



EMC® NetWorker®
Module for Microsoft Applications

Release 2.2

Installation Guide

P/N 300-008-850

REV A02

EMC Corporation

Corporate Headquarters:
Hopkinton, MA 01748-9103

1-508-435-1000

www.EMC.com

Copyright © 2007 - 2009 EMC Corporation. All rights reserved.

Published July, 2009

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Preface

Chapter 1 Introduction

Supported configurations..... 12

 Simple LAN-based configuration 12

 LAN-based configuration with a proxy client 13

 LAN-free configuration 14

Installation roadmap 16

Installation checklist..... 16

 Installation media 16

 Pathname 16

 License information..... 16

Installation requirements..... 17

 Privileged user level access 17

 Patches and hotfixes for NMM 2.2..... 17

 Patch for deduplication backup of NMM Client if using
NetWorker 7.5.1 server 18

 Exchange Server 2007 credentials 18

 SQL Server 2005 support 18

 Hardware requirements 18

 Software requirements..... 19

 Microsoft SQL and SharePoint VSS Writers 19

Installation directories..... 20

Chapter 2 Installing the Software

Installing NMM..... 22

 Access the installation files 22

 Install the software 23

Installing NMM in a MSCS environment..... 24

Verifying the installation..... 25

Maintaining the installation 25

 Changing the password or changing to a different authorized server.... 25

 Repairing the installation 26

Removing the software 26

Removing previous installation of Solutions Enabler 27

Upgrading the software 27

Upgrading to NMM storage node..... 27

Installing Microsoft Office SharePoint service pack 28

Chapter 3	Silent Installation of the Software	
	Overview	30
	Silent installation of NMM.....	30
	Commands for silent installation of NMM	30
	NetWorker NMM command line properties	31
	PowerSnap and Replication Manager command line properties	31
	Sample commands for silent installation of NMM	32
	Silent removal of NMM.....	32
	Commands for silent removal of NMM	32
	Sample scripts for installation and removal of NMM	33
	Installing and removing NMM by using SCCM 2007 Server	34
	Troubleshooting the installation	35
	Errors in installation of Replication Manager.....	35
	Using non-English characters in installation path	35
Chapter 4	Licensing and Enabling the Software	
	NMM client software licensing	38
	Add-on enabler names	38
	The evaluation process	39
	Evaluating a new installation	39
	Evaluating features on an existing installation.....	39
	The licensing process	40
	Type the license enabler code.....	40
	Obtain an authorization code.....	41
	Type the authorization code.....	42
	Update enablers.....	43
	Additional licenses.....	43
	Managing EMC licenses.....	44
Chapter 5	Configuring the Software	
	Using NMM with a VSS Hardware Provider.....	46
	Hardware array installation and configuration	46
	NMM installation and configuration for hardware provider support.....	47
	Setting up a proxy server for rapid backups of VSS snapshots.....	47
	Configurations specific to PowerSnap	47
	Configurations specific to CLARiiON	48
	Update the CLARiiON configuration file	48
	Update the SYMCFG authorization list.....	49
	Update the Navisphere Privileged Users list.....	49
	Configurations specific to Symmetrix.....	50
	Setting up the TimeFinder/Mirror (BCV) configuration for Symmetrix .	50
	Setting up the TimeFinder/Snap (VDEV) configuration for Symmetrix .	54
	Updating NMM settings with Exchange username, password, or domain ...	60
	Update account information in NMM for Exchange Server 2003.....	60
	Update Exchange Service account information in NMM for Exchange Server 2007	60
	Changing Replication Manager port settings	61
	Configuring NetWorker SharePoint services	62
	Matching NetWorker SharePoint Service credentials with credentials of SharePoint Server administrator.....	62
	Specifying temporary storage location	63
	Specifying the restore lock type	63

Configuring Windows firewall settings	64
Windows firewall exception error for irccd.exe.....	64
Manually creating NMM firewall exceptions.....	65

Index

As part of its effort to continuously improve and enhance the performance and capabilities of its product lines, EMC periodically releases revisions of its hardware and software. Therefore, some functions may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to the product release notes.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Audience

This guide is part of the EMC NetWorker Module for Microsoft Applications documentation set. It is intended for use by system administrators, during installation and setup of the product.

Readers should be familiar with the following technologies used in backup and recovery:

- ◆ EMC NetWorker software
- ◆ EMC NetWorker Snapshot management
- ◆ Microsoft Volume Shadow Copy Service (VSS) technology
- ◆ Storage subsystems, such as EMC CLARiiON or Symmetrix, if used

Related documentation

Related documents include:

- ◆ *EMC NetWorker Module for Microsoft Applications Release 2.2 Administration Guide*
- ◆ *EMC NetWorker Module for Microsoft Applications Release 2.2 Release Notes*
- ◆ *EMC NetWorker Release 7.5.x Multiplatform Version Administration Guide*
- ◆ *EMC NetWorker Release 7.5.x Multiplatform Version Installation Guide*
- ◆ *EMC NetWorker Release 7.5.x Multiplatform Version Release Notes*
- ◆ *EMC Information Protection Software Compatibility Guide*
- ◆ *EMC NetWorker License Manager Seventh Edition Installation and Administration Guide*
- ◆ *EMC Solutions Enabler Symmetrix CLI Version 6.3 Quick Reference*

Conventions used in this document

EMC uses the following conventions for special notices.

Note: A note presents information that is important, but not hazard-related.



CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: <ul style="list-style-type: none"> Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, utilities URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, notifications
Bold:	Used in running (nonprocedural) text for: <ul style="list-style-type: none"> Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system call, man pages Used in procedures for: <ul style="list-style-type: none"> Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) What user specifically selects, clicks, presses, or types
<i>Italic:</i>	Used in all text (including procedures) for: <ul style="list-style-type: none"> Full titles of publications referenced in text Emphasis (for example a new term) Variables
Courier:	Used for: <ul style="list-style-type: none"> System output, such as an error message or script URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
Courier bold:	Used for: <ul style="list-style-type: none"> Specific user input (such as commands)
<i>Courier italic:</i>	Used in procedures for: <ul style="list-style-type: none"> Variables on command line User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[]	Square brackets enclose optional values
	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces indicate content that you must specify (that is, x or y or z)
...	Ellipses indicate nonessential information omitted from the example

- Where to get help** EMC support, product, and licensing information can be obtained as follows.
- Product information** — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:
<http://Powerlink.EMC.com>
- Technical support** — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.
- Your comments** Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to:
techpubcomments@EMC.com

This chapter includes the following sections:

◆ Supported configurations	12
◆ Installation roadmap	16
◆ Installation checklist	16
◆ Installation requirements	17
◆ Installation directories	20

Supported configurations

EMC® NetWorker® Module for Microsoft Applications (NMM) can be set up in a LAN-based or LAN-free environment. These examples of supported configurations provide general software and hardware release information.

The current *EMC Information Protection Software Compatibility Guide* provides information on the supported hardware, software, and operating systems for the NetWorker Module for Microsoft Applications software..

Simple LAN-based configuration

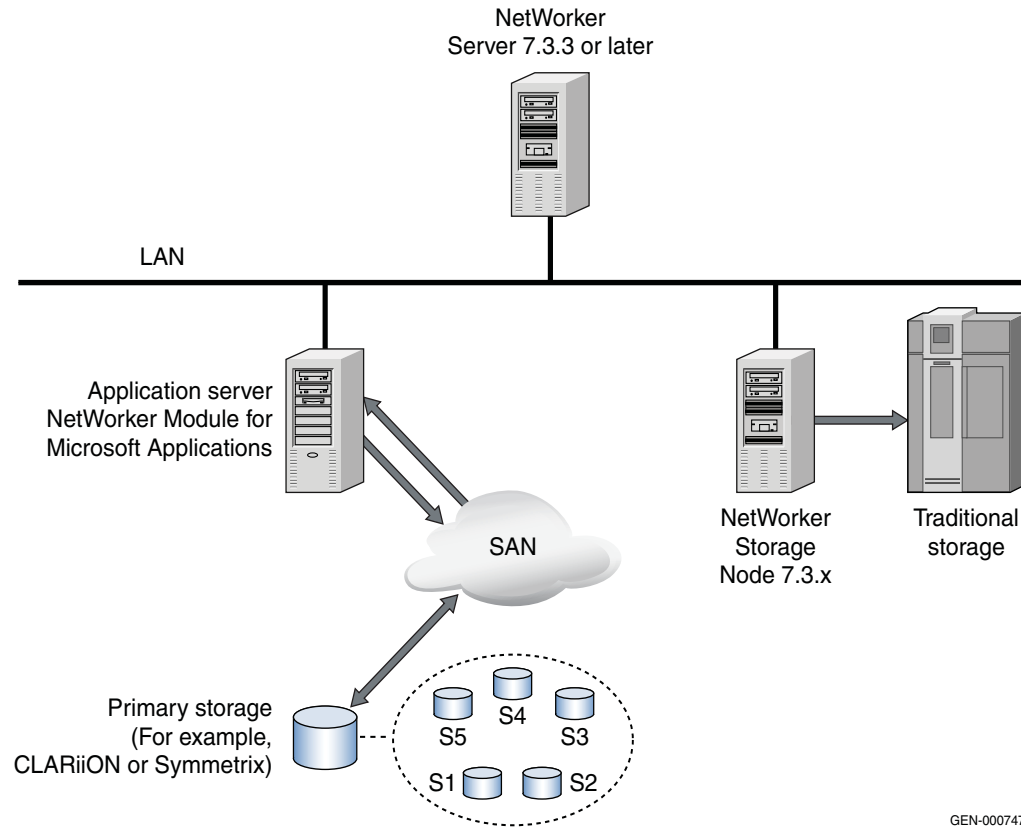
[Figure 1 on page 13](#) shows a simple LAN-based configuration with a storage area network. NMM is installed on the application server that is being protected.

The data moves as follows:

1. The NetWorker Server, which must be release 7.3.3 or later, initiates the process by contacting the application server where the NMM software is installed.
2. The application server with the NMM software creates a snapshot of the data on the storage volume.

Note: In [Figure 1 on page 13](#), snapshots are represented by S1 through S5.

The application server with the NMM software uses a snapshot in primary storage to transfer the data over the LAN and into traditional storage such as a file type disk, advanced file type disk, or tape.



GEN-00074;

Figure 1 Simple LAN-based configuration

LAN-based configuration with a proxy client

Figure 2 on page 14 shows a LAN-based configuration with a storage area network and a proxy client. NMM is installed on both the application server and the proxy client.

A proxy client is a host that acts as a remote data mover when snapshots are rolled over to traditional storage such as a file type disk, advanced file type disk, or tape. A proxy client frees resources on the application server by offloading the work of processing and backing up snapshots from the application server. When a backup operation uses a proxy client, it is known as a serverless backup.

