the following:

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

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

About using ssh or rsh with the installer

The installer uses passwordless Secure Shell (ssh) or Remote Shell (rsh) communications among systems. The installer uses the ssh daemon or rsh daemon that comes bundled with the operating system. During an installation, you choose the communication method that you want to use. Or, you can run the `installer -comsetup` command to set up ssh or rsh explicitly. You then provide the installer with the superuser passwords for the systems where you plan to install. When the

installation process completes, the installer asks you if you want to remove the password-less connection. If you choose yes, then the installer removes the password. If you choooose no, then the installer saves the password. If you use the `Ctrl+c` key to interrupt the installer, a message is displayed asking you if you want to remove the rsh/ssh password-less connection. If installation terminated abruptly, use the installation script's `-comcleanup` option to remove the ssh configuration 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, or use the `installer -comsetup` option to set up an ssh or rsh configuration from the systems.

- When you perform installer sessions using a response file.

See "About configuring secure shell or remote shell communication modes before installing products" on page 155.

Mounting the product disc

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

To mount the product disc

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

   The systems must be in the same subnet.

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

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

   The output resembles:

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

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

3 Make sure that the `/cdrom` file system is created:

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

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

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

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

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

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

6 Mount the disc:

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

Assessing the system for installation readiness

Symantec provides the following tools for assessing your system, to ensure that the system meets the requirements for installing Symantec Dynamic Multi-Pathing 6.2.

Symantec Operations Readiness Tools	Symantec Operations Readiness Tools (SORT) is a web-based application that is designed to support Symantec enterprise products. See "About Symantec Operations Readiness Tools" on page 15.

Prechecking your systems using the installer	Performs a preinstallation check on the specified systems. The product installer reports whether the specified systems meet the minimum requirements for installing Symantec Dynamic Multi-Pathing 6.2. See "Prechecking your systems using the installer" on page 36.

Prechecking your systems using the 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 Symantec programs for best performance
- Required operating system versions

To use the precheck option

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

   See "Installing DMP using the script-based installer" on page 39.

   See "Installing DMP with the web-based installer" on page 46.

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. Enter the system name or the IP address of the system that you want to check.
4. Review the output and make the changes that the installer recommends.

Chapter 6

Installing DMP using the script-based installer

This chapter includes the following topics:

- About the script-based installer
- Installing DMP using the script-based installer
- Performing a postcheck on a node

About the script-based installer

You can use the script-based installer to install Symantec products (version 6.1 and later) from a driver system that runs any supported platform to a target system that runs different supported platforms.

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

- The general product installer (`installer`). The general product installer script provides a menu that simplifies the selection of installation and configuration options. Use the general product installer if you want to install multiple products from a disc.
  See "Installing DMP using the script-based installer" on page 39.
- Product-specific installation scripts (`installdmp`). The product-specific installation scripts provide command-line interface options. Installing and configuring with the `installdmp` script is identical to running the general product installer and specifying DMP from the list of products to install. Use the product-specific installation scripts to install or configure individual products you download electronically. You can find these scripts at the root of the product media. These scripts are also installed with the product.

Table 6-1 lists all the SFHA Solutions product installation scripts. The list of product-specific installation scripts that you find on your system depends on the product that you install on your system.

Table 6-1 Product installation scripts

Symantec product name	Script name in the media	Script name after an installation
For all SFHA Solutions products	`installer`	N/A
Symantec ApplicationHA	`installapplicationha`	`installapplicationha <version>`
Symantec Cluster Server (VCS)	`installvcs`	`installvcs<version>`
Symantec Storage Foundation (SF)	`installsf`	`installsf<version>`
Symantec Storage Foundation and High Availability (SFHA)	`installsfha`	`installsfha<version>`
Symantec Storage Foundation Cluster File System High Availability (SFCFSHA)	`installsfcfsha`	`installsfcfsha<version>`
Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`	`installsfrac<version>`
Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE)	`installsfsybasece`	`installsfsybasece<version>`
Symantec Dynamic Multi-pathing (DMP)	`installdmp`	`installdmp<version>`

When you install from the installation media, the script name does not include a product version.

When you configure the product after an installation, the installation scripts include the product version in the script name.

For example, for the 6.2 version:

```
# /opt/VRTS/install/installdmp62 -configure
```

Note: The general product installer (`installer`) script does not include the product version.

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

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

See "Command options for the installation script" on page 137.

See "Command options for uninstall script" on page 142.

Installing DMP using the script-based installer

Use the installer program to install Symantec 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 155.

2. Load and mount the software disc.

   See "Mounting the product disc" on page 34.

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

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

4 From this directory, type the following command to install on the local system. Also use this command to install on remote systems provided that the Secure Shell (SSH) or Remote Shellrsh) 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 **Symantec Dynamic Multi-Pathing**, enter the corresponding number, and press the Return key.

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

8 Select one of the following installation options:

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

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

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

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

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

12 The installer installs the product filesets.

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 website:

http://go.symantec.com/sfhakeyless

---

13 The installer starts DMP processes. When you are prompted next, specify whether you want to send your installation information to Symantec. Note that the information that is sent to Symantec is only to help improve the installer software.

```
Installation procedures and diagnostic information were saved
in the log files under directory /var/tmp/installer-<platform>-<uuid>.
Analyzing this information helps Symantec discover and fix failed
operations performed by the installer. 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. If the `VRTSvxvm` fileset requires restart while installing it on the system, run the `/opt/VRTS/install/installdmp62 -configure` command after restart to start 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 Restart the systems if the installer prompts for a restart, to enable DMP native support.

16 Start the DMP processes.

See “Starting and stopping processes for the Symantec products ” on page 99.

Performing a postcheck on a node

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

To run the postcheck command on a node

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

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

   Or you can run the following command on your local macihne once DMP is installed.

   ```
   # /opt/VRTS/install/installdmp62 -postcheck
   ```

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

Chapter 7

Installing DMP using the web-based installer

This chapter includes the following topics:

- About the web-based installer
- Before using the web-based installer
- Starting the web-based installer
- Obtaining a security exception on Mozilla Firefox
- Performing a preinstallation check with the web-based installer
- Installing DMP with the web-based installer

About the web-based installer

Use the web-based installer interface to install Symantec 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 operates. While the installation processes operate, 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. Symantec recommends 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 web-based installer" on page 44.

See "Starting the web-based installer" on page 44.

Before using the web-based installer

The web-based installer requires the following configuration.

Table 7-1 Web-based installer requirements

System	Function	Requirements
Target system	The systems where you plan to install the Symantec products.	Must be a supported platform for Symantec Dynamic Multi-Pathing 6.2.
Installation server	The server where you start the installation. The installation media is accessible from the installation server.	Must be at one of the supported operating system update levels.
Administrative system	The system where you run the web browser to perform the installation.	Must have a web browser. Supported browsers: ■ Internet Explorer 6, 7, and 8 ■ Firefox 3.x and later

Starting the web-based installer

This section describes starting the web-based installer.

To start the web-based installer

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

```
# ./webinstaller start
```

The `webinstaller` script displays a URL. Note this URL.

Note: If you do not see the URL, please check your firewall and iptables settings. If you have configured a firewall, ensure that the firewall settings allow access to the port 14172. You can alternatively use the `-port` option to use a free port instead.

You can use the following command to display the details about ports used by webinstaller and its status:

```
# ./webinstaller status
```

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

5 Log in as superuser.

Obtaining a security exception on Mozilla Firefox

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

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

To obtain a security exception

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

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

3 Click **Get Certificate** button.

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

5 Click **Confirm Security Exception** button.

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

Performing a preinstallation check with the web-based installer

This section describes performing a preinstallation check with the web-based installer.

To perform a preinstallation check

1 Start the web-based installer.

See "Starting the web-based installer" on page 44.

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

3 Select **Symantec 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 If the validation completes successfully, click **Next**. The installer prompts you to begin the installation. Click **Yes** to install on the selected system. Click **No** to install later.

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

Installing DMP with the web-based installer

This section describes installing DMP with the Symantec web-based installer.

To install DMP using the web-based installer

1 Perform preliminary steps.

See "Performing a preinstallation check with the web-based installer" on page 46.

2 Start the web-based installer.

See "Starting the web-based installer" on page 44.

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

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

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

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

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

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

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

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

On the license page, select one of the following radio buttons:

- Enable keyless licensing and complete system licensing later

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

  For more information, go to the following website:

  http://go.symantec.com/sfhakeyless

  Click **Next**

- Enter a valid license key
  If you have a valid license key, input the license key and click **Next**.

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

If the `VRTSvxvm` fileset requires restart while installing it on the system, run the configure task after restart to start the DMP processes.

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

12 If you are prompted, enter the option to specify whether you want to send your installation information to Symantec.

```
Installation procedures and diagnostic information were saved in
the log files under directory
/var/tmp/installer-<platform>-<uuid>. Analyzing this information
helps Symantec discover and fix failed operations performed by
the installer. Would you like to send the information about this
installation to Symantec to help improve installation in the
future? [y,n,q,?]
```

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

13 Restart the systems if the installer prompts for a restart to enable DMP native support.

Chapter 8

Automated installation using response files

This chapter 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 script 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 that 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.

   See "About the script-based installer" on page 37.
7. Complete the DMP post-installation tasks.

   For instructions, see the chapter *Performing post-installation and configuration tasks* in this document.

Upgrading DMP using response files

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

To perform automated DMP upgrade

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

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

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

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

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

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

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

Uninstalling DMP using response files

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

To perform an automated uninstallation

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

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

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

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

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

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

See "About the script-based installer" on page 37.

Syntax in the response file

The syntax of the Perl statements that is 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 1 ", "value 2 ", "value 3 "];
```

Response file variable definitions

Table 8-1 lists the variables that are used in the response file and their definitions.

Table 8-1 Response file variables

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

Table 8-1 Response file variables *(continued)*

Variable	Description
CFG{opt}{keyfile}	Defines the location of an ssh keyfile that is used to communicate with all remote systems. List or scalar: scalar Optional or required: optional
CFG{opt}{patchpath}	Defines a location, typically an NFS mount, from which all remote systems can install product patches. The location must be accessible from all target systems. List or scalar: scalar Optional or required: optional
CFG{opt}{tmppath}	Defines the location where a working directory is created to store temporary files and the filesets that are needed during the install. The default location is /var/tmp. 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{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 filesets are installed using the `-install` option. List or scalar: scalar Optional or required: optional
CFG{opt}{upgrade}	Upgrades all filesets installed, without configuration. List or scalar: list Optional or required: optional

Table 8-1 Response file variables *(continued)*

Variable	Description
CFG{opt}{uninstall}	Uninstalls DMP filesets. List or scalar: scalar Optional or required: optional
CFG{opt}{disable_dmp_native_support}	If it is set to 1, Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools is disabled after upgrade. List or scalar: scalar Optional or required: optional

Chapter 9

Installing DMP using operating system-specific methods

This chapter includes the following topics:

- About installing DMP using operating system-specific methods
- Installing DMP using NIM and the installer
- Installing Symantec Dynamic Multi-Pathing using the mksysb utility

About installing DMP using operating system-specific methods

On AIX, you can install DMP using the following methods:

- You can use the product installer along with Network Installation Manager (NIM) to install the Symantec product, or to install the operating system with the Symantec product.
  See "Installing DMP using NIM and the installer" on page 56.
- You can use the `mksysb` utility to back up the system image. You can then install DMP through `mksysb` image.
  See "Installing Symantec Dynamic Multi-Pathing using the `mksysb` utility" on page 58.

Installing DMP using NIM and the installer

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

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

In the following samples, the LPP resource uses LPP-7100-up2date and its relevant SPOT resource is spot-7100-up2date.

Preparing the installation bundle on the NIM server

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

Note: Make sure that the appropriate NIM LPP_SOURCE and SPOT resources are present on the NIM server.

To prepare the installation bundle

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

```
# lsnim |grep -i lpp_source
LPP-7100-up2date resources lpp_source
```

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

```
# ./installdmp -nim LPP-7100-up2date
```

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

4 Enter a name for the bundle, for example *DMP62*.

5 Run the `lsnim -l` command to check that the installp_bundle resource is created successfully.

```
# lsnim -l DMP62
DMP62:
class = resources
type = installp_bundle
Rstate = ready for use
prev_state = unavailable for use
location = /opt/VRTS/nim/DMP62.bundle
alloc_count = 0
server = master
```

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

You can install DMP on the NIM client using the SMIT tool on the NIM server.

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

To install DMP

1 On the NIM server, start SMIT.

```
# smitty nim
```

2 In the menu, select **Perform NIM Software Installation and Maintenance Tasks**.

3 In the menu, select **Install and Update Software**.

4 In the menu, select **Install Software Bundle**.

5 Select the systems from the list on which to install the software bundle.

6 In the menu, select the LPP_SOURCE. In this example, specify **LPP-7100-up2date**.

7 In the menu, select the bundle, for example, **DMP62**.

8 For the `installp` flags, specify that the ACCEPT new license agreements flag has a **yes** value.

9 Press the Enter key to start the installation. Note that it may take some time to finish.

10 After the installation completes, configure DMP.

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

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

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

To install DMP and the operating system

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

   ```
   # smitty nim_bosinst
   ```

2. In the menu, select the standalone target.
3. In the menu, select **spot - Install a copy of a SPOT resource**.
4. In the menu, select the spot resource **spot-7100-up2date**.
5. In the menu, select the LPP_SOURCE. In this example, select **LPP-7100-up2date**.
6. In the menu, select the following options:
   - For the ACCEPT new license agreements option, specify **yes**.
   - For the Additional Bundles to Install option, specify **DMP62**.
7. For the `installp` flags, specify that the ACCEPT new license agreements flag has a **yes** value.
8. After the installation completes, configure DMP.

