Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide

Windows Server 2003
Windows Server 2008

5.1

Symantec

Veritas™ Dynamic Multi-Pathing for Windows Installation and Upgrade Guide

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

Product version: 5.1

Document version: 5.1.0

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 automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information

- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:
www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.
Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:
www.symantec.com/business/services/
Select your country or language from the site index.

Contents

Chapter 1

About Veritas Dynamic Multi-Pathing 5.1 for Windows (DMPW 5.1)

This chapter contains the following topics:

Overview

The Veritas Dynamic Multi-Pathing 5.1 for Windows (DMPW 5.1) adds additional fault tolerance to disk storage by making use of multiple paths between a computer and a disk in a storage array. A path is a connection between the computer and the storage array's disks and consists of a Host Bus Adapter (HBA) and a SCSI bus connection to one or more SCSI disks or a fiber optic channel connected to a hub, switch, or array. Thus, multiple paths are made possible by connecting two or more host bus adapters with either SCSI or fiber optic cabling to the storage array.

The Dynamic Multi-Pathing standalone software manages multiple paths so that the data on each of the array's disks is accessible to the host computer. If a path to a disk fails, Dynamic Multi-Pathing automatically transmits data to the disk over an alternate path.

The paths on an array are set up to work in two ways—either in a Active/Active mode which provides data load balancing between multiple paths, or in a Active/Passive mode where only one path is active and other remaining paths act as backups or standby paths.

Veritas Dynamic Multi-Pathing for Windows (DMPW) is a truly heterogeneous solution which fully integrates with the Microsoft Multipath I/O (MPIO) architecture, including several Device Specific Modules (DSMs) which provide support for a wide variety of the most popular array families available today from the leading storage vendors.

- Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 support (32-bit, x64, and IA64) support
- Fiber Channel StorPort Miniport HBA Driver support
- iSCSI HBA support
- Microsoft iSCSI Software Initiator support
- Microsoft MPIO-based
- Microsoft WHQL logo qualified
- SCSI-3 PGR Support
- Boot from SAN support
- Active/Active Dynamic Multi-Pathing with clustering support
- Following load balancing policies are supported on DMP DSMs:
  - Active/Passive (Failover only)
  - Round Robin
  - Dynamic Least Queue Depth
  - Least Blocks
  - Weighted Path
  - Balanced Path
  - Round Robin with Subset

For details refer to the Veritas *Dynamic Multi-Pathing for Windows Administrator's Guide*.

For DMP DSMs, Boot and data volumes are supported on the same bus/HBAs for non-clustered servers if the Boot from SAN recommendations from Microsoft are followed. DMP DSMs are not supported with fibre channel port drivers, fibre channel SCSI Miniport drivers or boot/cluster disks on the same bus/HBAs.

Active/Active and Active/Passive settings

The Dynamic Multi-Pathing software provides greater availability, reliability and performance by using path failover and load balancing. This feature is available for multiported disk arrays from various vendors.

Multiported disk arrays can be connected to host systems through multiple paths. To detect the various paths to a disk, DMP uses a mechanism that is

specific to each supported array type. DMP can also differentiate between different enclosures of a supported array type that are connected to the same host system.

The multipathing policy used by DMPW depends on the characteristics of the disk array.

DMPW supports the following standard array types:

Active/Active (A/A)

Allows several paths to be used concurrently for I/O. Such arrays allow DMP to provide greater I/O throughput by balancing the I/O load uniformly across the multiple paths to the LUNs. In the event that one path fails, DMP automatically routes I/O over the other available paths.

Asymmetric Active/Active (A/A-A)

Arrays based on the Asymmetric Logical Unit Access (ALUA) allow access to LUNs via the primary path or preferred path which is always active.

Can be accessed through secondary or standby paths with little performance degradation in the event of a primary path failure. Usually an A/A-A array behaves like an A/P array rather than an A/A array. However, during failover, an A/A-A array behaves like an A/A array.

Active/Passive (A/P)

A mode in which a path designated as the “Preferred Path” or “Primary Path” is always active and the other path or paths act as backups (standby paths) that are called into service if the current operating path fails.

Allows access to its LUNs via the primary (active) path on a single controller (also known as an access port or a storage processor) during normal operation.

In implicit failover mode, an A/P array automatically fails over by scheduling I/O to the secondary (passive) path on a separate controller if the primary path fails. This passive port is not used for I/O until the active port fails.

In A/P arrays, path failover can occur for a single LUN if I/O fails on the primary path.

Concurrent Active/Passive (A/P-C)

Supports concurrent I/O and load balancing by having multiple primary paths into a controller. This functionality is provided by a controller with multiple ports, or by the insertion of a SAN hub or switch between an array and a controller. Failover to the secondary (passive) path occurs only if all the active primary paths fail.

For details refer to the Veritas *Dynamic Multi-Pathing 5.1 for Windows Administrator's Guide.*

Best Practices

- It is recommended to set a single I/O path before installing DMPW. You can enable the additional paths later on after installation.
- Ensure that you have enabled the MPIO feature for Windows Server 2008 before proceeding with the DMPW 5.1 install.
- Setting SCSI-3 PGR reservations
  SCSI-3 PGR supports multiple nodes accessing a device while at the same time blocking access to other nodes. SCSI-3 PGR supports multiple paths from a host to a disk and SCSI-3 PGR reservations are persistent across SCSI bus resets.
  For DMP DSMs, the Active/Active setting is implemented by translating SCSI reserve/release commands to SCSI-3 PGR commands.
- Selecting the appropriate load-balancing policy
  In addition to the Round Robin algorithm, DMPW 5.1 offers the following load balancing options:
  - Active/Passive (Failover only)
  - Round Robin
  - Dynamic Least Queue Depth
  - Least Blocks
  - Weighted Path
  - Balanced Path
  - Round Robin with Subset

For details refer to the Veritas *Dynamic Multi-Pathing 5.1 for Windows Administrator's Guide.*

Veritas Operations Manager (VOM) support for DMPW 5.1

Veritas Operations Manager (VOM) centralizes visibility and control, ensures availability, scales operations, optimizes storage and maintains compliance across your server and storage assets. The VOM console is a web-based Graphical User Interface (GUI) that seamlessly integrates a wide range of management related tasks. At the same time, it enables you to centrally monitor

and visualize the DMP DSM hosts. You can generate reports related to product plug-in hosts and the storage resources.