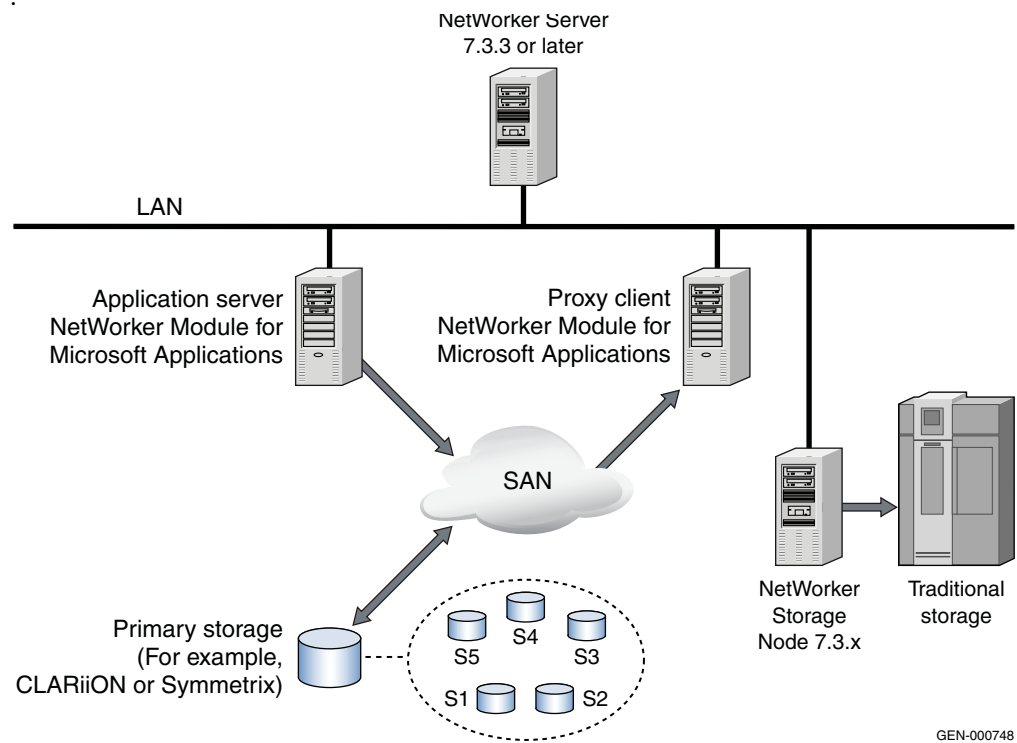
The data moves as follows:

1. The NetWorker Server initiates the process by contacting the application server where the NMM software is installed.
2. The application server with the NMM software creates a snapshot of the data on the storage volume.

Note: In Figure 2 on page 14, snapshots are represented by S1 through S5.

3. The snapshot is made visible to the proxy client.

- The proxy client uses a snapshot in primary storage to transfer the data over the LAN and into traditional storage such as a file type disk, advanced file type disk, or tape.



GEN-000748

Figure 2 LAN-based configuration with a proxy client

LAN-free configuration

[Figure 3 on page 15](#) shows a LAN-free configuration with a storage area network. The NMM Client is installed on the application server. The proxy client is installed on the NetWorker storage node.

You can set up a NetWorker storage node version 7.3.3 or later as a proxy client to avoid the network traffic that is generated when a snapshot is rolled over to a conventional backup medium. Network traffic is avoided because both the conventional backup device and the snapshot are directly attached to the storage node.

The data moves as follows:

- The NetWorker Server initiates the process by contacting the application server where the NMM software is installed.
- The application server with the NMM software creates a snapshot of the data on the storage volume.

Note: In [Figure 3 on page 15](#), snapshots are represented by S1 through S5.

- The snapshot is made visible to the proxy client.

- The proxy client, in this case the storage node, uses a copy in primary storage to transfer the data into traditional storage such as a file type disk, advanced file type disk, or tape.

The NetWorker Server and the application server communicate through the LAN. However, the data itself is not transferred across the LAN because the traditional storage is attached directly to the NetWorker storage node.

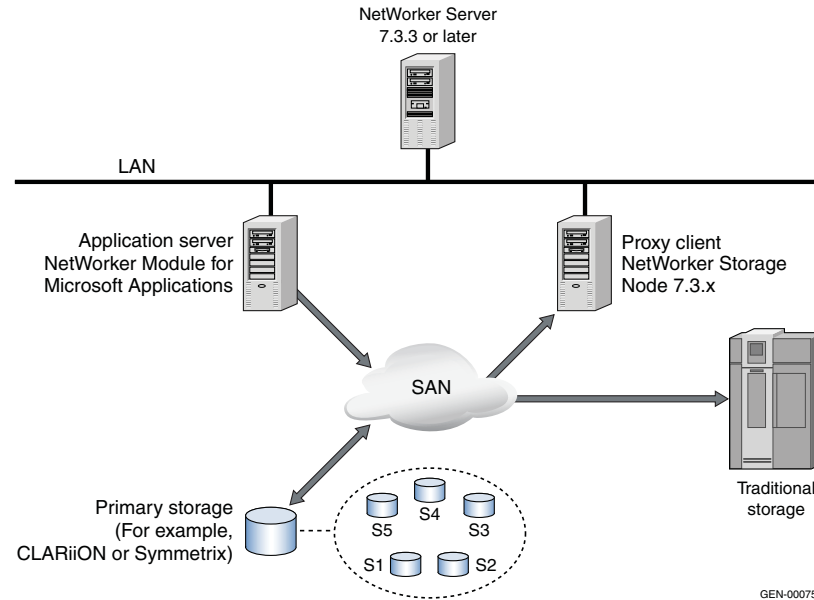


Figure 3 LAN-free configuration

Installation roadmap

Use the following roadmap when installing the software on supported Microsoft Windows platforms:

- ◆ Review “[Installation checklist](#)” on page 16 and ensure that you have all the required installation media, pathnames, and license information.
- ◆ Review “[Installation requirements](#)” on page 17 and ensure that you have the required software before installing NMM.
- ◆ Review “[Installation directories](#)” on page 20 and ensure that you have the required directories before installing NMM.
- ◆ Install the client according to the instructions given in [Chapter 2, “Installing the Software.”](#)
- ◆ After the installation is complete, configure the software components according to the instructions in [Chapter 3, “Silent Installation of the Software.”](#)

Installation checklist

Review the following checklist to ensure that you have the required media and information for the installation.

Installation media

The NMM software is distributed in the following formats:

- ◆ On a DVD included in the EMC media kit. The media kit contains software and online documentation for NMM and related NetWorker products.
- ◆ In the downloadable file of the evaluation software, available from the EMC website at <http://Powerlink.EMC.com>.

Pathname

The path of the NMM binaries is required for the installation.

License information

The following license information is required after the installation:

- ◆ NMM temporary evaluation enabler
- ◆ NetWorker base enabler
- ◆ NMM license add-on enabler

The NMM software requires a specific license: *NetWorker Module for Microsoft Applications*. This license must be installed on the NetWorker Server.

- ◆ NetWorker Client enabler

Although the NetWorker Client is included with the NMM software, make sure to purchase the NetWorker Client enabler.

[Chapter 3, “Silent Installation of the Software,”](#) provides more information on enablers and licensing.

Installation requirements

This section provides the installation requirements that must be met before installing the NMM software.

Privileged user level access

Because NMM requires access to protected server data and system files, NMM users must have administrator-level access privileges at all levels of operation:

- ◆ To install, configure, or repair NetWorker and NMM
- ◆ To run backup or recovery
- ◆ To configure or administer Windows Server, Microsoft applications servers such as Microsoft Exchange Server, SQL Server, DPM Server, or Office SharePoint Server
- ◆ To access other servers such as storage servers

Patches and hotfixes for NMM 2.2

In addition to the specific Microsoft Windows updates mentioned in this guide, make sure to keep NMM Client machine current with Microsoft Windows updates for the operating system, as well as updates and hotfixes for each installed Microsoft application protected by NMM. Otherwise NMM may not function correctly, or backup or recovery may fail. For example, the NMM UI may fail if the latest .NET updates are not installed.

The *EMC Module for Microsoft Applications Release 2.2 Release Notes* lists the Microsoft hotfixes that are required for NMM to work correctly. The hotfixes can be downloaded from the Microsoft website.

Patch for deduplication backup of NMM Client if using NetWorker 7.5.1 server

Make sure to install the patch, which is available at <ftp://ftp.legato.com/pub/NetWorker/Updates/NMM/NMM22/>. Without this patch, deduplication backup failure is observed when backups are performed by using a NetWorker 7.5.1 server and the error message

```
"50415:nsrsnap_vss_save:nsrsnap_vss_save: unable to extract key and value for argument '-A De-duplication'. Expecting '-A key=value' in this format.
69227:nsrsnap_vss_save:nsrsnap_vss_save: Failed to set value for a key=De-duplication" appears.
```

Exchange Server 2007 credentials

If Exchange Server 2007 is installed after NMM is installed, then NMM must be reinstalled after Exchange is installed. During NMM installation, add Exchange credentials. ["Installing NMM" on page 22](#) provides more information about initial setup of Exchange credentials during NMM installation.

SQL Server 2005 support

To successfully backup and restore SQL Server 2005 data, make sure that the Microsoft SQL hotfix KB934396 is installed on the client. To apply this hotfix, SQL Server 2005 Service Pack 2 must be installed.

Installation of Microsoft SQL Server 2005 Service Pack 3 includes this hotfix.

Hardware requirements

The following hardware requirements must be met before the installation:

- ◆ CPU: 2.0 GHz
- ◆ Physical memory: 1 GB
- ◆ Host architecture: x86 and x64 systems only

The current *EMC Information Protection Software Compatibility Guide* provides more information on the supported hardware, software, and operating systems for the NetWorker Module for Microsoft Applications software.

Software requirements

The current *EMC Information Protection Software Compatibility Guide* provides information on the supported hardware, software, and operating systems for the NetWorker Module for Microsoft Applications software.



CAUTION

To avoid potential data loss, do not install or use the NetWorker Module for Microsoft Applications with other vendor's VSS Requestor backup solutions. Data loss may occur if other VSS Requestor backup solutions delete shadowcopies created by the NetWorker Module for Microsoft Applications. Additionally, restoring an application by using another vendor's VSS Requestor backup solution may prevent the same application from being restored with the NetWorker Module for Microsoft Applications.

Microsoft SQL and SharePoint VSS Writers

If NMM is installed on a Microsoft Office SharePoint Server, make sure that the following Windows services have the startup type as Automatic and are running:

- ◆ SQL Server VSS Writer
- ◆ Windows SharePoint Services VSS Writer

If NMM is installed on a Microsoft SQL Server, make sure that the following Windows services have the startup type as Automatic and are running:

- ◆ SQL Server VSS Writer

Installation directories

When NMM is installed, the %ProgramFiles%\Legato\ directory are created by default. [Table 1 on page 20](#) lists the installation services for the NetWorker software, and PowerSnap™ and Replication Manager services.