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

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

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

The installation process involves the following steps:

- Creating the `mksysb` image.

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

Creating the `mksysb` backup image

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

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

To create an `mksysb` image using SMIT interface

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

   The recommended approach is to install all of the filesets. But do not configure the product stack before you take `mksysb` image if the image is to be installed on a different computer.
3. Enter fast path `smitty mksysb` and enter the required values.
4. Press enter to start the backup image creation.

To create an `mksysb` image using commands manually

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

   The recommended approach is to install all of the filesets. But do not configure product stack before you take the `mksysb` image if the image is to be installed on a different computer.
3. Create the `mksysb` image in one of the following ways:

   - If you want to restore the `mksysb` backup of SF-configured host on the same host, run the following command:

     ```
     # /usr/bin/mksysb '-i' '-X'  backup_file_name
     ```

   - If you want to restore the `mksysb` backup of SF-configured host on another host, run the following commands:
     Create the file `/etc/exclude.rootvg`.
     Add the following entries to the file `/etc/exclude.rootvg`.

```
# cat /etc/exclude.rootvg
^./etc/vx/cvmtab
^./etc/vx/ddlconfig.info
^./etc/vx/volboot
```

If DMP root support is enabled, run the following command:

```
# vxdmpadm native release
```

Run the following command to restore the backup:

```
# /usr/bin/mksysb -e '-i' '-X' backup_file_name
```

If DMP native support is run, execute the following:

```
# vxdmpadm native acquire
```

Installing `mksysb` image on alternate disk

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

Before you restore `mksysb` on an alternate disk, perform the following steps to prepare the target disk

1. If DMP root support is enabled, run the following command:

   ```
   # vxdmpadm native release
   ```

2. Remove the disk from VM.

   ```
   # vxdmpadm getsubpaths dmpnodename=disk_1 | grep hdisk
     hdisk1        ENABLED(A)     -           sas0        Disk          disk

   # vxdisk rm disk_1
   ```

3. Clear the PV id of the target disk.

   ```
   # chdev -l hdisk1 -a pv=clear
     hdisk1 changed
   ```

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

1. Type `smitty` and then select **Software Installation and Maintenance** -> **Alternate Disk Installation** -> **Install mksysb on an Alternate Disk**
2. Select target disks

3 Select `mksysb` image to be installed

4 Select appropriate values for remaining options

5 Press enter to start the `mksysb` image installation.

6 If DMP native support is enabled, execute this command before restarting:

```
# vxdmpadm native acquire
```

7 After installation is complete restart from the alternate disk.

8 If DMP was not configured in the `mksysb` image then run `/opt/VRTS/install/installdmp<version> -configure` after restart.

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

See "About the script-based installer" on page 37.

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

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

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

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

1 Create an `mksysb` resource from the `mksysb` image that has been created on NIM server.

2 Set up the system on which you want to install DMP as NIM client.

3 Type `smitty nim` then select **Perform NIM Software Installation and Maintenance Tasks** -> **Alternate Disk Installation** -> **Install mksysb on an Alternate Disk**

4 Select target system.

5 Select target disks.

6 Select `mksysb` image to be installed.

7 Select appropriate values for remaining options.

8 Press enter to start the `mksysb` image installation.

9 If DMP native support is enabled, execute this command before restarting:

```
# vxdmpadm native acquire
```

10 If DMP was not configured in the `mksysb` image then run `/opt/VRTS/install/installdmp<version> -configure` after you restart NIM client.

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

See "About the script-based installer" on page 37.

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

1 Create an `mksysb` resource from the `mksysb` image that has been created on NIM server.

2 Set up the system on which you want to install DMP as NIM client.

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

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

4 If DMP was not configured in the `mksysb` image then run `/opt/VRTS/install/installdmp<version> -configure` after you restart NIM client.

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

See "About the script-based installer" on page 37.

Verifying the installation

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

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

All the filesets should be installed properly.

See "Checking installed product versions and downloading maintenance releases and patches" on page 20.

Section 3

Managing your Symantec deployments

- Chapter 10. Performing centralized installations using the Deployment Server

Chapter 10

Performing centralized installations using the Deployment Server

This chapter includes the following topics:

- About the Deployment Server
- Deployment Server overview
- Installing the Deployment Server
- Setting up a Deployment Server
- Setting deployment preferences
- Specifying a non-default repository location
- Downloading the most recent release information
- Loading release information and patches on to your Deployment Server
- Viewing or downloading available release images
- Viewing or removing repository images stored in your repository
- Deploying Symantec product updates to your environment
- Finding out which releases you have installed, and which upgrades or updates you may need
- Defining Install Bundles
- Creating Install Templates

- Deploying Symantec releases
- Connecting the Deployment Server to SORT using a proxy server

About the Deployment Server

The Deployment Server makes it easier to install or upgrade SFHA releases from a central location. The Deployment Server lets you store multiple release images and patches in one central location and deploy them to systems of any supported UNIX or Linux operating system (6.1 or later).

Note: The script-based installer for version 6.1 and higher supports installations from one operating system node onto a different operating system. Therefore, heterogeneous push installations are supported for 6.1 and higher releases only.

Push installations for product versions 5.1, 6.0, or 6.0.1 releases must be executed from a system that is running the same operating system as the target systems. In order to perform push installations for product versions 5.1, 6.0, or 6.0.1 releases on multiple platforms, you must have a separate Deployment Server for each operating system.

The Deployment Server lets you do the following as described in Table 10-1.

Table 10-1 Deployment Server functionality

Feature	Description
Manage repository images	■ View available SFHA releases. ■ Download maintenance and patch release images from the Symantec Operations Readiness Tools (SORT) website into a repository. ■ Load the downloaded release image files from FileConnect and SORT into the repository. ■ View and remove the release image files that are stored in the repository.
Version check systems	■ Discover filesets and patches installed on your systems and informs you of the product and version installed ■ Identify base, maintenance, and patch level upgrades to your system and to download maintenance and patch releases. ■ Query SORT for the most recent updates.

Table 10-1 Deployment Server functionality *(continued)*

Feature	Description
Install or upgrade systems	■ Install base, maintenance, or patch level releases. ■ Install SFHA from any supported UNIX or Linux operating system to any other supported UNIX or Linux operating system. ■ Automatically load the script-based installer patches that apply to that release. ■ Install or upgrade an Install Bundle that is created from the **Define/Modify Install Bundles** menu. ■ Install an Install Template that is created from the **Create Install Templates** menu.
Define or modify Install Bundles	Define or modify Install Bundles and save them using the Deployment Server.
Create Install Templates	Discover installed components on a running system that you want to replicate on to new systems.
Update metadata	Download, load the release matrix updates, and product installer updates for systems behind a firewall. This process happens automatically when you connect the Deployment Server to the Internet, or it can be initiated manually. If the Deployment Server is not connected to the Internet, then the **Update Metadata** option is used to upload current metadata.
Set preferences	Define or reset program settings.

Note: The Deployment Server is available only from the command line. The Deployment Server is not available for the web-based installer.

Note: Many of the example outputs used in this chapter are based on Red Hat Enterprise Linux.

Deployment Server overview

After obtaining and installing the Deployment Server and defining a central repository, you can begin managing your deployments from that repository. You can load and store product images for Symantec products back to version 5.1 in your Deployment Server. The Deployment Server is a central installation server for storing and managing your product updates.

Setting up and managing your repository involves the following tasks:

- Installing the Deployment Server.
  See “Installing the Deployment Server” on page 67.
- Setting up a Deployment Server.
  See “Setting up a Deployment Server” on page 68.
- Finding out which products you have installed, and which upgrades or updates you may need.
  See “Viewing or downloading available release images” on page 75.
- Adding release images to your Deployment Server.
  See “Viewing or downloading available release images” on page 75.
- Removing release images from your Deployment Server.
  See “Viewing or removing repository images stored in your repository” on page 79.
- Defining or modifying Install Bundles to manually install or upgrade a bundle of two or more releases.
  See “Defining Install Bundles” on page 84.
- Creating Install Templates to discover installed components on a system that you want to replicate to another system.
  See “Creating Install Templates” on page 90.

Later, when your repository is set up, you can use it to deploy Symantec products to other systems in your environment.

See “Deploying Symantec product updates to your environment” on page 82.

See “Deploying Symantec releases” on page 92.

Installing the Deployment Server

You can obtain the Deployment Server by either:

- Installing the Deployment Server manually.
- Running the Deployment Server after installing at least one Symantec 6.2 product.

Note: The `VRTSperl` and the `VRTSsfcpi<version>`filesets are included in all Storage Foundation (SF) products, so installing any Symantec 6.2 product lets you access the Deployment Server.

To install the Deployment Server manually without installing a Symantec 6.2 product

1. Log in as superuser.
2. Mount the installation media.

   See "Mounting the product disc" on page 34.
3. Move to the top-level directory on the disc.

   ```
   # cd /mnt/cdrom
   ```
4. Navigate to the following directory:

   ```
   # cd pkgs
   ```
5. Run the following commands to install the `VRTSperl` and the `VRTSsfcpi<version>` filesets:

   ```
   # installp -C
   # installp -aXd ./VRTSperl.bff VRTSperl
   # installp -aXd ./VRTSsfcpi<version>.bff VRTSsfcpi<version>
   ```

To run the Deployment Server

1. Log in as superuser.
2. Navigate to the following directory:

   ```
   # cd /opt/VRTS/install
   ```
3. Run the Deployment Server.

   ```
   # ./deploy_sfha
   ```

Setting up a Deployment Server

Symantec recommends that you create a dedicated Deployment Server to manage your product updates.

A Deployment Server is useful for doing the following tasks:

- Storing release images for the latest upgrades and updates from Symantec in a central repository directory.
- Installing and updating systems directly by accessing the release images that are stored within a central repository.

- Defining or modifying Install Bundles for deploying a bundle of two or more releases.
- Discovering installed components on a system that you want to replicate to another system.
- Installing Symantec products from the Deployment Server to systems running any supported platform.
- Creating a file share on the repository directory provides a convenient, central location from which systems running any supported platform can install the latest Symantec products and updates.

Create a central repository on the Deployment Server to store and manage the following types of Symantec releases:

- Base releases. These major releases and minor releases are available for all Symantec products. They contain new features, and you can download them from FileConnect.
- Maintenance releases. These releases are available for all Symantec products. They contain bug fixes and a limited number of new features, and you can download them from the Symantec Operations Readiness Tools (SORT) website.
- Patches. These releases contain fixes for specific products, and you can download them from the SORT website.

Note: All base releases and maintenance releases can be deployed using the install scripts that are included in the release. Before version 6.0.1, patches were installed manually. From the 6.0.1 release and onwards, install scripts are included with patch releases.

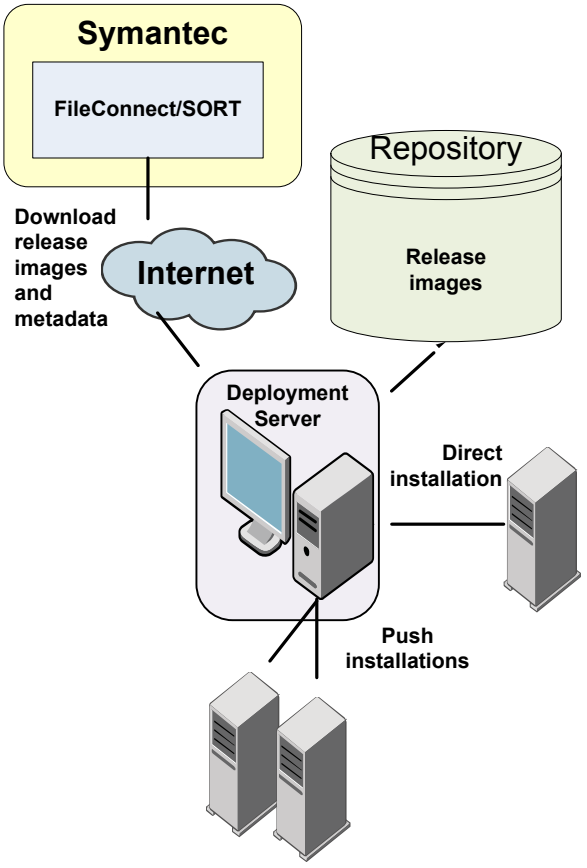
You can set up a Deployment Server with or without Internet access.

- If you set up a Deployment Server that has Internet access, you can download maintenance releases and patches from Symantec directly. Then, you can deploy them to your systems.
  Setting up a Deployment Server that has Internet access
- If you set up a Deployment Server that does not have Internet access, you can download maintenance releases and patches from Symantec on another system that has Internet access. Then, you can load the images onto the Deployment Server separately.
  Setting up a Deployment Server that does not have Internet access

Setting up a Deployment Server that has Internet access

Figure 10-1 shows a Deployment Server that can download product images directly from Symantec using the Deployment Server.