Using the VOM console, you can gather information, monitor, allocate resources, and perform operations on hosts, databases, applications, and storage resources throughout the data center. It thus facilitates administration of different roles and tasks of a host administrator, storage administrator, and application administrator all combined into one.

The central administrator can also generate status and inventory reports and distribute the report to others who need the information. VOM console, running as a thin client, is accessed through web browser. The console provides an entry point for Veritas Dynamic Multi-Pathing for Windows (DMPW) and Storage Foundation for Windows (SFW) products with the SFW Add-on installed.

Chapter 2

Preinstallation tasks

This chapter includes the following topics:

Prerequisites

Ensure that you have taken care of the following before installing Veritas Dynamic Multi-Pathing for Windows (DMPW):

- Review the *Veritas Dynamic Multi-Pathing for Windows Installation and Upgrade Guide*.
- Review the *Veritas Dynamic Multi-Pathing for Windows Release Notes*.
- Review the Hardware Compatibility List (HCL) for DMPW to confirm supported hardware:
  http://www.symantec.com/docs/TECH138719
- For Late Breaking News (LBN) refer to:
  http://www.symantec.com/business/support index?page=content&id=TECH59755
- Review the product installation requirements
  See "Requirements" on page 18.
- Exit all running applications

Requirements

Minimum requirements and Symantec recommended requirements may vary. Review the following product installation requirements for your system before installation:

- Disk space requirements for DMPW
- General requirements
- Remote Systems
- Driver Signing Options
- Permission requirements for DMPW
- Additional DMPW installation requirements
- System requirements

Disk space requirements for DMPW

For normal operation, all installations require a minimum of 50 MB of disk space in addition to the requirements listed in Table 2-1 below.

Note: For installation, space required is calculated regardless of selected options or components.

Table 2-1 summarizes approximate disk space requirements for DMPW Server and Client components on a 32-bit and 64 bit system:

Table 2-1 Disk space requirements

Installation Options	Install directory or drive 32-bit	Install directory or drive 64-bit
DMP DSMs + Server components	700 MB	850 MB
DMP DSMs + Client components	450 MB	450 MB

General requirements

Before you install Veritas Dynamic Multi-Pathing for Windows, verify that your configuration meets the following criteria and that you have reviewed the Hardware Compatibility List at http://www.symantec.com/docs/TECH138719 to confirm the supported hardware:

Table 2-2 summarizes the hardware requirements for DMPW installation

Table 2-2 Hardware requirements for DMP Standalone installation

Requirements	Specifications
Memory	1GB of RAM required
32-bit processor requirements	800-megahertz (MHz) Pentium III compatible or faster processor 1GHz or faster processor recommended
x64 processor requirements	1GHz AMD Opteron, ADM Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support processor or faster
IA64 processor requirements	1 GHz Itanium or faster processor 1 GHz Dual-Core Intel Itanium 2 or faster processor
Display	Minimum resolution: 1024 X 768 pixels or higher

Remote Systems

Installation on remote systems is supported using either the Graphical User Interface (GUI) option or silent install through the Command Line Interface (CLI). Silent installation may be done on one node at a time. Use the GUI to install on multiple nodes. Remote Desktop Protocol (RDP) connections must use the console switch. You must have network access or appropriate administrative privileges to each remote computer.

Driver Signing Options

When installing on systems running Windows Server 2003, you must either set the Windows driver signing option to ignore software authentication warning messages or select an installation option to install a Symantec Trusted Certificate for unsigned drivers.

For Windows Server 2008, this is set by default as changing the driver signing option is not supported. The Symantec product installer provides an installation option to install a Symantec Trusted Certificate to allow installation of Symantec drivers that are not certified by Microsoft.

See "Setting the Windows driver signing options" on page 26.

See "Installing Symantec Trusted certificate for unsigned drivers" on page 27.

Permission requirements for DMPW

You must be a member of the Local Administrators group or a domain administrator on all the nodes where you install Veritas Dynamic Multi-Pathing for Windows.

Additional DMPW installation requirements

The following are some additional DMPW installation requirements:

- Installation media for all products and third-party applications
- Licenses for all products and third-party applications

Note: The Windows MPIO feature must be enabled for Windows Server 2008 before you proceed with installing DMPW 5.1.

Note: DMPW supports SCSI, Fibre Channel, iSCSI Host Bus Adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage.

System requirements

The following system requirements must be met before you proceed with the Veritas Dynamic Multi-Pathing for Windows installation:

- A minimum memory of 1 GB RAM per server for DMPW installation.
- Ensure that you have a minimum of two IO paths from the server to the storage array for load balancing to happen.

Planning for a DMPW installation

During installation, the product installer automatically installs DMP and the selected DSMs. You may also choose to install simultaneously on more than one system or host during installation.

Review the following information and decide how you want to configure your install environment:

Setting up access rights

DMPW uses the standard Microsoft Windows administrative privileges which govern the access rights of users to the DMPW servers and services.

The following services are associated with the product:

- Veritas Enterprise Administrator service (vxob)
- Veritas Installer Service (vxinstaller) used during installation
- VxVM (Storage Agent) service
- Windows Management Instrumentation (WMI) service for DMP functionality

By default, administrators have the right to load and unload device drivers and install and uninstall the Veritas Dynamic Multi-Pathing for Windows. For accessing and using the program you must have administrative rights.

As an administrator, you need to grant these same administrative privileges to other users. For example, you can grant these rights in the Local Users and Groups function under Windows Server 2003 or Windows Server 2008 Administrative Tools.

For details refer to the Microsoft Windows Server documentation.

Before proceeding, exit all programs and log on with administrative rights.

About Licensing

Licensing for DMPW is based on the Microsoft Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 operating systems in use on a specific server. A license is required for each system that runs DMP.

Evaluation license key

An evaluation license key is embedded in the product. Note that this license key is valid for a period of two months only.

Table 2-3 lists the Veritas Dynamic Multi-Pathing for Windows (DMPW) license editions and the additional licensing terms that apply.

Table 2-3 DMPW licensing terms

Microsoft Operating System Edition	DMPW Licensing terms
■ Standard Edition ■ Web Edition	A separate license for the licensed software is required for each virtual or physical server, where the software is installed.