Table 1 Services

Service names (in service control manager)	Service nicknames (use with the 'net start' command)	Process names
NetWorker Remote Exec	nsrexeecd	nsrexeecd.exe
NetWorker PowerSnap Service	nsrpsd	nsrpsd.exe
Replication Manager Client for RMAgentPS	rmagentps	irccd.exe

This chapter includes the following sections:

◆ Installing NMM	22
◆ Installing NMM in a MSCS environment	24
◆ Verifying the installation	25
◆ Maintaining the installation.....	25
◆ Removing the software.....	26
◆ Removing previous installation of Solutions Enabler	27
◆ Upgrading the software	27
◆ Upgrading to NMM storage node	27
◆ Installing Microsoft Office SharePoint service pack	28

Installing NMM



CAUTION

Remove all previous installations of NetWorker before installing NMM, except if you want to use the LAN-free configuration. In the LAN-free configuration, only the NetWorker Storage Node should be installed.

To install the NMM software on a Microsoft Windows computer, complete the following tasks:

- ◆ “Access the installation files” on page 22
- ◆ “Install the software” on page 23

Access the installation files

Access the installation files from one of the following sources:

- ◆ “From a DVD” on page 22
- ◆ “From the EMC website” on page 22

From a DVD

To access the NMM software from a local DVD:

1. Log in as administrator or equivalent on the NetWorker Server.
2. Insert the NMM DVD into the DVD drive.
3. Run **setup.exe** directly from the DVD.

From the EMC website

To access the evaluation version of the NMM software from the EMC Support website:

1. Go to <http://Powerlink.EMC.com>.
2. Select **Support > Software Downloads and Licensing > Downloads J-O > NetWorker Module**.
3. In the table of **NetWorker Module Software Downloads**, click the **NetWorker Module for Microsoft Applications Release 2.2**.

Install the software

Once you have accessed the NMM software files, you are ready to begin the installation. The NetWorker Client is included with the NMM software, and you are *not* required to install a NetWorker Client before installing the NMM software.

To install NMM:

1. Run the Setup program (**setup.exe**) to launch the installation wizard.
The **Welcome to NetWorker Module for Microsoft Applications Installation** wizard appears.
2. Click **Next**.
The **Customer Information** dialog box appears.
3. Type the name and organization information and click **Next**.
The **License Agreement** dialog box appears.
4. Read the license agreement. To accept, select the **I accept the terms in the license agreement** option, and click **Next**.
The **Installation Location** dialog box appears.
5. To choose an alternate location for the installation folder, click **Change** and select a different installation location. Click **Next**.
6. In the **Change Folder** dialog box, specify the alternate folder location and name, and click **OK**.
The **Replication Manager Client Setup** dialog box appears.
7. For **Control Port** and **Data Port**, specify two different port number values that will be used by the Replication Manager Client service. For most installations, the values supplied will be satisfactory.



CAUTION

EMC Replication Manager is also sold as a separate product. If you have purchased Replication Manager as a separate product, do not attempt to run the product on the same system as NMM.

You may change the Replication Manager port settings from the command line after the installation is complete. [“Changing Replication Manager port settings” on page 61](#) provides more information.

Note: Occasionally, an error message is displayed that installation was unable to create a Windows firewall exception for `irccd.exe`. [“Windows firewall exception error for `irccd.exe`” on page 64](#) provides steps to manually add the exception.

8. In the **Ready to Install** dialog box, click **Next** to start the NMM installation.
The installation may take several minutes.
If Microsoft Exchange Server is installed on the same installation machine, the **nwexinfo** dialog box appears. In the **nwexinfo** dialog box, type the Exchange Server domain information (**Domain**, **Username**, and **Password**) and click **OK**.
9. In the **NetWorker User Module for Microsoft Applications Setup Complete** window, click **Finish** to complete the installation and exit the installation wizard.

During the NMM installation, Replication Manager and PowerSnap services are installed along with the NMM software, and all three appear as separate entries under **Add/Remove Programs** in Microsoft Windows Server 2003, or **Programs and Features** in Microsoft Windows Server 2008.

10. Enable and register the NMM software according to instructions in [Chapter 4, "Licensing and Enabling the Software."](#)
11. Configure the setup according to instructions in [Chapter 5, "Configuring the Software."](#)

Installing NMM in a MSCS environment

When installing the NMM software in a Microsoft Cluster Server (MSCS) environment, if you plan to use CLARiiON or Symmetrix hardware with EMC VSS Provider, ensure that first Microsoft Distributed Transaction Coordinator (MSDTC) is installed and running before installing the EMC VSS Provider. The EMC VSS Provider will install EMC Solutions Enabler, and Solutions Enabler requires that MSDTC be running. The *EMC Solutions Enabler Version 6.3 Installation Guide* provides details about installing and running Solutions Enabler.

Note: EMC Solutions Enabler will be present only when using EMC VSS Provider.

To install the NMM software in a MSCS environment:

1. Install the NMM software on the private disk of each physical node.
2. Configure each physical node as a client resource on the NetWorker Server.
3. In the **Remote Access** attribute of each virtual client resource, type the names of the physical nodes.
4. Configure privileges for each physical node on the NetWorker Server:
 - a. In the **Users** attribute of the **Administrators** user group, add the following values for each physical node in the cluster. Add each value on a separate line:


```
user=administrator,host=VSS_cluster_node
```

```
user=system,host=VSS_cluster_node
```

 where *VSS_cluster_node* is the DNS hostname of the physical node.
 - b. Click **OK**.

The *EMC NetWorker Module for Microsoft Applications Release 2.2 Administration Guide* provides more information about configuring a clustered client resource.

The Microsoft website provides information about deploying Microsoft Exchange Server 2003 in a cluster.

Verifying the installation

Ensure that the following services are up and running:

- ◆ For NetWorker—**nsrexecd.exe**
- ◆ For PowerSnap—**nsrpsd.exe**
- ◆ For Replication Manager—**ircd.exe**

Maintaining the installation

After installing the NMM software, you may run the Setup program in maintenance mode to change, repair, or remove the existing client installation.

To run the Setup program in maintenance mode:

1. Log in as administrator on the client server.
2. To run the Setup program in maintenance mode, do one of the following:
 - Run the **setup.exe** file.
 - Select **Start > Settings > Control Panel > Add/Remove Programs**. Select the NetWorker Module for Microsoft Applications and click **Change**.

The **Welcome to NetWorker User Module for Microsoft Applications Maintenance** dialog box appears.

3. Click **Next**.

The Setup program detects the existing NMM installation and displays the **Maintenance Type** dialog box.


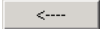
4. Select the type of maintenance to perform and click **Next**:
 - **Change** — Changes:
 - The password for Exchange Server using **nwexinfo**.
 - To a different authorized NetWorker Server.

[“Changing the password or changing to a different authorized server” on page 25](#) provides more information.
 - **Repair** — Replaces corrupt files and adds missing files, shortcuts, registries, and services. [“Repairing the installation” on page 26](#) provides more information.
 - **Remove** — Removes the NMM software from the system. [“Removing the software” on page 26](#) provides more information.

Changing the password or changing to a different authorized server

To change the password or change to a different authorized server:

1. Start the Setup program in the maintenance mode. [“Maintaining the installation” on page 25](#) provides more information.
2. In the **Maintenance Type** dialog box, select **Change** and click **Next**.
The **Ready to Change** dialog box appears.
3. In the **Ready to Change** dialog box, click **Change** to proceed.

4. In the **NetWorker Server Selection** dialog box, do any of the following:
 - a. Click **Update List** to browse for all the available servers, and click **Add** to add a server to the **Available Servers** list.
 - b. Select a server from the **Available Servers** list and click  to move the server to the **Selected Servers** list.
 - c. Select a server from the **Selected Servers** list and click  to return it to the **Available Servers** list.
 - d. Type a server name in the **Enter a server name** field.



CAUTION

If an authorized server list is used together with a proxy server, then the proxy server must also authorize the production server, and the production server authorize the proxy server.

5. Click **Next**.

The selected NetWorker Server is used to back up the data on the client. If you have not selected an alternate server, the default server is used to back up the data on the client.

Repairing the installation

To repair the software installation:

1. Start the Setup program in the maintenance mode. [“Maintaining the installation” on page 25](#) provides more information.
2. In the **Maintenance Type** dialog box, select **Repair** and click **Next**.
3. In the **Ready to Repair** dialog box, click **Repair** to proceed.

The Setup program repairs the NMM software. The process may take several minutes.

Removing the software

To remove the NMM software:

1. Start the Setup program in the maintenance mode. [“Maintaining the installation” on page 25](#) provides more information.
2. In the **Maintenance Type** dialog box, select **Remove** and then click **Next**.
3. In the **Ready to Remove** dialog box:
 - a. Select the **Remove NetWorker User Module for Microsoft Applications Metadata** option.

The Legato and rmagentps directories, and the Legato and RMSservice registry entries are removed.

- b. Check the **Remove NetWorker User Module for Microsoft Applications Metadata** option to remove the existing metadata. If you want to keep the existing metadata for installation of NMM 2.2, then leave the **Remove NetWorker User Module for Microsoft Applications Metadata** option cleared.

- c. Click **Remove**.

Removing NMM, also removes the PowerSnap and Replication Manager services. The three entries for these programs are removed from under **Add/Remove Programs** in the **Control Panel**.

Removing previous installation of Solutions Enabler

To uninstall Solutions Enabler:

1. Stop the Solutions Enabler services before uninstalling the Solutions Enabler software by using the following command:

```
net stop storapid
```

2. Select **Start > Settings > Control Panel > Add/Remove Programs**, and select **EMC Solutions Enabler**.
3. Click **Remove**.

Upgrading the software

A direct upgrade of an existing installation of NMM or NetWorker VSS Client to NMM 2.2 cannot be done. Before installing NMM release 2.2, remove any existing version of NMM or NetWorker VSS Client by running the Setup program in maintenance mode, and selecting the Remove option. You may decide to keep the existing metadata for installation of NMM 2.2. [“Removing the software” on page 26](#) provides more information.

Upgrading to NMM storage node

NMM supports upgrading NetWorker 7.3.3 or later to NMM storage node.

To upgrade to NetWorker Module for Microsoft Applications storage node:

1. Ensure that you have installed the NetWorker storage node on the server.

The *EMC NetWorker Release 7.5.x Multiplatform Version Installation Guide* provides information about installing the NetWorker storage node.

2. Install the NMM software. [“Installing NMM” on page 22](#) provides more information.

When the NMM installation detects that a NetWorker storage node is already installed on the server, a message window appears. It states that an existing NetWorker storage node installation has been detected, and asks if you want to install the NetWorker Module for Microsoft Applications Client as the storage node.

3. Click **OK** to upgrade to NMM storage node.

The NMM storage node is installed.

Although the PowerSnap service and Replication Manager service binaries are installed on the existing storage node during the upgrade procedure, the NMM storage node cannot be used as the NMM Client.