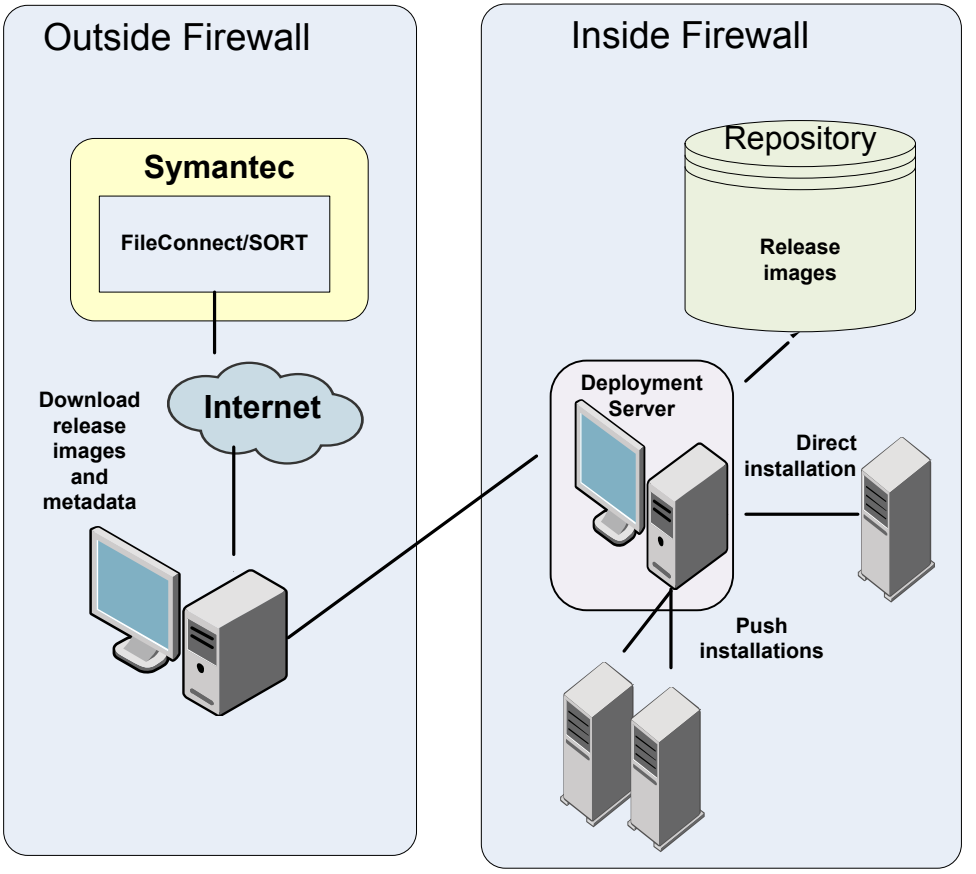
Figure 10-1 Example Deployment Server that has Internet access



Setting up a Deployment Server that does not have Internet access

Figure 10-2 shows a Deployment Server that does not have Internet access. In this scenario, release images and metadata updates are downloaded from another system. Then, they are copied to a file location available to the Deployment Server, and loaded.

Figure 10-2 Example Deployment Server that does not have Internet access



Release image files for base releases must be manually downloaded from FileConnect and loaded in a similar manner.

Setting deployment preferences

You can set preferences for managing the deployment of products dating back to version 5.1.

Note: You can select option **U (Terminology and Usage)** to obtain more information about Deployment Server terminology and usage.

To set deployment preferences

1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

```
Task Menu:

R) Manage Repository Images             M) Update Metadata
V) Version Check Systems                S) Set Preferences
I) Install/Upgrade Systems              U) Terminology and Usage
B) Define/Modify Install Bundles        ?) Help
T) Create Install Templates             Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

2 Select option **S**, **Set Preferences**.

You see the following output:

```
Current Preferences:

Repository            /opt/VRTS/repository
Selected Platforms    N/A
Save Tar Files        N/A

Preference List:

     1)  Repository
     2)  Selected Platforms
     3)  Save Tar Files
     b)  Back to previous menu

Select a preference to set: [1-3,b,q,?]
```

3 Do one of the following:

- To set the default repository, enter **1**. Then enter the name of the repository in which you want to store your downloads. For example, enter the following:

  ```
  # /opt/VRTS/install/ProductDownloads
  ```

  If the specified repository replaces a previous repository, the installer asks if you want to move all your files into the new repository. To move your files to the new repository, enter **y**.

- To add or remove a platform, enter **2**. You are provided selections for adding or deleting a platform. When a single platform is removed, it becomes **N/A**, which means that it is not defined. By default, all platforms are chosen. Once you select to add or remove a platform, the platform is added or removed in the preferences file and the preference platforms are updated.
  If only one platform is defined, no platform, architecture, distribution, and version selection menu is displayed.
- To set the option for saving or removing tar files, enter **3**. At the prompt, if you want to save the tar files after untarring them, enter **y**. Or, if you want to remove tar files after untarring them, enter **n**.
  By default, the installer does not remove tar files after the releases have been untarred.

Specifying a non-default repository location

You can specify a repository location other than the default that has been set within the system preferences by using the command line option. The command line option is mainly used to install a release image from a different repository location. When you use the command line option, the designated repository folder is used instead of the default for the execution time of the script. Using the command line option does not override the repository preference set by the **Set Preference** menu item.

Note: When you specify a non-default repository, you are allowed only to view the repository (**View/Remove Repository**), and use the repository to install or upgrade (**Install/Upgrade Systems**) on other systems.

To use the command line option to specify a non-default repository location

- At the command line, to specify a non-default repository location, enter the following:

  ```
  # ./deploy_sfha -repository repository_path
  ```

  where *repository_path* is the location of the repository.

Downloading the most recent release information

Use one of the following methods to obtain a `.tar` file with the most recent release information:

- Download a copy from the SORT website.
- Run the Deployment Server from a system that has Internet access.

To obtain a data file by downloading a copy from the SORT website

1 Download the `.tar` file from the SORT site at:

https://sort.symantec.com/support/related_links/offline-release-updates

2 Click on **deploy_sfha.tar [Download]**, and save the file to your desktop.

To obtain a data file by running the Deployment Server from a system with Internet access

1 Run the Deployment Server. Enter the following:

```
# /opt/VRTS/install/deploy_sfha
```

2 Select option **M**, **Update Metadata**.

You see the following output:

```
The Update Metadata option is used to load release matrix updates on to systems that do
not have an Internet connection with SORT (https://sort.symantec.com).  Your system has a
connection with SORT and is able to receive updates.  No action is necessary unless you
would like to create a file to update another Deployment Server system.

     1)  Download release matrix updates and installer patches
     2)  Load an update tar file
     b)  Back to previous menu

Select the option: [1-2,b,q,?]
```

3 Select option **1**, **Download release matrix updates and installer patches**.

Loading release information and patches on to your Deployment Server

In this procedure, the Internet-enabled system is the system to which you downloaded the `deploy_sfha.tar` file.

See "Downloading the most recent release information" on page 73.

To load release information and patches on to your Deployment Server

1. On the Internet-enabled system, copy the `deploy_sfha.tar` file you downloaded to a location accessible by the Deployment Server.
2. On the Deployment Server, change to the installation directory. For example, enter the following:

   ```
   # cd /opt/VRTS/install/
   ```

3. Run the Deployment Server. Enter the following:

   ```
   # ./deploy_sfha
   ```

4. Select option **M**, **Update Metadata**, and select option **2**, **Load an update tar file**. Enter the location of the `deploy_sfha.tar` file (the installer calls it a "meta-data tar file").

   ```
   Enter the location of the meta-data tar file: [b]
   (/opt/VRTS/install/deploy_sfha.tar)
   ```

   For example, enter the location of the meta-data tar file:

   ```
   /tmp/deploy_sfha.tar
   ```

Viewing or downloading available release images

You can use the Deployment Server to conveniently view or download available release images to be deployed on other systems in your environment.

Note: If you have Internet access, communication with the Symantec Operations Readiness Tools (SORT) provides the latest release information. If you do not have Internet access, static release matrix files are referenced, and the most recent updates may not be included.

See "Loading release information and patches on to your Deployment Server" on page 74.

To view or download available release images

1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

```
Task Menu:

R) Manage Repository Images              M) Update Metadata
V) Version Check Systems                 S) Set Preferences
I) Install/Upgrade Systems               U) Terminology and Usage
B) Define/Modify Install Bundles         ?) Help
T) Create Install Templates              Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

2 Select option **R**, **Manage Repository Images**.

You see the following output:

```
1)  View/Download Available Releases
2)  View/Remove Repository Images
3)  Load a Release Image
b)  Back to previous menu

Select the option you would like to perform [1-3,b,q,?]
```

3 Select option **1**, **View/Download Available Releases**, to view or download what is currently installed on your system.

You see a list of platforms and release levels.

```
To view or download available releases, the platform type and release
level type must be selected.

1)  AIX 5.3                   2)  AIX 6.1
3)  AIX 7.1                   4)  HP-UX 11.31
5)  RHEL5 x86_64              6)  RHEL6 x86_64
7)  RHEL7 x86_64              8)  SLES10 x86_64
9)  SLES11 x86_64             10) Solaris 9 Sparc
11) Solaris 10 Sparc          12) Solaris 10 x64
13) Solaris 11 Sparc          14) Solaris 11 x64
b)  Back to previous menu

Select the platform of the release to view/download [1-14,b,q]
```

4 Select the release level for which you want to get release image information. Enter the platform you want.

You see options for the Symantec release levels.

```
1) Base
2) Maintenance
3) Patch
b) Back to previous menu

Select the level of the <platform> releases to view/download
[1-3,b,q,?]
```

5 Select the number corresponding to the type of release you want to view (Base, Maintenance, or Patch).

You see a list of releases available for download.

```
Available Maintenance releases for aix71:

release_version SORT_release_name       DL OBS AI rel_date   size_KB
=====================================================================
5.1SP1PR1RP2    sfha-aix-5.1SP1PR1RP2   -  Y   Y  2011-09-28 288760
5.1SP1PR1RP3    sfha-aix71-5.1SP1PR1RP3 Y  Y   Y  2012-10-02 290321
5.1SP1PR1RP4    sfha-aix71-5.1SP1PR1RP4 -  -   Y  2013-08-21 304300
6.0RP1          sfha-aix-6.0RP1         -  -   Y  2012-03-22 293980
6.0.3           sfha-aix-6.0.3          -  -   Y  2013-01-31 294041
```

```
Enter the release_version to view details about a release or press 'Enter' to continue [b,q,?]
```

The following are the descriptions for the column headers:

- release_version: The version of the release.
- SORT_release_name: The name of the release, used when accessing SORT (https://sort.symantec.com).
- DL: An indicator that the release is present in your repository.
- OBS: An indicator that the release is obsolete by another higher release.
- AI: An indicator that the release has scripted install capabilities. All base and maintenance releases have auto-install capabilities. Patch releases with auto-install capabilities are available beginning with version 6.1. Otherwise the patch requires a manual installation.
- rel_date: The date the release is available.
- size_KB: The file size of the release in kilobytes.

6 If you are interested in viewing more details about any release, type the release version. For example, enter the following:

```
6.0.3
```

You see the following output:

```
release_version: 6.0.3
release_name: sfha-aix-6.0.3
release_type: MR
release_date: 2013-01-31
install_path: aix/installmr
upload_location: ftp://ftp.veritas.com/pub/support/patchcentral
/AIX/6.0.3/sfha/sfha-aix-6.0.3-patches.tar.gz
obsoletes: 6.0.1.200-fs,6.0.1.200-vm
obsoleted_by: None

Would you like to download this Maintenance Release? [y,n,q] (y) n

Enter the release_version to view the details about a release or press
'Enter' to continue [b,q,?]
```

7 If you do not need to check detail information, you can press **Enter**.

You see the following question:

```
Would you like to download a aix Maintenance Release Image?
[y,n,q] (n) y
```

If you select a **y**, you see a menu of all releases that are not currently in the repository.

```
    1)  5.1SP1PR1RP2
    2)  5.1SP1PR1RP4
    3)  6.0RP1
    4)  All non-obsoleted releases
    5)  All releases
    b)  Back to previous menu

Select the patch release to download, 'All non-obsoleted releases' to
download all non-obsoleted releases, or 'All releases' to download
all releases [1-5,b,q] 3
```

8 Select the number corresponding to the release that you want to download. You can download a single release, all non-obsoleted releases, or all releases.

The selected release images are downloaded to the Deployment Server.

```
Downloading sfha-aix-6.0RP1 from SORT - https://sort.symantec.com
Downloading 215118373 bytes (Total 215118373 bytes [205.15 MB]): 100%
Untarring sfha-aix-6.0RP1 ..................................................... Done

sfha-aix-6.0RP1 has been downloaded successfully.
```

9 From the menu, select option **2**, **View/Remove Repository Images**, and follow the prompts to check that the release images are loaded.

See "Viewing or downloading available release images" on page 75.

Viewing or removing repository images stored in your repository

You can use the Deployment Server to conveniently view or remove the release images that are stored in your repository.

To view or remove release images stored in your repository

1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

```
Task Menu:

R) Manage Repository Images              M) Update Metadata
V) Version Check Systems                 S) Set Preferences
I) Install/Upgrade Systems               U) Terminology and Usage
B) Define/Modify Install Bundles         ?) Help
T) Create Install Templates              Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

2 Select option **R**, **Manage Repository Images**.

You see the following output:

```
1)  View/Download Available Releases
2)  View/Remove Repository Images
3)  Load a Release Image
b)  Back to previous menu

Select the option you would like to perform [1-3,b,q,?]
```

3 Select option **2**, **View/Remove Repository Images**, to view or remove the release images currently installed on your system.

You see a list of platforms and release levels if you have downloaded the corresponding Base, Maintenance, or Patch release on that platform.

```
To view or remove repository images, the platform type and
release level type must be selected.