Table 2-3 DMPW licensing terms

Microsoft Operating System Edition	DMPW Licensing terms
■ Enterprise Edition	For each license, you may run one instance of the licensed software on one physical server and up to four simultaneous instances of the licensed software on virtual servers located on the physical server.
■ Datacenter Edition	For each license, you may run one instance of the licensed software on one physical server and an unlimited number of virtual servers located on the physical server.

Client license

A license is not required, if you install DMPW Client components.

License management

The product installer lets you add and remove specific licenses. Adding a license for an option does not install the option. Use the Windows **Control Panel > Add/Remove** program to install an option. License keys support installation on multiple systems.

Note: A default evaluation license key is supplied for your use. This license key is valid for a period of two months only. You must purchase the product to obtain a permanent license key.

vxlicrep command

The `vxlicrep` command generates licensing information reports for Symantec products licensed and installed on your system. The output includes product information (name, version, product ID) and the contents of the product-specific data encoded in each license key.

```
vxlicrep [-g][-s][-e][-i][-k key[,key2,key3,...]][-h][-v]
```

To display a license report using the vxlicrep command

1. Click **Start > Run** to open the command window.
2. Enter the `vxlicrep` command without any options to generate a default report.

3 Enter the `vxlicrep` command with any of the following options listed below to produce a report as per your requirement:

Values	Description
`-g`	When specified with the `vxlicrep` command generates a default report.
`-s`	Generates a short report
`-e`	Generates an enhanced/detailed report
`-i`	Prints report for input `key1, key2`
`-k`	print report for valid keys only
`-v`	Generates a print version
`-h`	Displays help

Using the Configuration Checker

The Configuration Checker wizard is a tool that enables you to verify your configuration before you install DMPW. The wizard can be accessed through the link given for Config Checker on the Symantec Product Installer.

See "Installing DMPW using the product installer" on page 25.

SORT and the Configuration Checker

Symantec's Veritas Operations Service (SORT) lets you verify that the systems in your environment meet the requirements to install or upgrade the DMPW software.

The Configuration Checker application and features have been incorporated into the SORT framework.
The SORT web site is located at:
https://sort.symantec.com/home

On the Sort web site, you are presented with the following options:

- Generate a detailed report that shows you whether your system is ready to install or upgrade the specified product
- Display a hardware and software checklist report that you can use to ensure that your system is ready to install or upgrade the specified product.

The SORT data collector is used to generate a report that shows whether your system is ready to install DMPW. The data collector is downloaded from the

SORT web site. The data collector then gathers information about your system and environment and saves it to a file. You can subsequently upload this file to the SORT web site for analysis and report creation.

The Configuration Checker also produces a SORT formatted result file (`SORT_results.xml`). After running the Configuration Checker and creating the `SORT_results.xml` file, you can save this file to a directory where you have saved the HTML file summary report. You can upload these file to the SORT web site for analysis and report creation.

Alternatively, you can also use the SORT hardware and software checklist report to ensure that your system is ready to install or upgrade the specified product. You do not have to download the data collector. This option provides a quick alternative to the detailed report. To generate a checklist, you must select responses at the SORT web site regarding questions about your system and environment. After submitting your responses, a checklist is generated for you to review.

Chapter 3

Installing the Veritas Dynamic Multi-Pathing 5.1 for Windows

Installation via GUI and CLI is supported for DMPW 5.1. You can use the following options:

- Installing DMPW using the product installer
- Installing DMPW through the command line

Installing DMPW using the product installer

The product installer enables you to install the software for Veritas Dynamic Multi-Pathing for Windows.

Note: The Windows MPIO feature must be enabled for Windows Server 2008 before you proceed with DMPW 5.1 installation.

Ensure that you have fulfilled the following pre-requisites before proceeding with installation:

- Setting the Windows driver signing options
- Installing Symantec Trusted certificate for unsigned drivers

See "Preinstallation tasks" on page 17 to ensure that you have fulfilled the installation prerequisite tasks.

Setting the Windows driver signing options

Some drivers provided by Symantec may not be signed by Microsoft. Depending upon your installation options, these unsigned drivers may stop your installation.

When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 3-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers on Windows Server 2003.

Table 3-1 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either **Ignore** or **Warn**. On remote systems set the option to **Ignore** in order to allow the installation to proceed without user interaction.

Note: Windows Server 2008 does not allow you to change the driver signing option. Symantec provides an installation option to install a Symantec Trusted certificate to allow installation of Symantec drivers that are not certified by Microsoft.

To change the driver signing options on each system

1. Log on locally to the system.
2. Click **Start** > **Control Panel** > **System**.
3. Select the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.
5. Click **OK**.

6 Repeat for each computer.
If you do not change the driver signing option, the installation may fail on a system during validation. After you complete the installation, reset the driver signing option to its previous state.

Installing Symantec Trusted certificate for unsigned drivers

The product installer provides an installation option for Symantec Trusted Software Publisher Certificate for Veritas Storage Foundation for Windows drivers that are not certified by Microsoft.

If you select this installation option, a Symantec Trusted certificate is installed on the systems you select for installation.

Warning: On Windows Server 2008, if this option is not selected, a remote install will not install any DMP drivers that are not certified by Microsoft. No notification is given and it will appear that installation was successful, but issues can arise later because the drivers were not installed.

If installing locally on Windows Server 2008, if this option is not selected, a driver signing popup will be displayed requiring user interaction.

If you select this option when installing on Windows Server 2003, you do not need to set the driver signing options to **Warn** or **Ignore**.

Perform the following to install the Veritas Dynamic Multi-Pathing 5.1 for Windows:

To install Veritas Dynamic Multi-Pathing for Windows through GUI

1 Insert the disc containing the installation software into your system's disk drive or download the installation software from the Symantec website.

2 Allow the autorun feature to start the installation or double-click **Setup.exe.** Veritas Dynamic Multi-Pathing 5.1 for Windows Installer screen appears.