Installing Microsoft Office SharePoint service pack

Microsoft Office SharePoint Service Pack 1 (SP1 or later) must be installed. Without this fix installed on SharePoint machines, NMM may incorrectly list the presence of the SharePoint Help Search Writer (SPSearch Writer) on a SharePoint machine that does not actually have the writer. This could lead to a user creating an invalid saveset, and backup or recovery failure.

Go to the Microsoft website and search for “Microsoft Office SharePoint Server 2007 Service Pack 1 (SP1).” Download and install this on all machines in the SharePoint Server farm. Once it is installed, no further action is required for NMM.

When installing SP1 on a SharePoint farm, Microsoft recommends installing it in a specific order:

1. Start the SP1 installation on all machines at the same time.
2. When the **Proceed** message box is displayed, click **OK** on all remote clients, but do not click **OK** to proceed on the web front end yet.
3. After installation completes on all remote clients, click **OK** on all remote clients, and then click **OK** to proceed with installation on the web front end.
4. Start the SharePoint configuration wizard.

This chapter includes the following sections:

◆ Overview	30
◆ Silent installation of NMM.....	30
◆ Silent removal of NMM.....	32
◆ Sample scripts for installation and removal of NMM	33
◆ Installing and removing NMM by using SCCM 2007 Server	34
◆ Troubleshooting the installation	35

Overview

This release of NMM 2.2 provides support for:

- ◆ Silent (unattended) installation and removal of the software on a stand-alone server.
[“Silent installation of NMM” on page 30](#) and [“Silent removal of NMM” on page 32](#) provide more information.
- ◆ Remote installation and removal of the software by using Microsoft System Center Configuration Manager 2007 (SCCM) Server.
[“Installing and removing NMM by using SCCM 2007 Server” on page 34](#) provides more information.

Silent installation of NMM

Silent installation of NMM 2.2 is a stand-alone method that uses the command line and scripts. In this process, all the information that is required for a successful installation is gathered by the Setup file (setup.exe) from the command line, which makes any GUI dialog boxes unnecessary. You may type full setup.exe commands directly in the command line, or may include such commands in scripts and save it as a .cmd file.

In a basic silent installation, first the NetWorker software is installed, and then the PowerSnap and Replication Manager services.

The silent (unattended) installation status log files are available in the client computer’s temp directory. For fast access to the temp directory, use **Start > Run**, and type **%temp%**.

Note: The following are not supported in this release of NMM:

1. Silent installation of NMM as a storage node
2. Silent installation, if Microsoft Exchange Server is installed on the same installation machine

Commands for silent installation of NMM

[Table 2 on page 30](#) lists the commands for silent installation of NMM 2.2.

Table 2 **Commands for silent installation of NMM**

Option	Description
<code>setup /s /v"qb"</code>	Silent installation with progress bar.
<code>setup /s /v"qn"</code>	Basic installation with no progress bar.
<code>setup /s /v"/qn /L*v """"%TEMP%\filename.log""""</code>	Installs NMM and creates a MSI log file. This command is useful for troubleshooting installation problems. The log file is created in the %TEMP% directory. Make sure to use triple quotes in the command in case the %TEMP% path contains spaces.

NetWorker NMM command line properties

Table 3 on page 31 lists the command line properties that are recognized for NetWorker NMM.

Table 3 NetWorker NMM command line properties

Property	Value	Description
INSTALLDIR	default = %SystemDrive%\Program Files\Legato\nsr	Changes the installation directory for NMM. To specify a pathname that contains spaces, use the following syntax: INSTALLDIR=""c:\program files\legato"". Make sure to use triple quotes in the syntax.
NW_REMOVEMETADATA	{0 1}default = 0 (leave metadata)	When removing NMM, if the value is set to 1, the metadata is removed.
NW_SERVERS	default = <no NW servers name specified>	By default, the \res\server file is blank when the "servers" command is not used or no name is used after the "server" command. To create the SERVERS file with a list of NetWorker servers to back up the NMM Client, use the following syntax: SERVERS=""srv1 srv2"". Make sure to use triple quotes when specifying more than one server. The use of triple quotes when specifying one server is optional.

PowerSnap and Replication Manager command line properties

Table 4 on page 31 lists the command line properties that are recognized for PowerSnap and Replication Manager.

Table 4 PowerSnap and Replication Manager command line properties

Property	Value	Description
ALLUSERS	1	Always set value to 1.
VSSREG	0	Always set value to 0.
REBOOT	S	Suppress Reboot. Always set value to S.
ADDLOCAL (x86)	Proxy, Host, VSS, and EMCRecoverPoint	Features to be installed for x86. All values must be specified.
ADDLOCAL (x64)	Proxy, Host, and VSS	Features to be installed for x64. All values must be specified.
DORMINST	1	Install Replication Manager. Always set value to 1.
DORMINST_VSS	1	Always set value to 1.
DORMINST_EXCH	{1 0}	To install Exchange, set value to 1, otherwise set value to 0.
RMCPORT	default = 6728	Specify Replication Manager control port.
RMDPORT	default = 6729	Specify Replication Manager data port.

Sample commands for silent installation of NMM

This section contains sample commands that you can use for silent installation of NetWorker, PowerSnap, and Replication Manager.

Sample 1

This sample command contains all the properties that can be passed from the command line for NetWorker. These properties are optional. In this sample command, NetWorker is installed in the C:\Legato\nsr directory, a MSI log file is created in %TEMP%\filename.log directory, and a *SERVERS* file containing the server names server1 and server2 is created:

```
\networkr\setup.exe /s /v"/qn /L*v "" "%TEMP%\filename.log" ""
INSTALLDIR="" "c:\Legato\nsr" "" SERVERS="" "server1 server2" ""
"/w
```

Sample 2

Use these sample commands for installing the PowerSnap and Replication Manager services. All the properties in the samples must be passed from the command line when installing the PowerSnap and Replication Manager services. None of the properties are optional. When the PowerSnap service is installed, the Replication Manager service is also installed.

PowerSnap/Replication Manager silent install for nt86

```
\networkr\ps\setup.exe /s /v"/qb ALLUSERS=1 VSSREG=0 REBOOT=S
RMCPORT=6728 RMDPORT=6729 DORMINST=1 DORMINST_EXCH=0
DORMINST_VSS=1 ADDLOCAL=Proxy,Host,VSS,EMCRecoverPoint"/w
```

PowerSnap/Replication Manager silent install for ntx64

```
\networkr\ps\setup.exe /s /v"/qb ALLUSERS=1 VSSREG=0 REBOOT=S
RMCPORT=6728 RMDPORT=6729 DORMINST=1 DORMINST_EXCH=0
DORMINST_VSS=1 ADDLOCAL=Proxy,Host,VSS"/w
```

Silent removal of NMM

In a silent removal of NMM 2.2, first the PowerSnap service is removed and then the NetWorker software. When the PowerSnap service is removed, the Replication Manager service is also removed.

Commands for silent removal of NMM

Use the following command to remove PowerSnap and Replication Manager services:

```
\networkr\ps\setup.exe /s /v"/qn /L*v
"" "%TEMP%\PSinstall.log" "" "/x
```

Use the following command to remove NetWorker, create a MSI log file, and remove the metadata:

```
\networkr\setup.exe /s /v"/qn /L*v
"" "%TEMP%\NMMinstall.log" "" "NW_REMOVEMETADATA=1" /x
```

Sample scripts for installation and removal of NMM

[Table 5 on page 33](#) lists sample scripts that you can use during the installation and removal of NMM. All of these samples are included in the NMM 2.2 installation media kit, in the directory where `setup.exe` is located.

Each sample script creates a log in the `%TEMP%` directory, whose name is the same as the script, the only difference being that the file extension `.cmd` is replaced by `.log`. For example, the log for `install_nmm_silent_sample.cmd` is named `install_nmm_silent_sample.log`. These logs can be used to troubleshoot installation problems.

The `install_nmm_silent_sample.cmd` script is used for the silent installation of the NMM 2.2 software. The `install_nmm_silent_sample.cmd` script is the master script, and executes all the scripts in [Table 5 on page 33](#), except for `uninstall_nmm_silent_sample.cmd`.

The `install_nmm_silent_sample.cmd` script does the following in the order listed next:

1. Checks if NMM or NetWorker is installed. If either is installed, the script exits.
2. Installs the Microsoft .NET Framework 2.0, if it is not installed.
3. Installs the Microsoft VC80 side-by-side redistributable DLLs.
4. Installs NetWorker.
5. Installs the PowerSnap and Replication Manager services.
6. Configures the Windows firewall.

You can modify these sample scripts to provide correct installations for your environment.

Table 5 Sample scripts for silent installation

Script name	Description
<code>install_nmm_silent_sample.cmd</code>	Silently installs the NMM 2.2 software. This sample script can be modified by the customer.
<code>uninstall_nmm_silent_sample.cmd</code>	Silently removes the NMM 2.2 software. This sample script can be modified by the customer.
<code>NMMInstalled.vbs</code>	Determines if NMM or NetWorker is currently installed.
<code>DotNetInstalled.vbs</code>	Determines if Microsoft .NET Framework 2.0 is currently installed.
<code>DotNetInst.cmd</code>	Installs Microsoft .NET Framework 2.0.
<code>NMMConfigFW.vbs</code>	Configures the Windows firewall for NMM.

The `install_nmm_silent_sample.cmd` script uses the `%~dp0\setup /s /v"/qn /L*v """"%TEMP%\NMMinstall.log"""" " /w` command to install NMM, and uses the default installation path and leaves `res\server` file blank.

To install NMM in a different location and have the NetWorker Server name listed in `res\servers` file, use `@rem %~dp0\setup /s /v"/qn /L*v """"%TEMP%\nmminstall.log""""
INSTALLDIR=""c:\Legato""NW_SERVERS=""serv1 serv2"" " /w
 command. By default, this command is disabled by rem in install_nmm_silent_sample.cmd file.`

Installing and removing NMM by using SCCM 2007 Server

To install NMM 2.2 by using the Microsoft System Center Configuration Manager (SCCM) 2007 server:

1. Use the **New Collection Wizard** to specify the client machine, where the NMM 2.2 software is to be installed.
2. Copy the NMM 2.2 installation package to the local drive on SCCM Server and specify a local SCCM machine name as a new distribution point for the distribution package.
3. Use the **New Package Wizard** to create a software distribution package. Specify general information, data source, distribution settings, and other information for the new package.
4. Use the **New Program Wizard** to create a installation program for a software distribution package:

Note: To simplify the source installation command used by SCCM Server, the `install_nmm_silent_sample.cmd` and `uninstall_nmm_silent_sample.cmd` files containing all the necessary scripts to install and remove NMM respectively are created as examples in the installation kit `\networkr` directory. ["Sample scripts for installation and removal of NMM" on page 33](#) provides details about the scripts' function.