1)  AIX 5.3                   2)  AIX 6.1
3)  AIX 7.1                   4)  HP-UX 11.31
5)  RHEL5 x86_64              6)  RHEL6 x86_64
7)  RHEL7 x86_64              8)  SLES10 x86_64
9)  SLES11 x86_64             10) Solaris 9 Sparc
11) Solaris 10 Sparc          12) Solaris 10 x64
13) Solaris 11 Sparc          14) Solaris 11 x64
b)  Back to previous menu

Select the platform of the release to view/remove [1-14,b,q]
```

4 Select the release level for which you want to get release image information. Enter the platform you want.

You see options for the Symantec release levels if you have downloaded the corresponding Base, Maintenance, or Patch release.

```
1) Base
2) Maintenance
3) Patch
b) Back to previous menu

Select the level of the <platform> releases to view/remove
[1-3,b,q]
```

5 Select the number corresponding to the type of release you want to view or remove (Base, Maintenance, or Patch).

You see a list of releases that are stored in your repository.

```
Stored Repository Releases:

release_version SORT_release_name        OBS AI
================================================
6.0RP1          sfha-aix-6.0RP1           -   Y
6.0.3           sfha-aix-6.0.3            -   Y
```

6 If you are interested in viewing more details about a release image that is stored in your repository, type the release version. For example, enter the following:

```
6.0.3
```

7 If you do not need to check detail information, you can press **Enter**.

You see the following question:

```
Would you like to remove a aix61 Maintenance Release Image?
[y,n,q] (n) y
```

If you select a **y**, you see a menu of all the releases that are stored in your repository that match the selected platform and release level.

```
1)  6.0RP1
2)  6.0.3
b)  Back to previous menu

Select the patch release to remove [1-2,b,q] 1
```

8 Type the number corresponding to the release version you want to remove.

The release images are removed from the Deployment Server.

```
Removing sfha-aix-6.0RP1-patches ........................... Done
sfha-aix-6.0RP1-patches has been removed successfully.
```

Deploying Symantec product updates to your environment

You can use the Deployment Server to deploy release images to the systems in your environment as follows:

- If you are not sure what to deploy, perform a version check. A version check tells you if there are any Symantec products installed on your systems. It suggests patches and maintenance releases, and gives you the option to install updates.
  See "Finding out which releases you have installed, and which upgrades or updates you may need" on page 83.

- If you know which update you want to deploy on your systems, use the Install/Upgrade Systems script to deploy a specific Symantec release.
  See "Deploying Symantec releases" on page 92.

Finding out which releases you have installed, and which upgrades or updates you may need

Use the Version Check option to determine which Symantec product you need to deploy. The Version Check option is useful if you are not sure which releases you already have installed, or you want to know about available releases.

The Version Check option gives you the following information:

- Installed products and their versions (base, maintenance releases, and patches)
- Installed filesets (required and optional)
- Available releases (base, maintenance releases, and patches) relative to the version which is installed on the system

To determine which Symantec product updates to deploy

1 Launch the Deployment Server. For example, enter the following:

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

```
Task Menu:

R) Manage Repository Images              M) Update Metadata
V) Version Check Systems                 S) Set Preferences
I) Install/Upgrade Systems               U) Terminology and Usage
B) Define/Modify Install Bundles         ?) Help
T) Create Install Templates              Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

2 Select option **V**, **Version Check Systems**.

3 At the prompt, enter the system names for the systems you want to check. For example, enter the following:

```
sys1
```

You see output for the installed filesets (required, optional, or missing).

You see a list of releases available for download.

```
Available Base Releases for Veritas Storage Foundation HA 6.0.1:
None

Available Maintenance Releases for Veritas Storage Foundation HA 6.0.1:

release_version SORT_release_name     DL OBS AI rel_date   size_KB
================================================================
6.0.3           sfha-aix-6.0.3        Y  -   -  2013-02-01 212507

Available Public Patches for Veritas Storage Foundation HA 6.0.1:

release_version SORT_release_name      DL OBS AI rel_date   size_KB
================================================================
6.0.1.200-fs    fs-aix-6.0.1.200       -  Y   -  2012-09-20 14346
6.0.1.200-vm    vm-aix-6.0.1.200       -  Y   -  2012-10-10 47880

Would you like to download the available Maintenance or Public Patch
releases which cannot be found in the repository? [y,n,q] (n) y
```

4 If you want to download any of the available maintenance releases or patches, enter **y**.

5 If you have not set a default repository for releases you download, the installer prompts you for a directory. (You can also set the default repository in **Set Preferences**).

See "Setting deployment preferences" on page 71.

6 Select an option for downloading products.

The installer downloads the releases you specified and stores them in the repository.

Defining Install Bundles

You can use Install Bundles to directly install the latest base, maintenance, and patch releases on your system. Install Bundles are a combination of base,

maintenance, and patch releases that can be bundled and installed or upgraded in one operation.

Note: Install Bundles can be defined only from version 6.1 or later. The exception to this rule is base releases 6.0.1, 6.0.2, or 6.0.4 or later and maintenance release 6.0.5 or later.

To define Install Bundles

1 Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

```
Task Menu:

R) Manage Repository Images             M) Update Metadata
V) Version Check Systems                S) Set Preferences
I) Install/Upgrade Systems              U) Terminology and Usage
B) Define/Modify Install Bundles        ?) Help
T) Create Install Templates             Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

2 Select option **B**, **Define/Modify Install Bundles**.

You see the following output:

```
Select a Task:

     1)  Create a new Install Bundle
     2)  Modify an Install Bundle
     3)  Delete an Install Bundle
     b)  Back to previous menu

Select the task you would like to perform [1-3,b,q]
```

3 Select option **1**, **Create a new Install Bundle**.

You see the following output:

```
Enter the name of the Install Bundle you would like to define:
{press [Enter] to go back)
```

For example, if you entered:

```
rhel605
```

You see the following output:

```
To create an Install Bundle, the platform type must be selected:

     1)  AIX 5.3                    2)  AIX 6.1
     3)  AIX 7.1                    4)  HP-UX 11.31
     5)  RHEL5 x86_64               6)  RHEL6 x86_64
     7)  RHEL7 x86_64               8)  SLES10 x86_64
     9)  SLES11 x86_64              10) Solaris 9 Sparc
     11) Solaris 10 Sparc           12) Solaris 10 x64
     13) Solaris 11 Sparc           14) Solaris 11 x64
     b)  Back to previous menu


Select the platform of the release for the Install Bundle rhel605:
[1-14,b,q]
```

4 Select the number corresponding to the platform you want to include in the Install Bundle. For example, select the number for the **RHEL5 x86_64** release, **5**.

You see the following output:

```
Details of the Install Bundle: rhel605

Install Bundle Name    rhel605
Platform               RHEL5 x86_64
Base Release           N/A
Maintenance Release    N/A
Patch Releases         N/A

     1)  Add a Base Release
     2)  Add a Maintenance Release
     3)  Add a Patch Release
     4)  Change Install Bundle Name
     b)  Back to previous menu

Select an action to perform on the Install Bundle rhel605 [1-4,b,q]
```

5 Select option **1**, **Add a Base Release**.

You see the following output:

```
     1)  6.0.1
     2)  6.0.2
     3)  6.1
     b)  Back to previous menu

Select the Base Release version to add to the Install Bundle rhel605
[1-3,b,q]
```

6 Select option **1**, **6.0.1**.

You see the following output:

```
Symantec Storage Foundation and High Availability Solutions 6.2 Deployment Server Program
                    pilotlnx11

Details of the Install Bundle: rhel605

Install Bundle Name    rhel605
Platform               RHEL5 x86_64
Base Release           6.0.1
Maintenance Release    N/A
Patch Releases         N/A

     1)  Remove Base Release 6.0.1
     2)  Add a Maintenance Release
     3)  Add a Patch Release
     4)  Change Install Bundle Name
     b)  Back to previous menu

Select an action to perform on the Install Bundle rhel605 [1-4,b,q]
```

7 Select option **2**, **Add a Maintenance Release**.

You see the following output:

```
     1)  6.0.5
     b)  Back to previous menu

Select the Maintenance Release version to add to the Install Bundle
rhel605 [1-1,b,q]
```

8 Select option **1**, **6.0.5**.

You see the following output:

```
Symantec Storage Foundation and High Availability Solutions 6.2 Deployment Server Program
                                  pilotlnx11

Details of the Install Bundle: rhel605

Install Bundle Name    rhel605
Platform               RHEL5 x86_64
Base Release           6.0.1
Maintenance Release    6.0.5
Patch Releases         N/A

     1)  Remove Base Release 6.0.1
     2)  Remove Maintenance Release 6.0.5
     3)  Add a Patch Release
     4)  Save Install Bundle rhel605
     5)  Change Install Bundle Name
     b)  Back to previous menu

Select an action to perform on the Install Bundle rhel605
[1-5,b,q]
```

9 Select option **4**, **Save Install Bundle**.

You see the following output:

```
Install Bundle rhel605 has been saved successfully

Press [Enter] to continue:
```

If there are no releases for the option you selected, you see a prompt saying that there are no releases at this time. You are prompted to continue.

After selecting the desired base, maintenance, or patch releases, you can choose to save your Install Bundle.

The specified Install Bundle is saved on your system. The specified Install Bundle is available as an installation option when using the **I) Install/Upgrade Systems** option to perform an installation or upgrade.

Creating Install Templates

You can use Install Templates to discover installed components (filesets, patches, products, or versions) on a system that you want to replicate. Use Install Templates to automatically install those same components on to other systems.

To create Install Templates

1. Launch the Deployment Server.

```
# /opt/VRTS/install/deploy_sfha
```

2. You see the following output:

```
Task Menu:

R) Manage Repository Images              M) Update Metadata
V) Version Check Systems                 S) Set Preferences
I) Install/Upgrade Systems               U) Terminology and Usage
B) Define/Modify Install Bundles         ?) Help
T) Create Install Templates              Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

3. Select option **T**, **Create Install Templates**.
4. You see the following output:

```
Select a Task:

     1)  Create a new Install Template
     2)  View Install Templates
     3)  Delete an Install Template
     b)  Back to previous menu

Select the task you would like to perform [1-3,b,q]
```

5 Select option **1**, **Create a new Install Template**.

You see the following output:

```
Enter the system names separated by spaces for creating an Install Template:
(press [Enter] to go back)
```

For example, if you entered **rhel89202** as the system name, you see the following output:

```
Enter the system names separated by spaces for version checking: rhel89202

Checking communication on rhel89202 ..... Done
Checking installed products on rhel89202 ..... Done

Platform of rhel89202:
   Linux RHEL 6.3 x86_64

Installed product(s) on rhel89202:
   Symantec Storage Foundation Cluster File System HA - 6.1.1 - license vxkeyless

Product:
   Symantec Storage Foundation Cluster File System HA - 6.1.1 - license vxkeyless

Packages:
   Installed Required packages for Symantec Storage Foundation Cluster File System HA 6.1.1:
          #PACKAGE     #VERSION
          VRTSamf      6.1.1.000
          VRTSaslapm   6.1.1.000
          ..........   .........
          ..........   .........
          VRTSvxfs     6.1.1.000
          VRTSvxvm     6.1.1.000

   Installed optional packages for Symantec Storage Foundation Cluster File System HA 6.1.1:
          #PACKAGE     #VERSION
          VRTSdbed     6.1.1.000
          VRTSgms      6.1.0.000
          ..........   .........
          ..........   .........
          VRTSvcsdr    6.1.0.000
          VRTSvcsea    6.1.1.000

   Missing optional packages for Symantec Storage Foundation Cluster File System HA 6.1.1:
          #PACKAGE
```

```
          VRTScps
          VRTSfssdk
          VRTSlvmconv

Summary:

Packages:
 17 of 17 required Symantec Storage Foundation Cluster File System HA 6.1.1 packages installed
 8 of 11 optional Symantec Storage Foundation Cluster File System HA 6.1.1 packages installed

Installed Public and Private Hot Fixes for Symantec Storage Foundation Cluster File
System HA 6.1.1:
 None

Would you like to generate a template file based on the above release information? [y,n,q] (y)

 1)  rhel89202
 b)  Back to previous menu

Select a machine list to generate the template file [1-1,b,q]
```

6 Select option **1**, **rhel89202**.

You see the following output:

```
Enter the name of the Install Template you would like to define:
(press [Enter] to go back)
```

7 Enter the name of your Install Template. For example, if you enter **MyTemplate** as the name for your Install Template, you would see the following:

```
Install Template MyTemplate has been saved successfully

Press [Enter] to continue:
```

All of the necessary information is stored in the Install Template you created.

Deploying Symantec releases

You can use the Deployment Server to deploy your licensed Symantec products dating back to version 5.1. If you know which product version you want to install, follow the steps in this section to install it.

You can use the Deployment Server to install the following:

- A single Symantec release
- Two or more releases using defined Install Bundles
  See "Defining Install Bundles" on page 84.
- Installed components on a system that you want to replicate on another system
  See "Creating Install Templates" on page 90.

To deploy a specific Symantec release

1 From the directory in which you installed your Symantec product (version 6.1 or later), launch the Deployment Server with the upgrade and install systems option. For example, enter the following:

```
# /opt/VRTS/install/deploy_sfha
```

You see the following output:

```
Task Menu:

R) Manage Repository Images              M) Update Metadata
V) Version Check Systems                 S) Set Preferences
I) Install/Upgrade Systems               U) Terminology and Usage
B) Define/Modify Install Bundles         ?) Help
T) Create Install Templates              Q) Quit

Enter a Task: [R,M,V,S,I,U,B,?,T,Q]
```

2 Select option **I**, **Install/Upgrade Systems**.

You see the following output:

```
    1)  AIX 5.3
    2)  AIX 6.1
    3)  AIX 7.1
    4)  RHEL5 x86_64
    b)  Back to previous menu

Select the platform of the available release(s) to be
upgraded/installed [1-4,b,q,?]
```

3 Select the number corresponding to the platform for the release you want to deploy. For example, select the number for the **RHEL5 x86_64** release or the **AIX 6.1** release.