3 Review the links on the Installer screen.

Late Breaking News	Select this option to access the latest information about updates, patches, and software issues for this release.
Configuration Checker	Select this option to run Configuration Checker to verify that your configuration meets all the software and hardware requirement for a smooth installation process. See "SORT and the Configuration Checker" on page 23

Getting Started	Click on this option to gain access to the Getting Started Guide for DMPW.
Installation Guide	Click on this option to gain access to the Installation Guide for DMPW.
Release Notes	Click on this option to gain access to the Release Notes for DMPW.
SORT	Select this option for the (SORT) website https://sort.symantec.com/home The SORT website contains reports for Symantec Enterprise products, checklist for recommended configuration, as well as the system and patch requirements to install or upgrade DMPW. See "SORT and the Configuration Checker" on page 23
Browse Content	Select this option to see the contents of the disc.
Technical Support	Specifies the link to Symantec Technical Support.
Install Veritas Dynamic Multi-pathing	In order to install the Veritas Dynamic Multi-Pathing for Windows, select one of the two options shown on the product installer screen: ■ Complete/Custom Click **Install** to install server and client (optional) components, and other product options. This launches the dialog box for LaunchVPI.exe. Click **Run** to launch the product installer ■ Administrative Console Click **Install** to install client components to manage servers from a remote system. This launches the dialog box for LaunchVPI.exe. Click **Run** to launch the product installer

Click **Next**.

4 Review the prerequisite information on the Welcome page.
Click **Next**.

5 Review the License Agreement by using the scroll arrows in the view window.
If you agree to the license terms, click the radio button for **I AGREE TO the terms of the license agreement**, and then click **Next**.

6 Enter the following information as per your installation requirements:

- Use embedded 2-month evaluation key
  Select this option to use the default evaluation license key. This license key has validity for 60 days only.
- Enter license key(s)
  Enable this option to provide the license key for your product.
  Click **Add**.
  Select the appropriate product options and its related license key to view the licensed options in the License key details box.
  To remove a license key, select it and click **Remove**.
  Additionally, you can save a report of this agreement by clicking the **Save** button.
  Click **Next**.

7 On the Option Selection page, select optional features to be installed on a system as shown below:

Veritas Dynamic Multi-Pathing 5.1 for Windows (Server Components)	Enable this option to install Server components, Client components (optional), other product options.
Veritas Dynamic Multi-Pathing 5.1 for Windows (Client Components)	Enable this option to install client components to manage servers from a remote system.

Install Path	Optionally, change the installation path.
	■ To change the path, select a computer in the Selected computers for installation field, type the new path, and click **Change**.
	■ To restore the default path, select a computer and click **Default**.
	The default path is:
	`C:\Program Files\Veritas`
	For 64-bit installations, the default path is:
	`C:\Program Files (x86)\Veritas`

Click **Next**.

8 On the System Selection page, specify the system name or IP address of the machines on which you want to install DMPW. Complete the information on this page as follows:

System Name or IP:	Enter the machine name or IP address to add a computer for installation. Click **Add**. Alternatively, click on **Browse** to select a system from the computer name list. If a computer fails validation, address the issue, and repeat the validation. Click on the **System verification information** icon to display information about the failure. Click **Re-verify** to begin the validation process again or enter a valid system name or IP address so that verification check for system address is successful. To remove a computer after adding it, click the **Remove System** icon to remove a system from the selected list. **Note:** When installing the software on multiple computers in a single installation using the product installer, all computers must have the same platform type (for example, x86 or x64). However, the computers can have different Windows operating systems. For example, you can install the software on multiple computers at once running Windows 2003 and Windows 2008.

DMPW can be installed on local as well remote systems.
Click **Next** when the installer shows **Status > Ready for Install**.
A warning is displayed for enabling the MPIO feature.
Ensure that you have enabled the Microsoft MPIO feature on Windows Server 2008 before proceeding with installation.
Click **OK**.

9 The Pre-Install Report is displayed.
Enable the checkbox **Automatically reboot systems after installer completes the operation** to activate the automatic reboot option.
To save this report click **Save Report**.
A warning message is displayed that a system reboot is required for the operation to complete successfully. Click **OK** to reboot the system. Click **Cancel** to change the automatic reboot option.
Click **Next** to proceed.

10 The product installer shows the progress status. The installation progress on the selected system can be seen by selecting the **Show Details** button.
The product gets installed on the specified system. This takes few minutes to complete.
Click **Next** when installation is complete on the selected system.

11 On the Post-Install Summary page, review the installation results. Click **Save Report** to save the post-install report summary.
Click **Next** to continue.

12 A dialog box for rebooting the system is displayed. Click **Yes** to reboot.
Click **No** to reboot later.
Click **Finish** to exit the installer wizard.

Installing DMPW through the command line

You can perform a silent installation using the Command Line Interface (CLI) option for Veritas Dynamic Multi-Pathing 5.1 for Windows (DMPW 5.1).

Note that with a silent installation, you can install the DMPW installer package on one computer at a time.

Note: For Windows Server 2008, all CLI commands must run on the command window in the "run as administrator" mode.

To install DMPW from the command line

1 Click **Start > Run**, type `cmd` and click **OK** to open the command prompt.

2 From the command prompt, navigate to the root directory where Setup.exe is located.

3 Use the following command syntax to install DMPW installer

```
Setup.exe /s solutions=<"Solution ID">
install_mode=<Install_mode> installdir=<"
Installdir"> reboot=<Reboot> node=<"target">
licensekey=<"licensekey"> options=<"options">
```

where,`Setup.exe /s solutions=1 install_mode=1` for installing Veritas Dynamic Multi-Pathing Server components.
Here `Setup.exe /s` denotes silent installation through CLI.

Syntax for setup.exe

Enter `setup.exe/?` to display help for the `setup.exe` command

The syntax for setup.exe command is:

```
Setup.exe /s solutions=<"Solution ID">
install_mode=<Install_mode> installdir=<"
Installdir"> reboot=<Reboot> node=<"target">
licensekey=<"licensekey"> options=<"options">
```

For example:

```
Setup.exe /s INSTALL_MODE="1" licensekey="AJZE-W49W-RT7U-ZZPP-
PPPP-P3PP-PPPC-BYV8-P" SOLUTIONS="1,3" installdir="E:\product"
OPTIONS="V3PARAA,VEQLOGIC,VEMCSYMM,VEMCCLAR,VHDSAA,VHDSAP,VHPMS
A2,VHPEVA,VIBMAADS,VIBMAP,VENGAP,VIBMAPDS,VXIV,VHUAWEIAP,VFUJIT
SUAA,VNETAPP,VPILLAR,VITARGET,VXIOTECH,VCOMPLNT,VSUN,SYMCCERT"
NODE=Localhost REBOOT="0"
```

Table 3-2 summarizes the values and related description for the `setup.exe` command

Table 3-2 Parameter values and relative description for setup.exe command.