- a. To use the `Install_nmm_silent_sample.cmd` file as a source installation file in SCCM Server, start the **New Program Wizard**, click **Browse** in the **General Tab**, select **Show all files**, and select the `install_nmm_silent_sample.cmd` file in `/networker` directory.
- b. In **Environment Wizard**, window make sure that the administrative rights are set to **Run Mode**. Use the default setting for all other options, and click **Close** to complete program creation.
5. Use the **New Advertisement Wizard** to create an advertisement. Specify general information, package name, program, and the collection to which the advertisement should be distributed:
 - a. For schedule option, select **Run as soon as possible**.
 - b. For delivery method, use **Run program from distribution point**.
 - c. For all other options, use default setting to complete **New Advertisement Wizard**.

Once the advertisement is created, the SCCM Server is set up to install the software. The **Advertisement Status** section in SCCM Server can be used to check the installation process status. It may take more than 30 minutes for the SCCM Server to process the advertised installation.

The SCCM server installation status log files are available in the client computer's C:\Windows\temp directory. For fast access to the temp directory, use **Start > Run**, and type %SystemRoot%\temp.

To remove NMM 2.2 by using the SCCM 2007 Server:

- ◆ The steps to remove NMM by using the SCCM Server are the same as that of installing NMM on the SCCM Server. Instead of using the install_nmm_silent_sample.cmd file, use uninstall_nmm_silent_sample.cmd file.

Troubleshooting the installation

This section provides tips to troubleshoot errors that may appear during installation, when moving from a previous release of NMM or NetWorker VVS Client to NMM 2.2, or if NMM is not running correctly after a fresh installation.

Errors in installation of Replication Manager

Most frequently, a problem in the installation is due to errors in the installation of Replication Manager services.

1. Check **Add/Remove Programs** in Microsoft Windows Server 2003, or **Programs and Features** in Microsoft Windows Server 2008. The NMM software, and Replication Manager and PowerSnap services should appear installed. The Replication Manager entry appears as RMagentPS:
 - a. If NMM, PowerSnap service or Replication Manager service is missing, remove all, and then reinstall.

Remove the programs in the following order:
 1. Replication Manager service
 2. PowerSnap service
 3. NMM software
 - b. Reinstall.
2. If all the three programs appear to be installed but not running, or you get an error about a service not starting, verify that the services for NMM, PowerSnap, and Replication Manager are running. If any of the services is not running, remove and reinstall all of the programs as described in [step a](#).

If **irccd.exe** is not running, but **nsrexecd.exe** and **nsrpsd.exe** are running, then manually install the Replication Manager service from the following directory networkr\ps\rmc\setup.exe.

Using non-English characters in installation path

During silent or GUI installation, make sure not to use non-English characters in the installation path because although NetWorker seems to be installed properly, the installation of PowerSnap service and Replication Manager service fail and an error message appears.

This chapter includes the following sections:

- ◆ NMM client software licensing 38
- ◆ The evaluation process 39
- ◆ The licensing process 40
- ◆ Update enablers 43
- ◆ Managing EMC licenses 44

NMM client software licensing

The NetWorker software is installed in evaluation mode. The licensing of NetWorker software means entry of enabler and authorization codes on the server for the NetWorker environment. Without these codes, the software or added features will not run beyond the evaluation period.

Each installation of NMM client must be licensed with an enabler that activates the software and allows you to use the software. All licensing takes place on the server. The licenses are typed and stored on the server, and the server enforces the licensing.

Base enablers come in different editions, which enable varying degrees of functionality. Add-on enablers allow a broader scope of features.

Add-on enabler names

The specific add-on enabler for the NMM client is *NetWorker Module for Microsoft Applications*. The enabler name for NMM may vary depending on which version of NetWorker is installed, whether NetWorker Server has been upgraded, and in what order it was installed or upgraded:

- ◆ If an NMM add-on enabler is installed on NetWorker 7.4 SP2 or later, the add-on enabler is displayed as *NetWorker Module for Microsoft Applications*.
- ◆ If an NMM add-on enabler is installed on NetWorker prior to release 7.4 SP2, the add-on enabler is displayed under the old VSS license name *Volume Shadowcopy Service for Windows*. If the same NetWorker Server is then upgraded to NetWorker 7.4 SP2 or later, the existing add-on enabler is still displayed under the old VSS license name *Volume Shadowcopy Service for Windows*.
- ◆ If an older version of NetWorker Server, with an add-on enabler that uses the old name, is upgraded to NetWorker Server 7.4 SP2 or later, and then a new NMM add-on enabler is installed, then the new add-on enabler is displayed as *NetWorker Module for Microsoft Applications* in addition to the old enabler *Volume Shadowcopy Service for Windows*. Even though both names are present, the enablers will be combined and used correctly as different client systems claim them.

The steps in this chapter assume that all of the software and hardware requirements have been met and the NMM client software is installed.

The evaluation process

Evaluating NMM client software can take place in two ways:

- ◆ By evaluating a new installation of the software on a Windows Server
- ◆ By evaluating NetWorker features on an existing NetWorker installation

Evaluating a new installation

When you first install the NMM client software, you can evaluate it with all the modules and features for 30 days free without typing any codes.

By the end of the evaluation period, you must purchase, type, and authorize a base enabler to continue to use the NMM client software to restore data. The base enabler is the license that enables the edition purchased.

To continue to use the modules and features that were available with the evaluation software, you might need to purchase the NMM client add-on enabler, depending on the edition of the base enabler.

Evaluating features on an existing installation

If you are evaluating one or more NMM client modules or features on an edition of the software that has already been installed and enabled, you must type a temporary enabler for each module or feature. The temporary enabler is valid for 45 days.

Contents documentation in the *EMC Information Protection and Availability Product Families Media Kit* and [“Where to get help” on page 9](#) provide information about how to obtain a temporary enabler code.

[“Typing a temporary enabler code” on page 39](#) provides information about how to type the temporary enabler code. By the end of the evaluation period, you must purchase, type, and authorize the corresponding license enablers to continue to use modules or features evaluated by you. [“The licensing process” on page 40](#) provides instructions.

Typing a temporary enabler code



CAUTION

The temporary enabler code is valid on only one computer in a network. If you type the same code on more than one computer in a network, a copy protection violation error occurs and the NMM client software is disabled on all NetWorker Servers with duplicate enablers.

To type the temporary enabler code:

1. Start the NetWorker Management Console software.
2. Launch the **Administration** window:
 - a. From the **Console** window, click **Enterprise**.
 - b. From the left pane, select a NetWorker Server in the **Enterprise** list.
 - c. From the right pane, select the application.
 - d. From the **Enterprise** menu, click **Launch Application**.

The **Administration** window is launched as a separate application.

3. From the **Administration** window, click **Configuration**.
4. In the left pane, select **Registration**.
5. From the **File** menu, select **New**.
6. In the **Enabler Code** attribute, type the enabler code.
7. In the **Name** attribute, type the name of the license.
8. (Optional) In the **Comment** attribute, type a description of the license.
9. Click **OK**.

The licensing process

To permanently use NMM client software, you must purchase and type a license enabler code, and then authorize it. This licensing process is the same for all editions of software as well as for individual modules and features.

The license enabler code that you purchase is valid for 45 days, as a registration period. During the registration period, you must obtain and type a corresponding authorization code.

The following sections explain how to type and authorize the license enabler:

- ◆ [“Type the license enabler code” on page 40](#)
- ◆ [“Obtain an authorization code” on page 41](#)
- ◆ [“Type the authorization code” on page 42](#)

Type the license enabler code

License enabler codes are included in either the letter announcing the updated or upgraded software, or on the Enabler Certificate you receive when you purchase a software license. This depends on whether the software purchased is a first-time purchase or an updated or upgraded version.

Note: To save time when typing multiple licenses, type the base enabler last. Otherwise, once a base enabler is typed, devices that do not yet have licenses typed may be disabled. Those devices would have to be reenabed manually after their licenses are installed.

To type the license enabler code:

1. Start the NetWorker Management Console software.
2. Launch the **Administration** window:
 - a. From the **Console** window, click **Enterprise**.
 - b. From the left pane, click a NetWorker Server in the **Enterprise** list.
 - c. From the right pane, click the application.
 - d. From the **Enterprise** menu, select **Launch Application**. The **Administration** window is launched as a separate application.
3. In the **Administration** window, click **Configuration**.
4. In the left pane, select **Registrations**.
5. From the **File** menu, select **New**.

The **Create Registration** dialog box appears.

6. In the **Enabler Code** attribute, type the enabler code.
7. In the **Name** attribute, type the name of the license.
8. (Optional) In the **Comment** attribute, type a description of the license.
9. Click **OK**.

The new license is added and appears in the right pane. Repeat the procedure to add any additional enabler codes. After you type a license enabler code, you have 45 days as a registration period to authorize the NMM client software.

Obtain an authorization code

Registration of NMM client software takes place by obtaining an authorization code. Obtain a unique authorization code through one of the following methods:

- ◆ “Using the EMC website” on page 41
- ◆ “Using email” on page 41



CAUTION

If the software or feature is not authorized by the end of the 45-day registration period, the NMM client function or feature is disabled.

Using the EMC website

Register products and obtain authorization codes online by completing a registration form on the EMC website at <http://Powerlink.EMC.com>. Web registration takes just a few minutes and is available 24 hours a day, 7 days a week.

An authorization code that permanently enables the NetWorker license is sent by email.

Using email

To register the software and obtain an authorization code by email:

1. Start the NetWorker Management Console software.
2. Launch the **Administration** window:
 - a. From the **Console** window, click **Enterprise**.
 - b. From the left pane, select a NetWorker Server in the **Enterprise** list.
 - c. From the right pane, click the application.
 - d. From the **Enterprise** menu, select **Launch Application**. The **Administration** window is launched as a separate application.
3. In the **Administration** window, click **Configuration**.
4. In the left pane, select the NetWorker Server.
5. From the **File** menu, select **Properties**.
The **Properties** dialog box appears.
6. Click the **Customer Information** tab and complete your contact information.
7. Email your registration information. For contact information, go to the EMC CustomerNet portal at <http://Powerlink.EMC.com>.

An authorization code that permanently enables the updated NetWorker software is sent to you.

Type the authorization code

To complete the licensing process, you must type the unique authorization code on the NetWorker Server within 45 days of typing the license enabler code.

If the authorization process is successful, the expiration date for the license displays "Authorized - No expiration date." If the authorization is not verified in this way, contact <http://Powerlink.EMC.com>.

To avoid an interruption in restores, if you move the NMM client software from one computer to another, or to change the network address of a computer after the software is installed, perform one of the following:

- ◆ Obtain a new authorization code. You need the host ID of the original server as well as the new server. The host ID appears in the server's Registration window.
- ◆ Install and configure the License Manager software. "Managing EMC licenses" on page 44 and the latest *EMC NetWorker License Manager Installation Guide* provide more information about using the License Manager.