You see the following output:

```
1) Install/Upgrade systems using a single release
2) Install/Upgrade systems using an Install Bundle
3) Install systems using an Install Template
b) Back to previous menu

Select the method by which you want to Install/Upgrade your systems
[1-3,b,q]
```

4 Section option **1**, **Install/Upgrade systems using a single release** if you want to deploy a specific Symantec release.

Select a Symantec product release.

The installation script is executed and the release is deployed on the specified server.

To deploy an Install Bundle

1 Follow Steps 1 - 3.

2 Select option **2**, **Install/Upgrade systems using an Install Bundle**.

You see the following output:

```
1) <NameofInstallBundle1>
2) <NameofInstallBundle2>
b) Back to previous menu

Select the bundle to be installed/upgraded [1-2,b,q]
```

You see the following output:

```
Enter the platform target system name(s) separated by spaces:
[press [Enter] to go back)
```

3 Enter the name of the target system for which you want to install or upgrade the Install Bundle.

The installation script for the selected Install Bundle is executed, and the Install Bundle is deployed on the specified target system.

To deploy an Install Template

1. Follow Steps 1 - 3.
2. Select option **3**, **Install/Upgrade systems using an Install Template**.

   You see the following output:

   ```
   1) <NameofInstallTemplate>
   b) Back to previous menu

   Select the template to be installed [1-1,b,q] 1
   ```

   You see the following output:

   ```
   Enter the platform target system name(s) separated by spaces:
   [press [Enter] to go back)
   ```

   The installation script for the selected Install Template is executed, and the Install Template is deployed on the specified target system.

Connecting the Deployment Server to SORT using a proxy server

You can use a proxy server, a server that acts as an intermediary for requests from clients, for connecting the Deployment Server to the Symantec Operations Readiness Tools (SORT) website.

To set up a proxy server

1. Set up a Red Hat Enterprise Linux 5 system, for example, 10.198.95.231, as a proxy server.
2. Install a squid proxy server by entering the following:
3. Change the squid configuration file, `/etc/squid/squid.conf`, to allow for connections from other computers by entering the following:

   ```
   # vim /etc/squid/squid.conf
   ```

4. Change the line `http_access deny all` to `http_access allow all`.
5. Restart the squid service by entering the following:

   ```
   # service squid restart
   ```

To set up a proxy client

1. Use another system, for example, 10.198.95.232, as the proxy client.
2. First disable Domain Name System (DNS) on this system by commenting out the `nameserver` entry in the `/etc/resolv.conf` file.

```
# cat /etc/resolv.conf
search cdc.veritas.com
#nameserver 10.198.88.18

# ping ftp.symantectest.com
ping: unknown host ftp.symantectest.com
```

Section 4

Post-installation tasks

- Chapter 11. Verifying the DMP installation

Chapter 11

Verifying the DMP installation

This chapter includes the following topics:

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

Verifying that the products were installed

Verify that the DMP products are installed.

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

```
# lslpp -L | grep VRTS
```

The filesets should be in the COMMITTED state, as indicated by a C in the output:

```
root@dbaix1-v3:[/] # lslpp -L | grep VRTSaslapm

VRTSaslapm    6.2.0.0  C  F   Array Support Libraries...
```

See "Symantec Dynamic Multi-Pathing installation filesets" on page 162.

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

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

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

See "About the script-based installer" on page 37.

Use the following sections to further verify the product installation.

Installation log files

The Symantec 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 the commands that are executed during the procedure, their output, and the errors that are generated. This file is for debugging installation problems and can be used for analysis by Symantec 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. See "Installing DMP using response files" on page 50.
Summary file	The summary file contains the results of the installation by the common product installer or product installation scripts. The summary includes the list of the filesets, and the status (success or failure) of each fileset. The summary also indicates which processes were stopped or restarted during the installation. After installation, refer to the summary file to determine whether any processes need to be started.

Starting and stopping processes for the Symantec products

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

To stop the processes

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

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

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

  or

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

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

  See "About the script-based installer" on page 37.

To start the processes

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

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

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

  or

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

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

  See "About the script-based installer" on page 37.

Section 5

Upgrade of DMP

- Chapter 12. Planning to upgrade DMP
- Chapter 13. Upgrading DMP
- Chapter 14. Upgrading DMP using an alternate disk
- Chapter 15. Upgrading DMP using Network Install Manager Alternate Disk Migration
- Chapter 16. Performing post-upgrade tasks

Chapter 12

Planning to upgrade DMP

This chapter includes the following topics:

- Upgrade methods for DMP
- Supported upgrade paths for DMP
- Preparing to upgrade DMP
- Using Install Bundles to simultaneously install or upgrade base releases, maintenance releases, and patches

Upgrade methods for DMP

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

Table 12-1 Review this table to determine how you want to perform the upgrade

Upgrade types and considerations	Methods available for upgrade
Typical upgrades—use a Symantec provided tool or you can perform the upgrade manually. Requires some server downtime.	Script-based—you can use this method to upgrade for the supported upgrade paths Web-based—you can use this method to upgrade for the supported upgrade paths Manual—you can use this method to upgrade from the previous release Response file—you can use this method to upgrade from the supported upgrade paths

Table 12-1 Review this table to determine how you want to perform the upgrade *(continued)*

Upgrade types and considerations	Methods available for upgrade
Native operating system upgrade—use the upgrade software that comes with the operating system. Note that not all operating systems support native upgrades.	Operating system-specific methods Operating system upgrades
Upgrade from any supported UNIX or Linux platform to any other supported UNIX or Linux platform.	Deployment Server See "About the Deployment Server" on page 65.
Simultaneously upgrade base releases, maintenance patches, and patches.	Install Bundles See "Using Install Bundles to simultaneously install or upgrade base releases, maintenance releases, and patches" on page 107.

Supported upgrade paths for DMP

The following tables describe upgrading to 6.2.

Table 12-2 AIX upgrades using the script- or web-based installer

Symantec software version	5.3	6.1 (TL6, TL7, TL8, TL9)	7.1 (TL0, TL1, TL2, TL3)
5.1 5.1 RPs 5.1SP1 5.1 SP1RP1	Upgrade the operating system to 6.1 TL6 or later - but do not upgrade to 7.1. Use the installer to upgrade your Symantec product to 6.2.	Upgrade the operating system to 6.1 TL6 or later - but do not upgrade to 7.1. Use the installer to upgrade your Symantec product to 6.2.	N/A
5.1 SP1RP2 5.1 SP1RP3 5.1 SP1RP4	Upgrade the operating system to 6.1 TL6 or later - but do not upgrade to 7.1. Use the installer to upgrade your Symantec product to 6.2.	Upgrade the operating system to 6.1 TL6 or later - but do not upgrade to 7.1. Use the installer to upgrade your Symantec product to 6.2.	Use the installer to upgrade your Symantec Product to 6.2.

Table 12-2 AIX upgrades using the script- or web-based installer *(continued)*

Symantec software version	5.3	6.1 (TL6, TL7, TL8, TL9)	7.1 (TL0, TL1, TL2, TL3)
5.1 SP1 PR1	N/A	N/A	Use the installer to upgrade your Symantec Product to 6.2.
6.0 6.0 RPs 6.0.1 6.0.3 6.0.5 6.1 6.1.1	N/A	Upgrade the operating system to 6.1 TL6 or later. Use the installer to upgrade your Symantec product to 6.2	Use the installer to upgrade your Symantec Product to 6.2.
No Symantec product	N/A	Perform a full 6.2 installation using the installer script.	Perform a full 6.2 installation using the installer script.

Preparing to upgrade DMP

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

Getting ready for the upgrade

Complete the following tasks before you perform the upgrade:

- Review the Symantec Technical Support website for additional information: http://www.symantec.com/techsupp/
- Make sure that the administrator who performs the upgrade has root access and a good knowledge of the operating system's administration.
- Make sure that all users are logged off and that all major user applications are properly shut down.
- Make sure that you have created a valid backup.
  See "Creating backups" on page 106.
- Ensure that you have enough file system space to upgrade. Identify where you want to copy the filesets, for example `/packages/Veritas` when the root file

system has enough space or `/var/tmp/packages` if the `/var` file system has enough space.

Do not put the files under `/tmp`, which is erased during a system restart. Do not put the files on a file system that is inaccessible before running the upgrade script.

You can use a Symantec-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/init.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 6.2 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 Symantec products. Depending on the configuration, the outage can take several hours.
- Make sure that the file systems are clean before upgrading.
- Upgrade arrays (if required).
  See "Upgrading the array support" on page 106.
- 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.
- If CP server-based coordination points are used in your current fencing configuration, then check that your CP servers are upgraded to 6.2 before starting the upgrade process.
- Make sure that DMP support for native stack is disabled (`dmp_native_support=off`). If DMP support for native stack is enabled (`dmp_native_support=on`), the installer may detect it and ask you to restart the system.

Preparing for an upgrade of Symantec Dynamic Multi-Pathing

Before you upgrade, perform the following procedure.

To prepare for an upgrade of Symantec Dynamic Multi-Pathing

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

   ```
   # umount mnt_point
   ```

3 Stop all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

4 Upgrade AIX on your system to the required levels if applicable.

Creating backups

Save relevant system information before the upgrade.

To create backups

1 Log in as superuser.

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

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

If not, a warning message is displayed.

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

---

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

Upgrading the array support

The Storage Foundation 6.2 release includes all array support in a single fileset, `VRTSaslapm`. The array support fileset includes the array support previously included in the `VRTSvxvm` fileset. The array support fileset also includes support previously packaged as external Array Support Libraries (ASLs) and array policy modules (APMs).

See the 6.2 Hardware Compatibility List for information about supported arrays.

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

After you have installed Storage Foundation 6.2, Symantec provides support for new disk arrays through updates to the `VRTSaslapm` fileset.

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

Using Install Bundles to simultaneously install or upgrade base releases, maintenance releases, and patches

Beginning with version 6.1, Symantec offers you a method to easily install or upgrade your systems directly to a base, maintenance, or patch level in one step using Install Bundles. With Install Bundles, the installers have the ability to merge so that customers can install or upgrade directly to maintenance or patch levels in one execution. The various scripts, filesets, and patch components are merged, and multiple releases are installed together as if they are one combined release. You do not have to perform two or more install actions to install or upgrade systems to maintenance levels or patch levels.

Releases are divided into the following categories:

Table 12-3 Release Levels

Level	Content	Form factor	Applies to	Release types	Download location
Base	Features	filesets	All products	Major, minor, Service Pack (SP), Platform Release (PR)	FileConnect
Maintenance	Fixes, new features	filesets	All products	Maintenance Release (MR), Rolling Patch (RP)	Symantec Operations Readiness Tools (SORT)
Patch	Fixes	filesets	Single product	P-Patch, Private Patch, Public patch	SORT, Support site

When you install or upgrade using Install Bundles:

- SFHA products are discovered and assigned as a single version to the maintenance level. Each system can also have one or more patches applied.
- Base releases are accessible from FileConnect that requires customer serial numbers. Maintenance and patch releases can be automatically downloaded

from SORT. You can download them from the SORT website manually or use the `deploy_sfha` script.

- Patch releases can be installed using automated installers from the 6.1 version or later.
- Patches can now be detected to prevent upgrade conflict. Patch releases are not offered as a combined release. They are only available from Symantec Technical Support on a need basis.

You can use the `-base_path` and `-patch_path` options to import installation code from multiple releases. You can find filesets and patches from different media paths, and merge fileset and patch definitions for multiple releases. You can use these options to use new task and phase functionality to correctly perform required operations for each release component. You can install the filesets and patches in defined phases using these options, which helps you when you want to perform a single start or stop process and perform pre and post operations for all level in a single operation.

Four possible methods of integration exist. All commands must be executed from the highest base or maintenance level install script.

For example:

1. Base + maintenance:

   This integration method can be used when you install or upgrade from a lower version to 6.2.1.

   Enter the following command:

   ```
   # installmr -base_path <path_to_base>
   ```

2. Base + patch:

   This integration method can be used when you install or upgrade from a lower version to 6.2.0.100.

   Enter the following command:

   ```
   # installer -patch_path <path_to_patch>
   ```

3. Maintenance + patch:

   This integration method can be used when you upgrade from version 6.2 to 6.2.1.100.

   Enter the following command:

   ```
   # installmr -patch_path <path_to_patch>
   ```

4. Base + maintenance + patch:

   This integration method can be used when you install or upgrade from a lower version to 6.2.1.100.

   Enter the following command:

   ```
   # installmr -base_path <path_to_base>
   -patch_path <path_to_patch>
   ```

   Note: From the 6.1 or later release, you can add a maximum of five patches using *-patch_path <path_to_patch> -patch2_path <path_to_patch> ... -patch5_path <path_to_patch>*

Chapter 13

Upgrading DMP

This chapter includes the following topics:

- Upgrading Symantec Dynamic Multi-Pathing with the product installer
- Upgrading DMP using the web-based installer
- Upgrade Symantec Dynamic Multi-Pathing and AIX on a DMP-enabled rootvg
- Upgrading DMP on a Virtual I/O server (VIOS) from 5.1SP1 or later to 6.2
- Upgrading the AIX operating system

Upgrading Symantec Dynamic Multi-Pathing with the product installer

This section describes upgrading from Symantec Dynamic Multi-Pathing products to 6.2.