Parameter values	Description
`solutions=<"Solution ID">`	■ `1:` Veritas Dynamic Multi-Pathing 5.1 for Windows (Server Components) ■ `3:` Veritas Dynamic Multi-Pathing 5.1 for Windows (Client Components) Multiple solution IDs can be entered by using ',' as separator
`install_mode`	Specifies values to be entered for installation or uninstallation. Multiple solution IDs can be entered by using ',' as separator. Possible values are: ■ `1=Installation` ■ `5=Uninstallation` For example, specifying `<install-mode=1>`, installs the DMPW product software.

Table 3-2 Parameter values and relative description for setup.exe command.

Parameter values	Description

`Installdir`	The default installation path is at:
	`C:\Program Files\Veritas`
	For 64-bit installations, the default path is at:
	`C:\Program Files (x86)\Veritas`
	Specify the install directory within double quotes.

`Reboot`	Optional Parameter: ■ `0`: Do not reboot after operation. This is the default setting. ■ `1`: Reboot after installation is complete.
`target` `local node`	■ `target`: Optional parameter. ■ `local node`: Default system name is the localnode. Specify the system name within double quotes. Example: `"System1"`
`License Key`	Optional Parameter. Specify licenses within quotes. Specify "`PERMANENT`" to install embedded permanent license key. Multiple licenses can be entered by using ',' as separator
`Options`	Optional parameter. Specify the DSM options within double quotes. Multiple options can be entered, use ',' as separator

Chapter 4

Uninstalling the Veritas Dynamic Multi-Pathing 5.1 for Windows

This chapter contains the following topics:

Uninstalling DMPW through the GUI

To uninstall DMPW through GUI, follow the procedure listed below:

To uninstall DMPW through the GUI

1. Use the Windows **Control Panel > Add Remove** program to uninstall DMPW. The installer for Veritas Dynamic Multi-Pathing 5.1 for Windows gets launched.
   Using the product installer, you can uninstall DMPW 5.1 on local as well as remote systems.
2. On the System Selection page, enter the IP address or name of the system that you want to uninstall.
   Click **Next**.
3. Review the information for Pre-Uninstall report that is displayed. Enable the checkbox **Automatically reboots system after installer completes the operation**.
   Click **Save Report** to save the report.
   Click **Next** to begin un-installation.

4 When the uninstallation process gets completed (the product installer shows the progress bar for the uninstallation procedure), Click **Next** to continue.

5 Review the information for Post-Uninstall Report.
Click **Save Report** to save the uninstall summary report.
Click **Next**.

6 Review the uninstallation progress. Click **Next** to continue.

7 Summary is displayed for the uninstalled DMP DSM options. Click **Finish** to exit.

Uninstalling DMPW through the command line

To uninstall DMW using command line

1 Click **Start > Run**, type `cmd` and click **OK** to open the command prompt.

2 From the command prompt, navigate to the root directory where Setup.exe is located.

3 Use the following command syntax to install DMPW installer:

```
Setup.exe /s solutions=<"Solution ID">
install_mode=<Install_mode> installdir=<"
Installdir"> reboot=<Reboot> node=<"target">
licensekey=<"licensekey"> options=<"options">
```

where,Setup.exe /s solutions=`1` install_mode=`5` for uninstallation.

Syntax for setup.exe

Enter `setup.exe/?` to display help for the `setup.exe` command

Table 4-1 specifies the values for `setup.exe/?` command

Table 4-1 Parameter values and relative description for setup.exe command.

Parameter values	Description
`solutions=<"Solution ID">`	■ `1`: Veritas Dynamic Multi-Pathing 5.1 for Windows (Server Components) ■ `3`: Veritas Dynamic Multi-Pathing 5.1 for Windows (Client Components) Multiple solution IDs can be entered by using ',' as separator

Table 4-1 Parameter values and relative description for setup.exe command.

Parameter values	Description
`install_mode`	Specifies values to be entered for installation or uninstallation. Multiple solution IDs can be entered by using ',' as separator. Possible values are: ■ `1=Installation` ■ `5=Uninstallation` For example, specifying `<install-mode=1>`, installs the DMPW product software.
`Installdir`	Default installation directory is `C:\Program Files\Veritas` Specify the directory within double quotes.
`Reboot`	Optional Parameter: ■ `0`: Do not reboot after operation. This is the default setting. ■ `1`: Reboot after installation is complete.
`target` `local node`	■ `target`: Optional parameter. ■ `local node`: Default system name is the localnode. Specify the system name within double quotes. Example: `"System1"`
`License Key`	Optional Parameter. Specify licenses within quotes. Specify "`PERMANENT`" to install embedded permanent license key. Multiple licenses can be entered by using ',' as separator
`Options`	Optional parameter. Specify the DSM options within double quotes. Multiple options can be entered, use ',' as separator

Chapter 5

Upgrading DMPW 5.1 to SFW 5.1 SP2

This chapter covers upgrading Veritas Dynamic Multi-Pathing 5.1 for Windows (DMPW 5.1) to Veritas Storage Foundation (SFW) 5.1 SP2 for Windows (SFW 5.1 SP2).

This chapter contains:

Before upgrading to SFW 5.1 SP2

Before upgrading, ensure that your systems meet the minimum product versions.

To upgrade to SFW 5.1 SP2 your system must meet the minimum supported product versions, which the product installer checks before it upgrades.

If your current installation does not meet the minimum level required by the installer, Symantec recommends manually applying the appropriate product upgrades to meet the minimum product level required before proceeding with the installer. You can get intermediate versions of the products on the Symantec Support site.

http://www.symantec.com/business/support/index?page=home

For license keys, contact Symantec Sales. You can also uninstall the older versions of the product and install the new product.

Preparing for the upgrade

Upgrading the product requires the following steps:

- Back up all your data in a safe location.
- Back up the system state.
- Check the hardware requirements for software upgrade.
- Check to see if you need to update the Microsoft Active Directory to support the upgraded software.
- Test the system after each upgrade, especially after applying product upgrades to meet the minimum version required. An incremental upgrade eases the troubleshooting process.