To type the authorization code:

1. Start the NetWorker Management Console software.
2. Launch the **Administration** window:
 - a. From the **Console** window, click **Enterprise**.
 - b. From the left pane, select a NetWorker Server in the **Enterprise** list.
 - c. From the right pane, click the application.
 - d. From the **Enterprise** menu, select **Launch Application**.

The **Administration** window is launched as a separate application.
3. In the **Administration** window, click **Configuration**.
4. In the left pane, select **Registration**.
5. In the right pane, select a license.
6. From the **File** menu, select **Properties**.
7. In the **Auth Code** attribute, type the authorization code for the product (the authorization code assigned to the specified permanent enabler or update enabler code).
8. Click **OK**.

The license is now permanently enabled.

Update enablers

To update existing NMM client software to a major release (one that introduces important new features), an update enabler is necessary. Update enablers are required for any major NetWorker software update, including the current NetWorker release. To use the License Manager, the NetWorker Server must be release 5.0 or later.

With a first-time purchase of NMM client software, a one-year update agreement might be included. After one year, an update enabler may be acquired with a new update agreement purchase.

Additional licenses

This section describes a few of the additional licenses required to operate some of the NetWorker features.

Client connection licenses

Every computer to be restored in a NetWorker datazone requires a client connection license, even the NetWorker Server. The client connection license may be one of the licenses supplied with the base enabler or purchased separately. A cluster client or NDMP data server requires a special type of client connection license, as described in [“Cluster clients” on page 43](#) or [“Managing EMC licenses” on page 44](#).

NetWorker application modules

NetWorker application modules are licensed on the basis of one enabler per database type host. For example, to back up the Exchange database on two hosts, two NetWorker module for Exchange enablers are required, even if the two hosts are backed up by the same server.

However, if multiple database instances are running on a NetWorker Client host, only one NetWorker module enabler is required for that one host.

Cluster clients

For each physical node in a cluster, you must purchase a Cluster Client Connection, which takes the place of one standard client connection. The *EMC NetWorker Release 7.5.x Multiplatform Version Administration Guide* provides more information on licensing computers in a cluster.

Managing EMC licenses

The License Manager provides centralized license management, allowing you to maintain all of an enterprise's NetWorker licenses from a single computer. With the License Manager, you can move NMM client software from one computer to another, or change the IP address on an existing NetWorker Server without having to reauthorize the software. The License Manager can be installed as an option during NMM client software installation.

To begin to implement the License Manager:

1. Contact Licensing to obtain bulk enabler codes. Go to <http://Powerlink.EMC.com> for more information.
2. Install the License Manager software.
3. Configure the License Manager software.
4. Configure the NetWorker Servers to access the License Manager for their licenses.

The *EMC NetWorker License Manager Installation Guide* provides details on installing and using the License Manager.

This chapter includes the following sections:

- ◆ Using NMM with a VSS Hardware Provider..... 46
- ◆ Setting up a proxy server for rapid backups of VSS snapshots..... 47
- ◆ Configurations specific to PowerSnap 47
- ◆ Configurations specific to CLARiON 48
- ◆ Configurations specific to Symmetrix 50
- ◆ Updating NMM settings with Exchange username, password, or domain 60
- ◆ Changing Replication Manager port settings 61
- ◆ Configuring NetWorker SharePoint services 62
- ◆ Configuring Windows firewall settings 64
- ◆ Manually creating NMM firewall exceptions 65

Using NMM with a VSS Hardware Provider

NMM can use a VSS Hardware Provider for persistent snapshots or off-host backups. To enable these to work together, use the following processes to configure the hardware array and NMM:

- ◆ “Hardware array installation and configuration” on page 46
- ◆ “NMM installation and configuration for hardware provider support” on page 47

Hardware array installation and configuration

Perform the following steps for hardware array installation and configuration:

1. Install and license the appropriate snapshot software for the array:
 - For EMC CLARiON:
 - SnapView™ Clone
 - SnapView Snapshots
 - For EMC DMX/Symmetrix:
 - TimeFinder®/Mirror
 - TimeFinder/Snap

“Configurations specific to Symmetrix” on page 50 provides details.
 - For EMC Celerra: Celerra Snapshots
 - For Dell EqualLogic PS Series: EqualLogic Snapshots
 - For IBM System Storage DS6000/DS8000: IBM FlashCopy
2. Install the appropriate HBA drivers and Windows VSS/VDS hotfixes.
3. Install the appropriate host-based EMC storage software, such as PowerPath®, Navisphere® host-based utilities, as required by the supporting array and customer environment.
4. Install the appropriate VSS HW Provider on the Windows Server hosting the application:
 - For EMC VSS Common Provider for EMC Symmetrix, Symmetrix DMX™ and CLARiON arrays:
 - The EMC VSS Common Provider is available on Powerlink at <http://Powerlink.EMC.com>.
 - Release notes for the EMC VSS Common Provider can be found on Powerlink at <http://Powerlink.EMC.com>.
 - For EMC Celerra VSS Provider for Celerra arrays: The EMC Celerra VSS Provider is available on Powerlink at <http://Powerlink.EMC.com>.
 - For Dell/EqualLogic Integration ToolKit for EqualLogic PS Series arrays: Check with Dell for access and support information.
 - For IBM DS6000 and DS8000 arrays:

The IBM System Storage DS Open API Package is available at <http://www-1.ibm.com/support/docview.wss?uid=ssg1S4000372&rs=555>.
 - For Windows Unified Data Storage Server (WUDSS):

Check Microsoft documentation for access and support information.

5. Configure LUNs for Clones or Snapshots as required.
6. Verify that the VSS HW Provider is available for use:
 - a. Run **vssadmin list providers** on the application server.
 - b. Test if the hardware provider is functioning properly using **VSHADOW.exe** in Windows Server 2003 or **DISKSHADOW.exe** in Windows Server 2008 to validate creation of hardware snapshots.

NMM installation and configuration for hardware provider support

To install and configure NMM for hardware provide support:

1. Install the NMM Client on the Windows Server hosting the application.
2. Configure a NetWorker Client scheduled backup as needed for the application:
 - a. Configure a snapshot policy to match application requirements.
 - b. Configure a backup group, referencing the snapshot policy.
 - c. Configure a client resource as required for the application, including NetWorker User Group entries.
 - d. Configure a proxy client if required, including NetWorker User Group entries.
3. Run and test the NMM scheduled backup.

Setting up a proxy server for rapid backups of VSS snapshots

To be able to take rapid backups of VSS snapshots created by NMM, you can set up the NMM software or the NMM storage node to act as the proxy client. The storage node acts as the proxy client in a SAN-based storage node configuration.

The *EMC NetWorker Module for Microsoft Applications Release 2.2 Administration Guide* provides more information.

Configurations specific to PowerSnap

If you do not have administrative rights and are running programs, add the username for the account that is logged in to the server:

1. Set the PowerSnap NetWorker security using *NMC* (from **Configuration > User Groups**).
2. Add the following values to the Administrators User Group for the production host and proxy host:

user=Administrator,host=<fqdn>

For example:

- For production host:
user=system,host=bv-clsrv.belred.emc.com
- For proxy host:
user=system,host=qe2.belred.emc.com

Configurations specific to CLARiiON

The CLARiiON documentation provides information about how to configure CLARiiON storage arrays. Additionally, ensure that the following configuration tasks are performed:

1. [“Update the CLARiiON configuration file” on page 48](#)
2. [“Update the SYMCFG authorization list” on page 49](#)
3. [“Update the Navisphere Privileged Users list” on page 49](#)

If a CLARiiON array is migrated, or the information in the CLARiiON configuration is not up-to-date, rollback may fail. If there is more than one entry in the CLARiiON clarcnfg file, Replication Manager only uses the first entry. If the clarcnfg file is not current, the first entry may be pointing to a CLARiiON that is no longer connected to the system. Edit the clarcnfg file so that there is only entry, pointing to the current CLARiiON you want to use.

Update the CLARiiON configuration file

To support Replication Manager, edit the CLARiiON configuration file (clarcnfg) with the CLARiiON array name and the IP addresses or DNS hostnames of the two storage processors that exist in each CLARiiON machine.

The clarcnfg file is located in the
%ProgramFiles%\EMC\SYMAPI\config\clarcnfg directory.

Use the following sample configuration file template as a guide when adding values to your CLARiiON configuration file. Obtain the values from the CLARiiON array configuration.

```
#####
#                               CLARiiON CONFIGURATION FILE TEMPLATE
# This CLARiiON configuration file provides network addresses
# (hostnames or IP addresses) for the two Storage Processors on
# each CLARiiON which can be seen by this host. To load
# information about CLARiiON systems, CLARAPI must be able to
# communicate with the Navisphere Agent that administers them.
# CLARAPI Discovery depends on valid entries in this file.
#
# CLARiiON Arrayname      Storage Processor A      Storage Processor B
# XXXXXXXXXXXX            losat246                  losat247
#
#                               APM00052211461          10.5.221.132          10.5.221.133
```

Update the SYMCFG authorization list

The SYMCFG authorization list must be updated to support the EMC VSS Provider. Use the following example to update the SYMCFG authorization list for your configuration. In the following example, the two hostname IP addresses identify the two storage processors that exist on each CLARiiON machine:

1. Update the SYMCFG authorization list with the hostname IP address, username, and password for storage processor A. For example:

```
%ProgramFiles%\EMC\SYMCLI\bin>>symcfg authorization add -host 10.5.221.132 -username gadmin -password rdc4xyz
```

2. Update the SYMCFG authorization list with the hostname IP address, username, and password for storage processor B. For example:

```
%ProgramFiles%\EMC\SYMCLI\bin>>symcfg authorization add -host 10.5.221.133 -username gadmin -password rdc4xyz
```

3. Verify that the SYMCFG authorization list has been updated correctly. For example:

```
%ProgramFiles%\EMC\SYMCLI\bin>>symcfg authorization list
```

Hostname	Username
-----	-----
10.5.221.132	gadmin
10.5.221.133	gadmin

Update the Navisphere Privileged Users list

EMC Navisphere is a software that enables the management of CLARiiON storage systems. To create a secure environment, update the EMC Navisphere Privileged Users list with the DNS hostname or IP address of the CLARiiON storage processors (SPA and SPB).

Type values in the Privileged Users list in the following format:

```
system@hostname_SPA
```

```
system@hostname_SPB
```

where *hostname_SPA* and *hostname_SPB* are the DNS hostnames or IP addresses of the CLARiiON storage processors.

The *EMC Navisphere Manager Administrator's Guide* provides more information about adding entries to the Privileged Users list.

Configurations specific to Symmetrix

The following sections describe how to set up Symmetrix for data protection. Before you begin, determine the Symmetrix technology that you will be using for data protection and the number of persistent snapshots that will be required.

The two primary options are:

- ◆ TimeFinder/Mirror, based on Symmetrix BCVs — Symmetrix BCVs are appropriate for data protection scenarios where you want to retain the snapshot as a backup copy for a full volume restore or rollback.
- ◆ TimeFinder/Snap, based on Symmetrix VDEVs — Symmetrix VDEVs are appropriate for temporary snapshot data protection scenarios where the snapshot is only used to create the backup copy to disk or tape and then deleted.