To upgrade Symantec Dynamic Multi-Pathing

1. Log in as superuser.
2. Load and mount the disc. If you downloaded the software, navigate to the top level of the download directory.
3. From the disc, run the `installer` command. If you downloaded the software, run the `./installer` command.

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

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

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

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

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

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

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

8 Stop the product's processes.

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

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

9 The installer stops, uninstalls, reinstalls, and starts specified filesets.

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

```
CPI WARNING V-9-40-5323 DMP license version 5.0 is not
updated to 6.2 on sys1. It's recommended to upgrade to a 6.2 key.
CPI WARNING V-9-40-5323 DMP license version 5.0 is not updated
to 6.2 on sys2. It's recommended to upgrade to a 6.2 key.
DMP is licensed on the systems.
Do you wish to enter additional licenses? [y,n,q,b] (n) n
```

11 The Symantec 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 Restart the systems if the installer prompts restart to enable DMP native support.

Upgrading DMP using the web-based installer

This section describes upgrading DMP with the 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 want to preserve. For example, make configuration file backups.
2. Start the web-based installer.

   See "Starting the web-based installer" on page 44.
3. On the Select a task and a product page, select **Upgrade a Product** from the Task drop-down menu.

   The product is discovered once you specify the system. Click **Next**.
4. Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click **Next**.
5. Installer detects the product that is installed on the specified system. It shows the cluster information and lets you confirm if you want to perform upgrade on the cluster. Select **Yes** and click **Next**.
6. 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.
7. If you have enabled security on the cluster, the installer displays the following question:

   Do you want to grant read access to everyone? [y,n,q,?]

   - To grant read access to all authenticated users, enter **y**.
   - To grant read access to specific user groups, enter **n** and then enter the user group names separated by spaces, such as **usergroup** or **usergroup@FQHN**.
     For example:

```
Enter the usergroup names separated by
spaces that you would like to grant read
access: [b] usergroup, usergroup@hostname.cdc.symantec.com
```

8. If you are prompted to restart the systems, enter the following restart command:

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

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

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

Table 13-1 Upgrade paths for DMP on a DMP-enabled rootvg

Upgrade path	Procedure
DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.2	See "Upgrading from DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.2 on a DMP-enabled rootvg" on page 113.
DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.2 on AIX 6.1/ 7.1	See "Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.2 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg" on page 114.

Upgrading from DMP 5.1SP1 (or later) on AIX 6.1 to DMP 6.2 on a DMP-enabled rootvg

When you upgrade from a previous version of DMP on a DMP-enabled rootvg to DMP 6.2, you must disable DMP root support before performing the upgrade. Enable the DMP root support after the upgrade. If the AIX version is less than 6.1, an operating system upgrade is required.

See "Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.2 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg" on page 114.

To upgrade from DMP 5.1SP1 or later to DMP 6.2 on a DMP-enabled rootvg

1. Disable DMP support for the rootvg:

```
# vxdmpadm native disable vgname=rootvg
Please reboot the system to disable DMP support for LVM
bootability
```

2. Restart the system.
3. Upgrade DMP to 6.2.

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

   See "Upgrading Symantec Dynamic Multi-Pathing with the product installer" on page 110.
4. Restart the system.

5 Enable DMP for rootvg.

```
# vxdmpadm native enable vgname=rootvg
Please reboot the system to enable DMP support for LVM bootability
```

6 Restart the system. After the restart, the system has DMP root support enabled.

Upgrading from DMP 5.1SP1 (or later) on AIX 5.3 to DMP 6.2 on AIX 6.1 or AIX 7.1 on a DMP-enabled rootvg

DMP 6.2 requires at least AIX 6.1. When you upgrade DMP from a previous version on a system that uses AIX 5.3, you must also upgrade the AIX operating system. If the rootvg is enabled for DMP, follow these steps.

To upgrade from DMP 5.1SP1 or later to DMP 6.2 on a DMP-enabled rootvg

1 Disable DMP support for the rootvg:

```
# vxdmpadm native disable vgname=rootvg
Please reboot the system to disable DMP support for LVM
bootability
```

2 Upgrade the AIX operating system from 5.3 to 6.1 before restarting.

3 Restart the system.

4 Upgrade DMP to 6.2.

See "Upgrading Symantec Dynamic Multi-Pathing with the product installer" on page 110.

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

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

5 Enable DMP for `rootvg`.

```
# vxdmpadm native enable vgname=rootvg
Please reboot the system to enable DMP support for LVM
bootability
```

6 Restart the system. After the restart, the system has DMP root support enabled.

Upgrading DMP on a Virtual I/O server (VIOS) from 5.1SP1 or later to 6.2

This section provides the instructions to upgrade DMP on a Virtual I/O server (VIOS) from 5.1SP1 or later to 6.2.

To upgrade DMP on VIOS

1. Shut down all Virtual I/O clients not having a failover capability, and only dependent on the Virtual I/O server being upgraded.
2. Disable DMP support for the `rootvg`:

   ```
   # vxdmpadm native disable vgname=rootvg
   Please reboot the system to disable DMP support for LVM
   bootability
   ```

3. Restart the system.
4. Log in to the VIO Server partition.

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

   ```
   $ oem_setup_env
   ```

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

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

5. Unconfigure all virtual devices from all virtual adapters.

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

6. Follow the procedure to upgrade DMP on a Virtual I/O server.

   See “Upgrading Symantec Dynamic Multi-Pathing with the product installer” on page 110.

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

   ```
   # cfgmgr -p vhost0
   ```

8 Enable DMP for `rootvg`.

```
# vxdmpadm native enable vgname=rootvg
Please reboot the system to enable DMP support for LVM bootability
```

9 Restart the system. After the restart, the system has DMP root support enabled.

10 For all the Virtual I/O servers, repeat step 1 through step 5.

11 Restart all the Virtual I/O clients you had shut down, and verify the configuration.

Upgrading the AIX operating system

Use this procedure to upgrade the AIX operating system if DMP 6.2 is installed. You must upgrade to a version that DMP 6.2 supports.

To upgrade the AIX operating system

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

```
# vxdmpadm native release
```

2 Upgrade the AIX operating system. See the operating system documentation for more information.

3 Apply the necessary APARs.

4 Restart the system.

```
# shutdown -Fr
```

Chapter 14

Upgrading DMP using an alternate disk

This chapter includes the following topics:

- About upgrading DMP using an alternate disk
- Supported upgrade scenarios
- Supported upgrade paths for DMP using alternate disks
- Preparing to upgrade DMP on an alternate disk
- Upgrading DMP on an alternate disk
- Verifying the upgrade

About upgrading DMP using an alternate disk

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

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

Upgrading DMP on an alternate disk has the following advantages:

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

Supported upgrade scenarios

The following upgrade scenarios are supported on an alternate disk:

- Upgrading only DMP
  See " Upgrading DMP on an alternate disk" on page 120.
- Upgrading only the operating system (Technology Level (TL) and Service Pack (SP) releases)

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

- Upgrading the operating system (Technology Level (TL) and Service Pack (SP) releases) and DMP
  See " Upgrading DMP on an alternate disk" on page 120.

Supported upgrade paths for DMP using alternate disks

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

AIX version	Technology Level and Service Pack releases of AIX 6.1/ 7.1
DMP version	5.1 and later

Preparing to upgrade DMP on an alternate disk

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

To prepare to upgrade DMP on an alternate disk

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

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

   ```
   # lspv
   Output similar to the following displays:
   hdisk0          0009710fa9c79877    rootvg    active
   hdisk1          0009710f0b90db93    None
   ```

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

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

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

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

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

   where install_option is one of the following:

   -minpkgs: For installing the minimum set of filesets

   -recpkgs: For installing the recommended filesets

   -allpkgs: For installing all filesets

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

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

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

Upgrading DMP on an alternate disk

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

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

To upgrade DMP on an alternate disk

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

Manual

Run the following command:

```
# /usr/sbin/alt_disk_copy -I "acNgXY" -P "all" \
-l "/tmp/prod_name" -w "all" -d "hdisk1"
```

Where:

- -d indicates the name of the target disk on which you clone the primary disk.
- -l indicates the full path of the directory that contains the filesets to be upgraded
- -w indicates the list of DMP filesets that you want to upgrade on the alternate boot disk. The option `all` indicates that all the filesets that are contained in the directory you specified (using option -l) must be installed to the alternate boot disk.

Using SMIT interface

Start the SMIT menu and enter the required information at the prompts:

```
# smitty alt_clone
```

- Target disk to install: **hdisk1**
- Fileset(s) to install: **all**
- Directory or Device with images (full path of the directory that contains the filesets to be upgraded): **/tmp/prod_name**
- ACCEPT new license agreements? **yes**
- Set `bootlist` to boot from this disk on next restart**yes**

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

Note: DMP rootability-enabled systems require additional steps. For instructions, see the topic "Cloning an LVM `rootvg` that is enabled for DMP" in the *Symantec Dynamic Multi-Pathing Administrator's Guide*.

2 Verify that the alternate disk is created:

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

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

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

4 Restart all the nodes in the cluster. The boot environment on the alternate disk is activated when you restart the nodes.

```
# shutdown -r
```

5 Copy the product installation scripts to the alternate disk:

```
# /opt/VRTS/install/bin/UXRT<version>/add_install_scripts
```

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

See "About the script-based installer" on page 37.

The command copies the installation scripts and uninstallation scripts to the alternate disk.

6 Start all the processes and ports.

```
# ./installsf -start
```

7 Verify the upgrade.

See "Verifying the upgrade" on page 121.

Verifying the upgrade

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

To verify the upgrade

1 Verify that the alternate boot environment is active:

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

If there are multiple boot disks for rootvg, run the following command to verify the disk the system has booted from:

```
# bootlist -m normal -o
hdisk1 blv=hd5 pathid=0
```

2 Verify that the version of the upgraded filesets on the alternate boot disk is `6.2.0.0`.

Note: The `VRTSsfcpi60` fileset still exists on the alternate boot disk. You need to manually uninstall the fileset.

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

```
# oslevel -s
```

Chapter 15

Upgrading DMP using Network Install Manager Alternate Disk Migration

This chapter includes the following topics:

- Supported upgrade paths for DMP using NIM ADM
- Preparing to upgrade DMP and the operating system using the nimadm utility
- Preparing the installation bundle on the NIM server
- Upgrading DMP and the operating system using the nimadm utility
- Verifying the upgrade performed using the NIM ADM utility

Supported upgrade paths for DMP using NIM ADM

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

The supported upgrade paths are as follows:

AIX version	AIX 5.3
	AIX 6.1
	AIX 7.1
DMP version	5.1 SP1 and later

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

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

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

1. Make sure that the DMP installation media is available.
2. Check the status of the physical disks on each node in the cluster.

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

   ```
   # lspv
   Output similar to the following displays:
   hdisk0          0009710fa9c79877    rootvg    active
   hdisk1          0009710f0b90db93    None
   ```

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

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

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

Preparing the installation bundle on the NIM server

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

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

To prepare the installation bundle

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

   ```
   # lsnim |grep -i lpp_source
   LPP-7100-up2date resources lpp_source
   ```

3 Check that the NIM LPP_RESOURCE and corresponding SPOT are in healthy state before you start upgrade:

```
# nim -Fo check LPP-7100-up2date
# nim -Fo check SPOT-7100-up2date
```

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

```
# ./installdmp -nim LPP-7100-up2date
```

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

5 Enter a name for the bundle, for example *DMP62*.

6 Run the `lsnim -l` command to check that the installp_bundle resource is created successfully.

```
# lsnim -l DMP62
DMP62:
class = resources
type = installp_bundle
Rstate = ready for use
prev_state = unavailable for use
location = /opt/VRTS/nim/DMP62.bundle
alloc_count = 0
server = master
```

Upgrading DMP and the operating system using the `nimadm` utility

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

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

To upgrade DMP and the operating system using the nimadm utility

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

Manual

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

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

For example:

```
# nimadm -l LPP-7100-up2date -c node1 \
-s spot-7100-up2date -b dmp62 \
-d hdisk1 -Y
```

Where:

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

Using SMIT interface

Start the SMIT menu:

```
# smit nimadm
```

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

Enter the required information at the prompts:

- Target NIM Client: **sys1**
- NIM LPP_SOURCE resource: **LPP-7100-up2date**
- NIM SPOT resource: **SPOT-7100-up2date**
- Bundle name: **dmp62**
- Target disk(s) to install: **hdisk1**
- Phase to execute: **all**
- Set Client `bootlist` to alternate disk? **yes**
- ACCEPT new license agreements? **yes**

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

2 Verify that the alternate disk is created:

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

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

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

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

```
# shutdown -r
```

5 Verify the upgrade.

See "Verifying the upgrade" on page 121.

Note: If the operating system version is incorrect, and the `bos.txt.spell` and `bos.txt.tfs` filesets are missed, update these filesets manually through `nim 6.1TL7SPX lpp_source`.

```
# oslevel -rl 6100-07
Fileset              Actual Level        Recommended ML
-------------------------------------------------------------
bos.txt.spell        5.3.12.0            6.1.6.0
bos.txt.tfs          5.3.12.0            6.1.6.0
```

To update the `bos.txt.spell` fileset manually, do the following:

smitty nim >> Perform NIM Software Installation and Maintenance Tasks >> Install and Update Software >> Install Software >> Select corresponding LPP_SOURCE >> * Software to Install >> Select bos.txt.spell

Follow the same procedure for the `bos.txt.tfs` fileset.