Additional upgrade information

This section includes the following information for upgrading:

- During an upgrade, you might encounter messages while the installer validates the selected systems. These informational messages do not indicate an error. If an error occurs, the system's status confirms the problem.
- To perform this upgrade, use a rolling upgrade procedure that involves installing SFW 5.1 SP2 on the inactive nodes of a cluster. Use the **Move Group** command in MSCS or Microsoft Failover Clustering to move the active node and install SFW on the cluster's remaining nodes.

Upgrading DMPW 5.1 to SFW 5.1 SP2

Refer to the Hardware Compliance List on the Symantec Support web site at http://www.symantec.com/business/support/index.jsp to determine the approved hardware for SFW 5.1 SP2.

Connect no more than one path from the new host adapters to the array storage before upgrading to SFW 5.1 SP2 and uninstalling DMP DSMs. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.

Warning: Always back up your data before upgrading.

For upgrading DMPW 5.1 to SFW 5.1 SP2, use the sequence as follows:

- "Preparing an existing DMPW environment for upgrading" on page 41
- See "Upgrading to SFW 5.1 SP2" on page 42.

Preparing an existing DMPW environment for upgrading

If you are preparing to upgrade an existing DMP DSM environment, it is recommended to physically disconnect all but one path of the multipath storage to shorten upgrade time. It is important that you detach all but the primary path to the array storage before you uninstall.

Ensure that you have fulfilled the following before proceeding with the upgrade procedure:

- You must uninstall DMP DSM before the upgrade.
- Before uninstalling DMP DSM from a node in a cluster environment, the cluster resources should be moved to another node.
  See "Additional upgrade information" on page 40.

To uninstall DMPW

1. Make sure that only one path is attached for each array managed by DMP DSM.
2. Select **Actions** > **Rescan** from the VEA menu bar.
   Veritas Storage Foundation for Windows rescans the array and updates the display.
3. Uninstall DMPW using the Windows Add or Remove program through the installer.
   Click **Remove** to begin the uninstallation.
   See "Uninstalling DMPW through the GUI" on page 35.
4. After the uninstall process completes, reboot the system.

Upgrading to SFW 5.1 SP2

The installer automatically upgrades DMPW 5.1 to SFW 5.1 SP2.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 5-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 5-1 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either **Ignore** or **Warn**. On remote systems set the option to **Ignore** in order to allow the installation to proceed without user interaction.

To change the driver signing options on each system

1. Log on locally to the system.
2. Open the Control Panel and click **System**.
3. Click the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.
5. Click **OK**.
6. Repeat for each computer.
   If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Upgrading the software

Use the product installer to upgrade the software.

To upgrade to SFW 5.1 SP2

1. Allow the autorun feature to start the installation or double-click **Setup.exe**.
2. Choose the default language for your installation and click **OK**.
3. Click **Storage Foundation 5.1 SP2 for Windows**.
4. Click the **Complete/Custom** link. The installer starts to copy files.
5. Review the information on the Welcome page.
   Click **Next**.
6. Review the License Agreement. If you agree to the license terms, click the **I accept the terms of the license agreement** radio button.
   Click **Next**.
7. Enter license keys for each Symantec product option that you are upgrading or installing:
   - Enter the license key in the top field.
   - To add a key, click **Add**. To remove a key, click the key to select it, and click **Remove**.
   - Repeat the first two bulleted steps for each Symantec product and feature that you want to install. Click a key to see its details.
     Click **Next**.

   Choose the options that you want to install by selecting or clearing the appropriate check boxes. You must select all currently installed options for upgrade.
   Displayed at the bottom of the screen is the total hard disk space required for the installation. When you add or remove an option, the total space changes.
   Click **Next**.
8. Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.

Upgrading DMPW 5.1 to SFW 5.1 SP2

Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description.
Install Path	The install path cannot be changed for the upgrade.

9 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**.
Note that the Install Type for the nodes is listed as **Upgrade**.
If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

10 Review the pre-upgrade summary and click **Install**.
Click **Back** to make necessary changes.

11 If the installation is successful on all computers, the installer automatically proceeds to the summary page described in step 12.
If an installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the installation or uninstall and re-install. If a security alert asks you to accept the Symantec driver software, click **Yes**.

12 A report summarizing the upgrade appears. Review it and click **Next**.

13 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Perform the following steps in order.
- Select the upgraded remote computers.
- Click **Reboot**.
- Click **Next**.

14 Click **Finish**.

15 Click **Yes** to reboot the local computer.

16 After upgrading, reset the driver signing option to its original setting. Failure to do this can compromise system security. If you are performing more upgrades, do not reset the options until you have completed the upgrade.
See "Resetting the driver signing options" on page 45.

Resetting the driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1. Open the Control Panel, and click **System**.
2. Click the **Hardware** tab and click **Driver Signing**.
3. In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.
4. Click **OK**.
5. Repeat for each computer.

Chapter 6

Upgrading DMPW 5.1 to SFW HA 5.1 SP2

This chapter covers upgrading Dynamic Multi-Pathing 5.1 for Windows (DMPW 5.1) to Veritas Storage Foundation HA 5.1 SP2 for Windows (SFW HA 5.1 SP2).

This chapter contains the following topics:

Before upgrading DMPW 5.1 to SFW HA 5.1 SP2

Before upgrading, ensure that your system meets the supported minimum product version. You must also do some preparation for the upgrade.

To upgrade to SFW HA 5.1 SP2 your system must meet the minimum supported product versions, which the product installer checks before it upgrades.

If your current installation does not meet the minimum level required by the installer, Symantec recommends manually applying the appropriate product upgrades to meet the minimum product level required before proceeding with the installer. You can get intermediate versions of the products on the Symantec Support site.

http://www.symantec.com/business/support/index?page=home

For license keys, contact Symantec Sales. You can also uninstall the older versions of the product and install the new product.

Preparing for the upgrade

When upgrading the product, perform the following tasks:

- Back up all your data in a safe location.

- Back up the system state.
- Check the hardware requirements for the software upgrade.
- Test the system after each upgrade, especially after applying product upgrades to meet the minimum version required. An incremental upgrade eases the troubleshooting process.