The initialization of Symmetrix for these two technologies is quite different. The TimeFinder/Clone technology also exists, but is currently not qualified with NMM. However, the command set for TimeFinder/Clone is very much like TimeFinder/Snap.

For the following discussion, it is assumed that Symmetrix volumes 8B and 8C are being backed up using BCVs and Symmetrix volumes 7D and 7E, which are being backed up with VDEVs. Further, it is assumed that two snapshots a day are going to be created.

Note: If both BCVs and VDEVs are available for use with an STD, then the determination of the backup being a Copy-On-Write copy (snapshot) or a full copy (BCV) is made by the EMC VSS Provider.

Setting up the TimeFinder/Mirror (BCV) configuration for Symmetrix

The TimeFinder/Mirror technology is a full copy technology where a Business Continuance Volume (BCV) is mirrored or *established* to a production volume, referred to as a Standard Device (STD). While being established, the BCV synchronizes with the STD and once fully synchronized any new writes to the STD are copied to the BCV as well. When the BCV is disconnected from the STD, also known as *split*, it becomes a point-in-time copy of the STD.

The relationship between a BCV and a STD can be thought of as permanent until the BCV is mirrored to a different STD. Once fully synchronized and split the Symmetrix tracks change to either the STD and BCV. When the two are reestablished, the tracks that were changed on STD are copied to the BCV. Any tracks that have changed on the BCV is refreshed from the STD so that the BCV is once again a full mirror of the STD.

Preparation of TimeFinder/Mirror for use with a proxy consists of the establishing one or more BCVs to the production volume (STD) and waiting for them to become synchronized. Note that if more than two BCVs are required then the first BCVs will need to be split after they have become synchronized in order to allow new BCVs to be synchronized.

Solutions Enabler's SYMCLI is used to do this work. The SYMCLI is very flexible and in many cases there is more than one way to accomplish a given task. The procedures described in this section reflect the simplest steps whenever possible. In the example, the BCV volumes are B6, B7, B8 and B9. The example establishes B6 and B7 to volume 8B, and B8 and B9 to volume 8C.

Setting up the device group and establishing mirrors with BCVs on Symmetrix

This section contains instructions for setting up the device group and establishing mirrors with BCVs on Symmetrix. A device group is a SYMCLI object created on hosts. It is a logical grouping of production volumes (STDs) and copy volumes (BCVs, VDEVs, and so on).

For all other options, use the **-help** option with any SYMCLI command. The *EMC Solutions Enabler Symmetrix CLI Version 6.3 Quick Reference* or *EMC Solutions Enabler Symmetrix TimeFinder Family CLI Version 6.3 Product Guide* provides more information about using the **-help** option.

To set up the device group, complete the following tasks:

1. Create a device group.

To create a device group, use the following command:

```
symdg create <device group name>
```

For example:

```
symdg create mgrp
```

2. Add devices to the device group.

The STDs is assigned a logical name based on the order in which they are entered. To add a STD device to the device group, use the following command:

```
symlid -sid <Symm ID> -g <group> add dev <Symm device>
```

For example:

```
symlid -sid 829 -g mgrp add dev 8b
```

```
symlid -sid 829 -g mgrp add dev 8c
```

The Symmetrix ID is typically the *last digits* of Symmetrix's serial number to make it unique if there is more than one Symmetrix that can be seen by the host.

After the STD device is added, to add a BCV to the device group, use the following command:

```
symbcv -g <device group name> -sid <Symm id> add dev <symm device name>
```

For example:

```
symbcv -sid 829 -g mgrp add dev b6
```

```
symbcv -sid 829 -g mgrp add dev b7
```

```
symbcv -sid 829 -g mgrp add dev b8
```

```
symbcv -sid 829 -g mgrp add dev b9
```

3. Verify the group.

To check what is in a group, use the following command:

```
symdg show <group name>
```

For example:

```
symdg show mgrp
```

Figure 4 on page 52 displays the output.

```

Group Name: mgrp

Group Type                : REGULAR
Device Group in GNS      : No
Valid                     : Yes
Symmetrix ID             : 000190300829
Group Creation Time      : Fri Jun 12 16:08:50 2009
Vendor ID                 : EMC Corp
Application ID           : SYMCLI

Number of STD Devices in Group      : 2
Number of Associated GK's           : 0
Number of Locally-associated BCU's  : 4
Number of Locally-associated VDEV's : 0
Number of Locally-associated TGT's  : 0
Number of Remotely-associated VDEV's(STD RDF): 0
Number of Remotely-associated BCU's (STD RDF): 0
Number of Remotely-associated TGT's(TGT RDF) : 0
Number of Remotely-associated BCU's (BCU RDF) : 0
Number of Remotely-assoc'd RBCU's (RBCU RDF) : 0
Number of Remotely-assoc'd BCU's (Hop-2 BCU) : 0
Number of Remotely-assoc'd VDEV's(Hop-2 VDEV): 0
Number of Remotely-assoc'd TGT's (Hop-2 TGT) : 0

Standard (STD) Devices (2):
{
-----
LdevName          PdevName          Sym  Att.  Sts  Cap
Dev              Dev              Dev  Att.  Sts  (MB)
-----
DEV001            \\.\PHYSICALDRIVE14  008B  RW    4314
DEV002            \\.\PHYSICALDRIVE15  008C  RW    4314
}

BCU Devices Locally-associated (4):
{
-----
LdevName          PdevName          Sym  Att.  Sts  Cap
Dev              Dev              Dev  Att.  Sts  (MB)
-----
BCV001            N/A              0086  NR    4314
BCV002            N/A              0087  NR    4314
BCV003            N/A              0088  NR    4314
BCV004            N/A              0089  NR    4314
}

```

Figure 4 Output of verify the group command

4. Perform the initial device establish.

For the initial establish of the STDs to their partner BCVs, use the following command:

```

symmir -g <device group name> establish <STD logical device>
bcv ld <BCV logical device>

```

For example:

```

symmir -g mgrp establish DEV001 bcv ld BCV001 -full
symmir -g mgrp establish DEV001 bcv ld BCV002 -full
symmir -g mgrp establish DEV002 bcv ld BCV003 -full
symmir -g mgrp establish DEV002 bcv ld BCV004 -full

```

5. Query the mirror state.

Do not initiate a backup until the BCVs are fully synchronized. To check the state of the mirrors, use the following command:

```
symmir -g <device group name> query -multi
```

For example,

```
symmir -g mgrp query -multi
```

Figure 5 on page 53 displays the output.

Standard Device			BCV Device			State
Logical	Sym	Inv. Tracks	Logical	Sym	Inv. Tracks	STD <=> BCV
DEV001	008B	0	BCV002	0087 *	0	Synchronized
		0	BCV001	0086 *	0	Synchronized
DEV002	008C	0	BCV004	0089 *	0	Synchronized
		0	BCV003	0088 *	0	Synchronized
Total		-----			-----	
Track(s)		0			0	
MB(s)		0.0			0.0	

Figure 5 Output of query the mirror state command

When at least one BCV for each production volume is synchronized the system is ready to be used for NMM backups. If more BCVs are needed to cover the number of snapshots then the currently synchronized BCVs must be manually split with the following command:

```
symmir -g <group> split <logical device> bcv ld <logical device>
```

For example:

```
symmir -g mgrp split DEV001 bcv ld BCV001
```

```
symmir -g mgrp split DEV001 bcv ld BCV002
```

```
symmir -g mgrp split DEV002 bcv ld BCV003
```

```
symmir -g mgrp split DEV002 bcv ld BCV004
```

At this point another pair of BCVs can be established to the STDs and synchronized. Once the BCVs are established with an STD, the BCVs are rotated by the EMC VSS Provider as needed.

6. Rerun the mirror query after the backup.

Once the backup is complete, it is useful to rerun the mirror query command.

Figure 6 on page 54 displays the output.

```

Device Group (DG) Name: mgrp
DG's Type           : REGULAR
DG's Symmetrix ID   : 000190300829
  
```

Standard Device			BCV Device			State
Logical	Sym	Inv. Tracks	Logical	Sym	Inv. Tracks	STD <=> BCU
DEV001	008B	0	BCV001	0086 *	0	Synchronized
		0	BCV002	0087 *	0	Split
DEV002	008C	0	BCV003	0088 *	0	Synchronized
		0	BCV004	0089 *	0	Split
Total		-----			-----	
Track(s)		0			0	
MB(s)		0.0			0.0	

Figure 6 Output of mirror query rerun command

Notice that one BCV for each production volume is split from its STD. These are the copies that were used to make the backup.

During subsequent backups, all the BCVs will most likely be seen to be in the split state. What happens is that when a backup is requested the EMC VSS Provider establishes BCV to each of the production volumes. When the BCVs are synchronized the EMC VSS Provider then splits them and the actual backup starts.

Setting up the TimeFinder/Snap (VDEV) configuration for Symmetrix

The TimeFinder/Snap technology is a copy-on-write technology, where a virtual device (VDEV) is connected paired to a STD (production volume). The pairing is done by creating a *session* between the STD and VDEV. Once paired with an STD the VDEV can be *activated* at which moment it becomes a copy-on-write snapshot of the STD for that point-in-time.

Note: The VDEV is really a block of logical pointers that are initially set to point to the STD. As new writes are made to the STD the old data is first copied to a persistent Save Device (SDEV) that backs up the VDEV. The logical pointer on the VDEV for that data region is then updated to point to the old data on the SDEV.

SDEVs are allocated to named pools. The default pool is named DEFAULT_POOL. When a session between a STD and VDEV is created the pool for the SDEVs must be specified. NMM currently is limited by underlying technology to using the default pool.

Unlike a BCV, when a *terminate* operation is done to a VDEV, its relationship to a particular STD stops and the SDEVs connected with that VDEV are freed.

In the example, the STD volumes being backed up are Symmetrix devices 7D and 7E. Symmetrix VDEVs DF -> EE use the SDEVs from the default pool for persistent storage.

Preparing for backups with NMM is only necessary to create the initial sessions between a STD and the VDEVs that are used as snapshots.

In the examples used in the following tasks, the STD volumes that are backed up are Symmetrix devices 7D and 7E. Symmetrix VDEVs DF -> EE then uses the SDEVs from the default pool for persistent storage.

To set up the TimeFinder Snap configuration for Symmetrix, complete the following tasks:

1. Add SDEVs to a pool.

Note: This step might not be necessary depending on how the Symmetrix has been configured. It is provided for completeness.