Verifying the upgrade performed using the NIM ADM utility

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

To verify the upgrade using the NIM ADM utility

1 Verify that the alternate boot environment is active:

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

If there are multiple boot disks for rootvg, run the following command to verify the disk the system has booted from:

```
# bootlist -m normal -o
hdisk1 blv=hd5 pathid=0
```

2 Verify that the version of the upgraded filesets on the alternate boot disk is `6.2.0.0`.

Note: The `VRTSsfcpi61` fileset still exists on the alternate boot disk. You need to manually uninstall the fileset.

If you upgraded the operating system:

```
# oslevel -s
```

Chapter 16

Performing post-upgrade tasks

This chapter includes the following topics:

- Updating variables
- Verifying the Symantec Dynamic Multi-Pathing upgrade

Updating variables

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

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

Verifying the Symantec 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 98.

Section 6

Uninstallation of DMP

- Chapter 17. Uninstalling DMP

Chapter 17

Uninstalling DMP

This chapter includes the following topics:

- Uninstalling DMP
- Uninstalling DMP with the web-based installer
- Removing Storage Foundation products using SMIT

Uninstalling DMP

Use the following procedure to remove Symantec 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 155.

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

3. Run the `uninstalldmp` command.

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

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

   See "About the script-based installer" on page 37.

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

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

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

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

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

7 Restart all the nodes.

Uninstalling DMP with the web-based installer

This section describes how to uninstall using the 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 6.2 with a previous version of DMP.

To uninstall DMP

1 Perform the required steps to save any data that you want to preserve. For example, take backups of configuration files.

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

```
# vxdmpadm settune dmp_native_support=off
# reboot
```

3 Start the web-based installer.

See "Starting the web-based installer" on page 44.

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

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

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

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

8 Restart the systems if DMP native support is `on`, and the systems need a restart to disable DMP native support, if the step 2 is not already executed. Re-run the uninstallation after the restart.

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

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

Click **Next**.

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

12 Click **Finish**.

Most filesets have kernel components. To ensure their complete removal, a system restart is recommended after all the filesets have been removed.

Removing Storage Foundation products using SMIT

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

To remove the filesets using SMIT

1 Stop the following SFCFSHA modules: VCS, VxFEN, ODM, GAB, and LLT.

Run the following commands to stop the SFCFSHA modules:

```
# hastop -all
# /etc/methods/glmkextadm unload
# /etc/rc.d/rc2.d/s99odm stop
# /etc/methods/gmskextadm unload
# /etc/init.d/vxfen.rc stop
# /etc/init.d/gab.rc stop
# /etc/init.d/llt.rc stop
```

Run the following commands to check if all the modules have been stopped:

```
# gabconfig -a
# ltconfig
```

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

```
# vxdmpadm settune dmp_native_support=off
# reboot
```

3 Enter this command to invoke SMIT:

```
# smit
```

4 In SMIT, select **Software Installation and Maintenance** > **Software Maintenance and Utilities** > **Remove Installed Software**.

5 Under the **SOFTWARE name** menu, press F4 or Esc-4 to list all the software that is installed on the system.

6 Enter "/" for Find, type "VRTS" to find all Symantec filesets, and select the filesets that you want to remove.

7 Restart the system after removing all Storage Foundation filesets.

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

8 Depending on the choices that were made when Storage Foundation was originally installed, you may find that not all of the listed Storage Foundation filesets are installed on the system. You may also choose to remove the `VRTSvlic` licensing fileset unless some other Symantec software requires it.

Section 7

Installation reference

- Appendix A. Installation scripts
- Appendix B. Tunable files for installation
- Appendix C. Configuring the secure shell or the remote shell for communications
- Appendix D. DMP components
- Appendix E. Troubleshooting installation issues
- Appendix F. Compatibility issues when installing DMP with other products

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 [ sys1 sys2... ]
 [ -configure | -license | -upgrade | -precheck | -requirements
  | -start | -stop | -postcheck ]
 [-require installer_hot_fix_file ]
 [ -responsefile response_file ]
 [ -logpath log_path ]
 [ -tmppath tmp_path ]
 [ -tunablesfile tunables_file ]
 [ -timeout timeout_value ]
 [ -hostfile hostfile_path ]

 [ -keyfile ssh_key_file ]

 [ -prod product_name ]

 [ -hotfix_path hotfix_path ]
 [ -hotfix2_path hotfix2_path ]
 [ -hotfix3_path hotfix3_path ]
 [ -hotfix4_path hotfix4_path ]
 [ -hotfix5_path hotfix5_path ]

 [ -nim LLT_SOURCE ]
```

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

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

Table A-1 installdmp options

Option and Syntax	Description
`-allpkgs`	View a list of all DMP filesets and patches. The installdmp lists the filesets 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.
`-disable_dmp_native_support`	Disables Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools during upgrade. Retaining Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools during upgrade increases fileset upgrade time depending on the number of LUNs and native LVM volume groups and ZFS pools configured on the system.
`-hotfix_path`	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed .
`-hotfix2_path`	Defines the path of a second patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
`-hotfix3_path`	Defines the path of a third patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
`-hotfix4_path`	Defines the path of a fourth patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-hotfix5_path`	Defines the path of a fifth patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
`-hostfile` *`full_path_to_file`*	Specifies the location of a file that contains the system names for the installer.
`-installallpkgs`	Selects all the filesets for installation. See the `-allpkgs` option.
`-installminpkgs`	Selects the minimum filesets for installation. See the `-minpkgs` option.
`-installrecpkgs`	Selects the recommended filesets for installation. See the `-recpkgs` option.
`-keyfile` *`ssh_key_file`*	Specifies a key file for SSH. The option passes `-i` *`ssh_key_file`* with each SSH invocation.
`-license`	Register or update product licenses on the specified systems. This option is useful to replace a demo license.
`-logpath` *`log_path`*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where install log files, summary files, and response files are saved.
`-makeresponsefile`	Create a response file. This option only generates a response file and does not install DMP.
`-minpkgs`	View a list of the minimal filesets and the patches that are required for DMP. The installdmp lists the filesets and patches in the correct installation order. The list does not include the optional filesets. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -recpkgs options.
`-nim` *`LLT_SOURCE`*	Generates an installp_bundle for the NIM Server to install DMP. You must specify a valid *LLT_SOURCE* location.
`-noipc`	Disables installdmp from making outbound networking calls to SORT in order to automatically obtain patch and release information updates.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-nolic`	Allows installation of product filesets without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.
`-pkginfo`	Displays a list of filesets 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
`-pkgset`	Discovers and lists the 6.2 filesets installed on the systems that you specify.
`-pkgtable`	Displays the DMP 6.2 filesets 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.
`-prod`	Specifies the product for the operations.
`-recpkgs`	View a list of the recommended filesets and the patches that are required for DMP. The installdmp lists the filesets and patches in the correct installation order. The list does not include the optional filesets. You can use the output to create scripts for command-line installation, or for installations over a network. See the -allpkgs and the -minpkgs options.
`-redirect`	Specifies that the installer need not display the progress bar details during the installation.
`-require`	Specifies an installer patch file.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-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 50. See "Upgrading DMP using response files" on page 50.
`-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.
`-settunables`	Specify this option when you want to set tunable parameters after you install and configure a product. You may need to restart processes of the product for the tunable parameter values to take effect. You must use this option together with the `-tunablesfile` option.
`-start`	Starts the daemons and processes for DMP. If the installdmp failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -stop option. See "Starting and stopping processes for the Symantec products " on page 99.

Table A-1 installdmp options *(continued)*

Option and Syntax	Description
`-stop`	Stops the daemons and processes for DMP. If the installdmp failed to start up all the DMP processes, you can use the -stop option to stop all the processes and then use the -start option to start the processes. See the -start option. See "Starting and stopping processes for the Symantec products " on page 99.
`-timeout`	The `-timeout` option is used to specify the number of seconds that the script must wait for each command to complete before timing out. Setting the `-timeout` option overrides the default value of 1200 seconds. Setting the `-timeout` option to 0 prevents the script from timing out. The `-timeout` option does not work with the `-serial` option.
`-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 filesets on remote systems before installation.
`-tunables`	Lists all supported tunables and create a tunables file template.
`-tunablesfile`	Specify this option when you specify a tunables file. The tunables file should include tunable parameters.
`-upgrade`	Upgrades the installed filesets on the systems that you specify.
`-version`	Checks and reports the installed products and their versions. Identifies the installed and missing filesets and patches where applicable for the product. Provides a summary that includes the count of the installed and any missing filesets and patches where applicable. Lists the installed patches, patches, and available updates for the installed product if an Internet connection is available.

Command options for uninstall script

The `uninstalldmp` command usage takes the following form:

```
uninstalldmp [ <sys1> <sys2>... ]
        [ -require <installer_hot_fix_file> ]
```

```
        [ -responsefile <response_file> ]
        [ -logpath <log_path> ]
        [ -tmppath <tmp_path> ]
        [ -timeout <timeout_value> ]
        [ -hostfile <hostfile_path> ]
        [ -keyfile <ssh_key_file> ]
        [ -prod <product_name> ]
        [ -hotfix_path <hotfix_path> ]
        [ -hotfix2_path <hotfix2_path> ]
        [ -hotfix3_path <hotfix3_path> ]
        [ -hotfix4_path <hotfix4_path> ]
        [ -hotfix5_path <hotfix5_path> ]

  [ -serial | -rsh | -redirect | -makeresponsefile | -comcleanup
| -comsetup | -version | -noipc | -disable_dmp_native_support ]
```

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

Table A-2 uninstalldmp options

Option and Syntax	Description
`-comcleanup`	The `-comcleanup` option removes the ssh or rsh configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of ssh or rsh are abruptly terminated.
`-hostfile` *`full_path_to_file`*	Specifies the location of a file that contains the system names for the installer.
`-disable_dmp_native_support`	Disables Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools during upgrade. Retaining Dynamic Multi-pathing support for the native LVM volume groups and ZFS pools during upgrade increases fileset upgrade time depending on the number of LUNs and native LVM volume groups and ZFS pools configured on the system.
`-hotfix_path`	Defines the path of a patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed .
`-hotfix2_path`	Defines the path of a second patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.

Table A-2 uninstalldmp options *(continued)*

Option and Syntax	Description
`-hotfix3_path`	Defines the path of a third patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
`-hotfix4_path`	Defines the path of a fourth patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
`-hotfix5_path`	Defines the path of a fifth patch level release to be integrated with a base or a maintenance level release in order for multiple releases to be simultaneously installed.
`-keyfile` *`ssh_key_file`*	Specifies a key file for SSH. The option passes `-i` *`ssh_key_file`* with each SSH invocation.
`-logpath` *`log_path`*	Specifies that log_path, not /opt/VRTS/install/logs, is the location where uninstalldmp log files, summary file, and response file are saved.
`-makeresponsefile`	Use this option to create a response file or to verify that your system configuration is ready for uninstalling DMP.
`-redirect`	Displays progress details without showing progress bar.
`-require`	Specifies an installer patch file.
`-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 51.
`-rsh`	Specifies that *rsh* and `rcp` are to be used for communication between systems instead of ssh and `scp`. This option requires that systems be preconfigured such that *rsh* commands between systems execute without prompting for passwords or confirmations
`-serial`	Performs the installation, uninstallation, start, and stop operations on the systems in a serial fashion. By default, the installer performs these operations simultaneously on all the systems.

Table A-2 uninstalldmp options *(continued)*

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

Appendix B

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 147.

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

  ```
  # ./installer -tunablesfile tunables_file_name -settunables [
  sys1 sys2 ...]
  ```

See "Setting tunables with no other installer-related operations" on page 148.

- 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 149.

See "About response files" on page 49.

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

See "Tunables value parameter definitions" on page 151.

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 151.

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 150.

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
 -settunables [sys1 sys2 ...]
```

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 151.

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 150.

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 151.

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 150.

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

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

6 Start the installer with the `-responsefile` and `-tunablesfile` options.

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

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

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

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

Preparing the tunables file

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

You can use the installer to create a tunables file template, or manually format tunables files you create.

To create a tunables file template

- Start the installer with the `-tunables` option. Enter the following:

  ```
  # ./installer -tunables
  ```

  You see a list of all supported tunables, and the location of the tunables file template.

To manually format tunables files

- Format the tunable parameter as follows:

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

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

The following is an example of a tunables file.