Additional upgrade information

This section includes the following information for upgrading:

- During an upgrade, you might encounter messages while the installer validates the selected systems. These informational messages do not indicate an error. If an error occurs, the system's status confirms the problem.
- To perform this upgrade, use a rolling upgrade procedure that involves installing SFW 5.1 SP2 on the inactive nodes of a cluster. Use the **Move Group** command in MSCS or Microsoft failover clustering to move the active node and install SFW on the cluster's remaining nodes.

Upgrading from DMPW 5.1 to SFW HA 5.1 SP2

This section describes the following procedures for upgrading DMPW 5.1 to SFW HA 5.1 SP2.

- Preparing an existing DMPW environment for upgrading
- "Upgrading to SFW HA 5.1 SP2" on page 49

Refer to the Hardware Compliance List on the Symantec Support web site at to determine the approved hardware for SFW HA 5.1 SP2.

http://www.symantec.com/docs/TECH138719

Connect no more than one path from the new host adapters to the array storage before upgrading to SFW HA 5.1 SP2 and uninstalling DMP DSMs. Select the DMP DSM option or the appropriate DMP DSMs while running the installer.

Warning: Always back up your data before upgrading.

Preparing an existing DMPW environment for upgrading

If you are preparing to upgrade an existing DMP DSM environment, it is recommended to physically disconnect all but one path of the multipath storage

to shorten upgrade time. It is important that you detach all but the primary path to the array storage before you uninstall.

Ensure that you have fulfilled the following before proceeding with the upgrade procedure:

- You must uninstall DMP DSM before the upgrade.
- Before uninstalling DMP DSM from a node in a cluster environment, the cluster resources should be moved to another node.

To uninstall DMPW

1. Make sure that only one path is attached for each array managed by DMP DSM.
2. Select **Actions** > **Rescan** from the VEA menu bar.
   Veritas Storage Foundation for Windows rescans the array and updates the display.
3. Uninstall DMPW using the Windows Add or Remove program through the installer.
   Click **Remove** to begin the uninstallation.
   See "Uninstalling DMPW through the GUI" on page 35.
4. After the uninstall process completes, reboot the system.

Upgrading to SFW HA 5.1 SP2

The installer automatically upgrades DMPW 5.1 to SFW HA 5.1 SP2.

Changing driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 6-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 6-1 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed

Table 6-1 Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either **Ignore** or **Warn**. On remote systems set the option to Ignore in order to allow the installation to proceed without user interaction.

To change the driver signing options on each system

1. Log on locally to the system.
2. Open the Control Panel and click **System**.
3. Click the **Hardware** tab and click **Driver Signing**.
4. In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.
5. Click **OK**.
6. Repeat for each computer.
   If you do not change the driver signing option, the installation may fail on a system during validation. After you complete the installation, reset the driver signing option to its previous state.

Upgrading the software

Use the product installer to upgrade the software.

To upgrade the product using the installer

1. Allow the autorun feature to start the installation or double-click **Setup.exe.**
2. Choose the default language for your installation and click **OK**. The Symantec product selection screen appears.
3. Click **Storage Foundation HA 5.1 SP2 for Windows**.
4. Click **Complete/Custom** to begin installation. The **Administrative Console** link allows you to install only the Client components.

5 Review the information on the welcome page.
Click **Next**.

6 If you agree to the terms of the license agreement, click "**I accept the terms of the license agreement**", and then click **Next**.

7 Enter the license key for each Symantec product option that you are upgrading or installing in the top field.

8 To add a key, click **Add**.
To remove a key, click the key to select it, and click **Remove**.

9 Repeat step 7 and step 8 for each Symantec product and feature that you want to install. Click a key to see its details.

10 Click **Next**.

11 Select the domain and the computers for the upgrade and click **Next**.

Domain	Select a domain from the list. Depending on domain and network size, speed, and activity, the domain and computer lists can take some time to populate.
Computer	To add a computer for installation, select it from the Computer list or type the computer's name in the Computer field. Then click **Add**. To remove a computer after adding it, click the name in the Selected computers for installation field and click **Remove**. Click a computer's name to see its description.
Install Path	The install path cannot be changed for the upgrade.

12 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**. Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box, click **Validate Again**, and click **Next**.

13 Review the pre-upgrade summary. Click **Back** to make changes if necessary. Click **Install**.

14 If the installation is successful on all nodes, the installer automatically proceeds to the summary page.
Click **Next** after the progress indicator shows the installation is complete to proceed to the summary report in order to review the details of the failed installation. Note that if a security alert asks you to accept the Symantec driver software, click **Yes**.

15 Review the installation report, taking action where necessary, and click **Next**.

16 Reboot the remote computers. Note that you cannot reboot the local computer now, and that failed computers are unchecked by default. Select the upgraded remote computers and click **Reboot**.
Wait for the remote computer to come back online. Click **Next**.

17 Click **Finish**.

18 Click **Yes** to reboot the local node.

Resetting the driver signing options

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat for each computer.

Chapter 7

Migrating from EMC PowerPath to Veritas Dynamic Multi-Pathing 5.1 for Windows

This chapter contains the following topics:

Uninstalling EMC PowerPath and Installing DMPW

This section describes removing devices from EMC PowerPath (PP) control and enabling DMPW on the devices.

Prerequisites

Plan for system downtime. The migration steps may involve some system downtime on a host due to the following procedures:

- Stopping applications
- Stopping VCS services if using VCS

To uninstall EMC PowerPath and install Veritas Dynamic Multi-Pathing 5.1 for Windows, perform the following:

To remove devices from EMC PowerPath control and enable DMPW

1 Disable/disconnect all but one path from the host to the storage.

2 Remove the EMC PowerPath (PP).
Refer to the EMC instructions for removing PowerPath.

3 Reboot the system after the PowerPath has been removed.

4 Install the Veritas Dynamic Multi-Pathing 5.1for Windows (DMPW 5.1).

5 Under Dynamic Multi-Pathing, select MPIO Device Specific modules (DSMs) for the attached storage (for example, EMC CLARiiON and Hitachi AMS)

6 Reboot the node.

Configuring DMPW for Active/Active load balancing in a cluster

SCSI-3 is required for configuring Active/Active (A/A) load balancing in a clustered environment. SCSI-3 is enabled by default on Windows Server 2008 When DMPW is installed in a clustered environment.