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

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

1;
```

Setting parameters for the tunables file

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

See “Tunables value parameter definitions” on page 151.

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 *Symantec Storage Foundation Cluster File System High Availability Administrator's Guide* for detailed information on product tunable ranges and recommendations.

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

Table B-1 Supported tunable parameters

Tunable	Description
autoreminor	(Veritas Volume Manager) Enable reminoring in case of conflicts during disk group import.
autostartvolumes	(Veritas Volume Manager) Enable the automatic recovery of volumes.
dmp_cache_open	(Symantec Dynamic Multi-Pathing) Whether the first open on a device performed by an array support library (ASL) is cached.
dmp_daemon_count	(Symantec Dynamic Multi-Pathing) The number of kernel threads for DMP administrative tasks.
dmp_delayq_interval	(Symantec Dynamic Multi-Pathing) The time interval for which DMP delays the error processing if the device is busy.

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

Tunable	Description
dmp_fast_recovery	(Symantec Dynamic Multi-Pathing) Whether DMP should attempt to obtain SCSI error information directly from the HBA interface. This tunable must be set after Symantec Dynamic Multi-Pathing is started.
dmp_health_time	(Symantec Dynamic Multi-Pathing) The time in seconds for which a path must stay healthy.
dmp_log_level	(Symantec Dynamic Multi-Pathing) The level of detail to which DMP console messages are displayed.
dmp_low_impact_probe	(Symantec Dynamic Multi-Pathing) Whether the low impact path probing feature is enabled.
dmp_lun_retry_timeout	(Symantec Dynamic Multi-Pathing) The retry period for handling transient errors.
dmp_monitor_fabric	(Symantec Dynamic Multi-Pathing) Whether the Event Source daemon (`vxesd`) uses the Storage Networking Industry Association (SNIA) HBA API. This tunable must be set after Symantec Dynamic Multi-Pathing is started.
dmp_monitor_osevent	(Symantec Dynamic Multi-Pathing) Whether the Event Source daemon (vxesd) monitors operating system events.
dmp_monitor_ownership	(Symantec Dynamic Multi-Pathing) Whether the dynamic change in LUN ownership is monitored.
dmp_native_support	(Symantec Dynamic Multi-Pathing) Whether DMP does multi-pathing for native devices.
dmp_path_age	(Symantec Dynamic Multi-Pathing) The time for which an intermittently failing path needs to be monitored before DMP marks it as healthy.
dmp_pathswitch_blks_shift	(Symantec 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.

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

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

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

Tunable	Description
reclaim_on_delete_start_time	(Veritas Volume Manager) Time of day to start reclamation for deleted volumes. This tunable must be set after Veritas Volume Manager is started.
reclaim_on_delete_wait_period	(Veritas Volume Manager) Days to wait before starting reclamation for deleted volumes. This tunable must be set after Veritas Volume Manager is started.
same_key_for_alldgs	(Veritas Volume Manager) Use the same fencing key for all disk groups. This tunable must be set after Veritas Volume Manager is started.
sharedminorstart	(Veritas Volume Manager) Start of range to use for minor numbers for shared disk groups. This tunable must be set after Veritas Volume Manager is started.
storage_connectivity	(Veritas Volume Manager) The CVM storage connectivity type. This tunable must be set after Veritas Volume Manager is started.
usefssmartmove	(Veritas Volume Manager) Configure SmartMove feature (all, thinonly, none). This tunable must be set after Veritas Volume Manager is started.

Appendix C

Configuring the secure shell or the remote shell for communications

This appendix includes the following topics:

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

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

Establishing communication between nodes is required to install Symantec 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 Symantec 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 (sys1) that contains the installation directories, and a target system (sys2). This procedure also applies to multiple target systems.

Note: The script- and web-based installers support establishing passwordless communication for you.

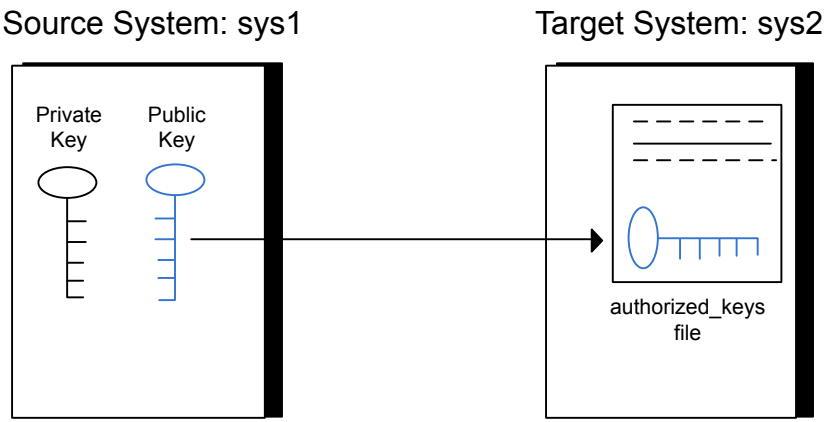
Manually configuring and passwordless ssh

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

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

Figure C-1 illustrates this procedure.

Figure C-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 (sys1), log in as root, and navigate to the root directory.

   ```
   sys1 # cd /
   ```

2. Make sure the `/.ssh` directory is on all the target installation systems (sys2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

   ```
   sys2 # mkdir /.ssh
   ```

   Change the permissions of this directory, to secure it.

   ```
   sys2 # chmod go-w /.ssh
   ```

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

   ```
   sys1 # 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):
   ```

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

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

   Do not enter a passphrase. Press Enter.

   ```
   Enter same passphrase again:
   ```

   Press Enter again.

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

1. From the source system (sys1), move the public key to a temporary file on the target system (sys2).

   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:

   ```
   sys1 # sftp sys2
   ```

   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 sys2 ...
   The authenticity of host 'sys2 (10.182.00.00)'
   can't be established. DSA key fingerprint is
   fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
   Are you sure you want to continue connecting (yes/no)?
   ```

2. Enter `yes`.

   Output similar to the following is displayed:

   ```
   Warning: Permanently added 'sys2,10.182.00.00'
   (DSA) to the list of known hosts.
   root@sys2 password:
   ```

3. Enter the root password of sys2.
4. At the `sftp` prompt, type the following command:

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

   The following output is displayed:

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

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

   ```
   sftp> quit
   ```

6 To begin the `ssh` session on the target system (sys2 in this example), type the following command on sys1:

```
sys1 # ssh sys2
```

Enter the root password of sys2 at the prompt:

```
password:
```

7 After you log in to sys2, enter the following command to append the `id_dsa.pub` file to the `authorized_keys` file:

```
sys2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

8 After the `id_dsa.pub` public key file is copied to the target system (sys2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, enter the following command on sys2:

```
sys2 # rm /id_dsa.pub
```

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

```
sys2 # exit
```

10 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`:

```
sys1 # exec /usr/bin/ssh-agent $SHELL
sys1 # 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 (sys1), enter the following command:

   ```
   sys1 # ssh -l root sys2 uname -a
   ```

   where sys2 is the name of the target system.

2. The command should execute from the source system (sys1) to the target system (sys2) 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 (sys1), bring the private key into the shell environment.

   ```
   sys1 # exec /usr/bin/ssh-agent $SHELL
   ```

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

   ```
   sys1 # ssh-add
   ```

Enabling rsh for AIX

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

sysname.*domainname*.com root

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

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

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

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

Appendix D

DMP components

This appendix includes the following topics:

- Symantec Dynamic Multi-Pathing installation filesets

Symantec Dynamic Multi-Pathing installation filesets

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

Table D-1 Symantec Dynamic Multi-Pathing filesets

filesets	Contents	Configuration
VRTSaslapm	Symantec Array Support Library (ASL) and Array Policy Module(APM) binaries Required for the support and compatibility of various storage arrays.	Minimum
VRTSperl	Perl 5.16.1 for Symantec.	Minimum
VRTSveki	Symantec Kernel Interface Contains a common set of modules that other Symantec drivers use.	Minimum
VRTSvlic	Symantec 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

Table D-1 Symantec Dynamic Multi-Pathing filesets *(continued)*

filesets	Contents	Configuration
VRTSvxvm	Symantec Volume Manager binaries	Minimum
VRTSsfcpi62	Symantec Storage Foundation Common Product Installer The Storage Foundation Common Product installer fileset 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	Symantec 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	Symantec Software Support Tools	Recommended

Appendix E

Troubleshooting installation issues

This appendix includes the following topics:

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

Restarting the installer after a failed connection

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

What to do if you see a licensing reminder

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

```
WARNING V-365-1-1 This host is not entitled to run Symantec Storage
Foundation/Symantec 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' and validate using the command
'vxkeyless set NONE'.
```

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

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

  ```
  # /opt/VRTS/bin/vxlicrep
  ```

- Continue with keyless licensing by managing the server or cluster with a management server.
  For more information about keyless licensing, see the following URL: http://go.symantec.com/sfhakeyless

Troubleshooting an installation on AIX

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

Then reinstall.

Incorrect permissions for root on remote system

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

```
Failed to setup rsh communication on 10.198.89.241:
'rsh 10.198.89.241 <command>' failed
```

```
Trying to setup ssh communication on 10.198.89.241.
Failed to setup ssh communication on 10.198.89.241:
Login denied

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

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

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

System verification did not complete successfully

The following errors were discovered on the systems:

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

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

See "About configuring secure shell or remote shell communication modes before installing products" on page 155.

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

Resource temporarily unavailable

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

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

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

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

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

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

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

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

```
# smitty chgsys
```

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

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

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

See the `smitty` and `chdev` manual pages.

Inaccessible system

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

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

Appendix F

Compatibility issues when installing DMP with other products

This appendix includes the following topics:

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

Installing Storage Foundation when other Symantec 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 VOM Central Server is present, the installer skips the VRTSsfmh upgrade and leaves the VOM Central Server and Managed Host filesets as is.
- When uninstalling Storage Foundation products where VOM Central Server is present, the installer does not uninstall VRTSsfmh.
- When you install or upgrade Storage Foundation products where 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

A

about
- Deployment Server 65
- DMP 14
- installation and configuration methods 23
- installation preparation 32
- installation using operating system-specific methods 55
- planning for installation 23
- response files 49
- SORT 15
- Symantec product licensing 26
- upgrading using an alternate disk 117
- Veritas Operations Manager 15
- web-based installer 43

assesing system
- installation readiness 35

B

before using
- web-based installer 44

C

checking
- installation readiness 35

checking product versions 20
configuring
- rsh 33
- ssh 33

creating
- backups 106
- Install Templates 90

D

defining
- Install Bundles 84

deploying
- Symantec product updates to your environment 82
- Symantec releases 92

deploying using
- Install Bundles 92

deploying using Install Templates
- Install Templates 92

deployment preferences
- setting 71

Deployment Server
- about 65
- downloading the most recent release information from the SORT site 73
- installing 67
- loading release information and patches on to 74
- overview 66
- setting up 68
- specifying a non-default repository location 73

disabling
- external network connection attempts 22

disk space requirements 19
DMP installation
- preinstallation information 18

downloading maintenance releases and patches 20
downloading the most recent release information
- by running the Deployment Server from a system with Internet access 73

I

Install Bundles
- defining 84
- deploying using the Deployment Server 92
- integration options 107

Install Templates
- creating 90
- deploying using Install Templates 92

installation
- log files 99
- using the mksysb utility 58

installer
- about the script-based installer 37

installer patches
- obtaining either manually or automatically 21

installer program 39

Installing
DMP with the web-based installer 46
web-based installer 46
installing
DMP 39, 131
DMP using operating system-specific methods 55
on NIM client using SMIT on NIM server 57
operating system on the NIM client using SMIT 58
Symantec product license keys 29
the Deployment Server 67
using NIM 56
using response files 50

K

keyless licensing
setting or changing the product level 27

L

licensing
installing Symantec product license keys 29
setting or changing the product level for keyless licensing 27

M

mksysb
creating backup image 59
installation 58
installing image on alternate disk 60
verifying installation 62
mounting
software disc 34

N

NIM
installing 56
preparing the installation bundle 56
NIM ADM
preparing the installation bundle 124
preparing to upgrade 124
supported upgrade paths 123
upgrading DMP and the operating system 125
verifying the upgrade 127

O

obtaining
installer patches either automatically or manually 21
security exception on Mozilla Firefox 45
overview
Deployment Server 66

P

performing
postcheck on a node 42
post-upgrade
updating variables 129
verifying 129
prechecking
using the installer 36
preinstallation check
web-based installer 46
preparing to upgrade 104
using alternate disk 118

R

release images
viewing or downloading available 75
release information and patches
loading using the Deployment Server 74
release notes 18
releases
finding out which releases you have, and which upgrades or updates you may need 83
removing Storage Foundation products using SMIT 133
repository images
viewing and removing repository images stored in your repository 79
response files
about 49
installation 50
syntax 51
uninstalling 51
upgrading 50
variable definitions 52
rsh
configuration 33

S

script-based installer
about 37

setting
deployment preferences 71
environment variables 33
setting up
Deployment Server 68
simulataneous install or upgrade 107
specifying
non-default repository location 73
ssh
configuration 33
starting
web-based installer 44
supported operating systems 19
supported upgrade paths
using alternate disks 118
using NIM ADM 123
Symantec product license keys
installing 29
Symantec product updates
deploying to your environment 82
Symantec products
starting process 99
stopping process 99
Symantec releases
deploying a specific release 92

T

tunables file
about setting parameters 146
parameter definitions 151
preparing 150
setting for configuration 147
setting for installation 147
setting for upgrade 147
setting parameters 150
setting with no other operations 148
setting with un-integrated response file 149

U

uninstalldmp command 131
uninstalling
Storage Foundation products using SMIT 133
using response files 51
using the web-based installer 132
upgrade
array support 106
creating backups 106
getting ready 104
upgrade *(continued)*
methods 102
preparing for upgrade 105
supported upgrade paths 103
upgrades or updates
finding out which releases you have 83
upgrading
AIX operating system 116
DMP-enabled rootvg 113–114
on a Virtual I/O server (VIOS) 115
on an alternate disk 120
using product installer 110
using response files 50
using the web-based installer 111
upgrading using alternate disk
preparing to upgrade 118
verifying 121
upgrading using alternate disks
supported upgrade paths 118
upgrading using an alternate disk
about 117
supported upgrade scenarios 118

V

verifying
product installation 98
upgrading using alternate disk 121
viewing and removing repository images
stored in your repository 79
viewing or downloading
available release images 75
VIOS requirements 19

W

web-based installer 46
about 43
before using 44
installation 46
preinstallation check 46
starting 44
uninstalling 132
upgrading 111