For Windows Server 2003, SCSI-2 is enabled by default. Ensure to set SCSI-3 at array level before creating any disk resources in a cluster.

Note: If you are using MSCS on Windows Server 2003 or VCS for Windows and there are disk resources in the cluster, then the disks would get reserved using the SCSI-2 reservation policy. In this case, the DSM will support only Active/Passive (A/P) load balancing policy even if other load balancing policies are set.

If the disk resources have already been created before setting SCSI-3 support at array level, then they are reserved using SCSI-2 and A/A load balancing policies will not work on those disks.

To use A/A load balancing, enable SCSI-3 reservation for all disk under an array using the `vxdmpadm setarray` command. This ensures that the disks under the selected array will be reserved using SCSI-3 even if the cluster application issues SCSI-2 reservation for these disks.

Syntax for `vxdmpadm setarray` command:

```
vxdmpadm setarrayscsi3 scsi3support=1 <Harddisk name>.
```

Refer to the *Veritas Dynamic Multi-Pathing for Windows Administrator's Guide* for details.

Chapter 8

Migrating Hitachi Data Link Manager to Veritas Dynamic Multi-Pathing 5.1 for Windows

This chapter contains the following topics:

Uninstalling Hitachi Dynamic Link Manager (HDLM) and installing DMPW

This section describes removing devices from HDLM control and enabling DMPW on the devices.

Note: DMPW cannot co-exist with HDLM and hence, HDLM must be removed from a system before installing DMPW.

Plan for system downtime. The migration steps involve system downtime on a host due to the following:

- Stopping applications
- Stopping VCS services if using VCS
- Rebooting one or more hosts after uninstalling HDLM

Prerequisites

Back up all the data on the host where HDLM is installed. Also, if necessary,

back up the data on the management target device. Depending on the environment, uninstalling HDLM might take some time. Do not terminate the uninstallation process while a progress bar for uninstallation is displayed.

After HDLM is uninstalled, sometimes the following files listed below would not be deleted. The following files will be deleted when you restart the host:

- HDLM-installation-folder\DLMTools\perfhdlm\provhdlm.dll
- HDLM-installation-folder\lib\libdlm.dll
- HDLM-installation-folder\lib\hdlmhcc60.dll

The default installation folder for HDLM is Windows-installation-drive:

C: \Program Files\HITACHI\DynamicLinkManager. For Windows Server 2003 (excluding the x86 edition) or Windows Server 2008 (excluding the x86 edition), Program Files is Program Files (x86).

Refer to HDLM documentation for details.

Uninstalling HDLM in a non-Clustered environment

To uninstall HDLM in a non-clustered environment, perform the following steps. Refer to HDLM documentation for details:

1. Log on to Windows as a member of the Administrators group.
2. Stop all the processes and services that use the HDLM management-target paths.
   Stop any processes or application services, such as a DBMS, that are using the HDLM management-target paths.
   In Windows Server 2008, if you are not logged on as an administrator, use the Run as administrator functionality.
3. If the host and the storage subsystem are connected via multiple paths, reconfigure it so that only one path connects the host to the storage subsystem.
   After uninstalling HDLM, if you start the host in a multi-path configuration, the disk contents might become corrupted.
4. Start the uninstallation procedure.
5. When uninstallation finishes, a dialog box appears prompting you to restart the host.
   Click **OK** to restart the host.
6. Now, install the Veritas Dynamic Multi-Pathing (DMPW) 5.1 for Windows.

See "Installing DMPW using the product installer" on page 25.
See "Installing DMPW through the command line" on page 31.

Uninstalling HDLM in a clustered (MSCS or VCS) environment

To uninstall HDLM in an MSCS or VCS environment perform the following steps. Refer to HDLM documentation for details.

Uninstalling HDLM in a clustered (MSCS or VCS) environment

1. Log on to Windows as a member of the Administrators group.
2. Stop all the processes and services that use the HDLM management-target paths.
   Stop any processes or application services, such as a DBMS, that are using the HDLM management-target paths.
3. In Windows Server 2008, if you are not logged on as an administrator, use the Run as administrator functionality.
4. Stop MSCS or VCS on all the hosts that make up the cluster. When MSCS is used, follow this procedure:
   Choose **Administrative Tools** and then **Services**. In the list of services, right-click **Cluster Service**, and then from the **Action** menu choose **Stop** to stop the service.
   A message prompting you to restart the system might be displayed. If this happens, choose No.
5. If a host and a storage subsystem are connected via multiple paths, reconfigure it so that only one path connects the host to the storage subsystem
   Uninstalling HDLM in a multi-path configuration, might cause the disk contents to become corrupted when the host restarts. Make sure that you uninstall HDLM from a single path configuration only.
6. Start the uninstallation procedure.
7. When uninstallation finishes, a dialog box appears prompting you to restart the host.
   Click **OK** to restart the host.
8. Now, Install the Veritas Dynamic Multi-Pathing 5.1 for Windows 5.1
   See "Installing DMPW using the product installer" on page 25.
   See "Installing DMPW through the command line" on page 31.

Configuring DMPW for Active/Active load balancing in a cluster

SCSI-3 is required for configuring Active/Active (A/A) load balancing in a clustered environment. SCSI-3 is enabled by default on Windows Server 2008 When DMPW is installed in a clustered environment.

For Windows Server 2003, SCSI-2 is enabled by default. Ensure to set SCSI-3 at array level before creating any disk resources in a cluster.

Note: If you are using MSCS on Windows Server 2003 or VCS for Windows and there are disk resources in the cluster, then the disks would get reserved using the SCSI-2 reservation policy. In this case, the DSM will support only Active/Passive (A/P) load balancing policy even if other load balancing policies are set.

If the disk resources have already been created before setting SCSI-3 support at array level, then they are reserved using SCSI-2 and A/A load balancing policies will not work on those disks.

To use A/A load balancing, enable SCSI-3 reservation for all disk under an array using the `vxdmpadm setarray` command. This ensures that the disks under the selected array will be reserved using SCSI-3 even if the cluster application issues SCSI-2 reservation for these disks.

Syntax for `vxdmpadm setarray` command:

```
vxdmpadm setarrayscsi3 scsi3support=1 <Harddisk name>.
```

Refer to the *Veritas Dynamic Multi-Pathing for Windows Administrator's Guide* for details.

Index

V

W