To add SDEVs to a pool, use the following command:

```
symconfigure -sid <Symm Id> -cmd "ADD DEV <sdev device range> TO POOL DEFAULT_POOL TYPE=SNAP MEMBER_STATE=ENABLE;"
commit
```

For example:

```
symconfigure -sid 829 -cmd "ADD DEV F7:107 TO POOL
DEFAULT_POOL TYPE=SNAP MEMBER_STATE=ENABLE;", commit
```

2. Create a device group.

To create a device group, use the following command:

```
syndg create <group name>
```

For example:

```
syndg create sgrp
```

3. Add devices to the device group.

Next add the STDs to the device group. The STDs will be assigned a logical name based on the order in which they are entered.

To add a device to the device group, use the following command:

```
symld -sid <Symm ID> -g <group> add dev <Symm device>
```

For example:

```
symld -sid 829 -g sgrp add dev 7d
```

```
symld -sid 829 -g sgrp add dev 7e
```

The Symmetrix ID is typically enough *last digits* of Symmetrix's serial number to make it unique if there is more than one Symmetrix that can be seen by the host.

After the STD volumes are added, to add the VDEV devices, use the following command:

```
symld -sid <Symm ID> -g <group> add dev <Symm device> -vdev
```

For example:

```
symld -sid 829 -g sgrp add dev df -vdev
```

```
symld -sid 829 -g sgrp add dev e0 -vdev
```

```
symld -sid 829 -g sgrp add dev e1 -vdev
```

```
symld -sid 829 -g sgrp add dev e2 -vdev
```

4. Verify the group.

To check what is in a group, use the following command:

```
syndg show <group name>
```

For example:

```
syndg create sgrp
```

5. Create the initial sessions.

To create initial sessions, use the following command:

```
symsnap -g <group> create -svp <pool name> <STD logical name> vdev ld <VDEV logical name> -nop
```

For example:

```
symsnap -g sgrp create -svp DEFAULT_POOL DEV001 vdev ld  
VDEV001 -nop
```

```
symsnap -g sgrp create -svp DEFAULT_POOL DEV001 vdev ld  
VDEV002 -nop
```

```
symsnap -g sgrp create -svp DEFAULT_POOL DEV002 vdev ld  
VDEV003 -nop
```

```
symsnap -g sgrp create -svp DEFAULT_POOL DEV003 vdev ld  
VDEV004 -nop
```

Figure 7 on page 57 displays the output.

```

Group Name:  sgrp

Group Type           : REGULAR
Device Group in GNS : No
Valid                : Yes
Symmetrix ID        : 000190300829
Group Creation Time  : Mon Jun 15 16:29:53 2009
Vendor ID            : EMC Corp
Application ID       : SYMCLI

Number of STD Devices in Group      : 2
Number of Associated GK's           : 0
Number of Locally-associated BCU's  : 0
Number of Locally-associated VDEV's : 4
Number of Locally-associated TGT's  : 0
Number of Remotely-associated VDEV's(STD RDF): 0
Number of Remotely-associated BCU's (STD RDF): 0
Number of Remotely-associated TGT's(TGT RDF) : 0
Number of Remotely-associated BCU's (BCU RDF) : 0
Number of Remotely-associ'd RBCU's (RBCU RDF) : 0
Number of Remotely-associ'd BCU's (Hop-2 BCU) : 0
Number of Remotely-associ'd VDEV's(Hop-2 VDEV) : 0
Number of Remotely-associ'd TGT's (Hop-2 TGT) : 0

Standard (STD) Devices (2):
{
-----
LdevName          PdevName          Sym   Att.  Sts   Cap
Dev              (MB)
-----
DEV001            \\.\PHYSICALDRIVE7 007D   RW    4314
DEV002            \\.\PHYSICALDRIVE8 007E   RW    4314
}

VDEV Devices Locally-associated (4):
{
-----
LdevName          PdevName          Sym   Att.  Sts   Cap
Dev              (MB)
-----
VDEV001           N/A               00DF   NR    4314
VDEV002           N/A               00E0   NR    4314
VDEV003           N/A               00E1   NR    4314
VDEV004           N/A               00E2   NR    4314
}

```

Figure 7 Output of initial sessions

6. Query the snap state.

The state of the snapshots is done with the following command.

```
symsnap -g <group> query -multi
```

For example:

```
symsnap -g sgrp query -multi
```

Figure 8 on page 58 displays the output.

```

Device Group (DG) Name: sgrp
DG's Type           : REGULAR
DG's Symmetrix ID   : 000190300829
    
```

Source Device			Target Device			State	Copy
Logical	Sym	Protected Tracks	Logical	Sym	G	Changed Tracks	SRC <=> TGT (%)
DEV001	007D	69030	UDEV002	00E0	X	0	Created 0
		69030	UDEV001	00DF	X	0	Created 0
DEV002	007E	69030	UDEV004	00E2	X	0	Created 0
		69030	UDEV003	00E1	X	0	Created 0
Total							
	Track(s)	276120				0	
	MB(s)	17257.5				0.0	

Legend:
(G): X = The Target device is associated with this group,
. = The Target device is not associated with this group.

Figure 8 Output of querying the snap state command

7. Running snapshot againquery after the backup.

At this point the system is ready to be used for NMM backups. Once the backup is complete, run the following commands:

- a. Run the snapshot query again.

Figure 9 on page 58 displays the output.

```

Device Group (DG) Name: sgrp
DG's Type           : REGULAR
DG's Symmetrix ID   : 000190300829
    
```

Source Device			Target Device			State	Copy
Logical	Sym	Protected Tracks	Logical	Sym	G	Changed Tracks	SRC <=> TGT (%)
DEV001	007D	69026	UDEV002	00E0	X	4	CopyOnWrite 0
		69030	UDEV001	00DF	X	0	Created 0
DEV002	007E	69025	UDEV004	00E2	X	5	CopyOnWrite 0
		69030	UDEV003	00E1	X	0	Created 0
Total							
	Track(s)	276111				9	
	MB(s)	17256.9				0.6	

Legend:
(G): X = The Target device is associated with this group,
. = The Target device is not associated with this group.

Figure 9 Output of running the snapshot query command again

- b. The second command is a similar view, but is done by pool. Note that this command displays all the sessions that are using SDEVs in the pool, and not just the ones that are yours.

```
symsnap -svp <pool> list
```

For example:

```
symsnap -svp DEFAULT_POOL list
```

Figure 10 on page 59 displays the output.

Symmetrix ID: 000190300829

Source Device		Target Device		Status	SaveDev
Sym	Protected Tracks	Sym	G SRC <=> TGT		PoolName
007D	69030	00DF	X	Created	DEFAULT_POOL
007D	69026	00E0	X	CopyOnWrite	DEFAULT_POOL
007E	69030	00E1	X	Created	DEFAULT_POOL
007E	69025	00E2	X	CopyOnWrite	DEFAULT_POOL
Total		-----			
Tracks	276111				
MB(s)	17256.9				

Legend:

(G): X = The Target device is associated with a group,
 . = The Target device is not associated with a group.

Figure 10 Output of second command of running the snapshot query again

Updating NMM settings with Exchange username, password, or domain

If changes are made to the Microsoft Exchange Services account, changes may be necessary in the NMM settings to continue NMM access to the account. The steps for updating the Exchange username or account information in NMM are different for Exchange Server 2003 and Exchange Server 2007.

Update account information in NMM for Exchange Server 2003

When NMM is installed on an Exchange Server 2003, the **nwexinfo.exe** utility runs as part of the NMM installation. This utility updates the NMM software with the Exchange username, password, and domain.

Run the **nwexinfo.exe** utility again if:

- ◆ The Exchange Server is installed after the NMM is installed.
- ◆ The username, password, or domain changes after the NMM is installed.

To run the **nwexinfo.exe** utility, double-click the **nwexinfo.exe** file from the *%ProgramFiles%\Legato\nsr\bin* directory.

Update Exchange Service account information in NMM for Exchange Server 2007

When changes are made to the Exchange Services account in Exchange Server 2007, the username and account information must be updated in:

- ◆ The Replication Manager-supplied Exchange 2007 Service for NMM.
- ◆ The COM registration associated with that Replication Manager-supplied Exchange 2007 Service for NMM.

Changing Replication Manager port settings

The Replication Manager port settings are specified during the NMM installation. However, you can use the following procedure to change the Replication Manager port settings after NMM is installed.

To change the Replication Manager port settings:

1. From the command line, stop the **rmagentps** service.

For example:

```
net stop rmagentps
```

2. From the *%ProgramFiles%\EMC\rmagentps\client\bin* directory, run the **irccd** command to change the port settings.

For example:

```
irccd -p <control_channel_port> -P <data_channel_port>
```

3. From the *%ProgramFiles%\Legato\nsr\res* directory, edit **mps.res**.

For example:

```
type: RM Service Ports;
```

```
Control Port: <control_channel_port>
```

```
Data Port: <data_channel_port>
```

For example:

```
type: RM Service Ports;
```

```
Control Port: 6728;
```

```
Data Port: 6729;
```

4. Start the **rmagentps** service.

For example:

```
net start rmagentps
```

Configuring NetWorker SharePoint services

During NMM installation, the NetWorker SharePoint Service Configuration dialog box appears. You can:

- ◆ Match the NetWorker SharePoint Service credentials with credentials of SharePoint Server administrator
- ◆ Specify the temporary storage location
- ◆ Specify the restore lock type

To view the NetWorker SharePoint Service Configuration dialog box after the installation is complete, type the following command at the command line:

```
C:\Program Files\Legato\nsr\bin\nwmoosinst.exe
```

Matching NetWorker SharePoint Service credentials with credentials of SharePoint Server administrator

The NetWorker SharePoint Service credentials specified in the NetWorker SharePoint Service Configuration dialog box must match the user and password credentials used for SharePoint Server administration. If proper credentials are not specified then backup of SharePoint data fails.

The NetWorker SharePoint Service Configuration dialog box provides fields to specify the Domain/User Name and Password for SharePoint Service credentials. If you do not fill in the fields to specify the same credentials as those of the SharePoint Server administrator, backup of SharePoint data fails with a Windows E_ACCESSDENIED error.

If you have already completed installation and want to test whether your credentials are correct, you can run the following commands at the command line on the SharePoint machine:

```
nsr_moss_save.exe -f
nsr_moss_save.exe -w
nsr_moss_save.exe -w <web application name>
nsr_moss_save.exe -u <site collection URL>
```

If no error messages appear, your credentials are probably specified correctly. But if you get error messages or failures with SharePoint backups, you can update the NetWorker SharePoint Service credentials.

To update or correct SharePoint credentials by using the NetWorker SharePoint Service Configuration dialog box:

1. In the **Domain\User Name** field, specify the domain and username you use for your Microsoft SharePoint Server administrator account.
2. In **Password** and **Confirm Password**, specify the password you use for your Microsoft SharePoint Server administrator account.
3. Click **OK** to save your changes.

Specifying temporary storage location

You can browse and select the temporary storage location in the NetWorker SharePoint Service Configuration dialog box. The temporary storage location is a temporary staging area and is reclaimed after recovery. This area is used to:

- ◆ Temporarily store the backup data going to the NetWorker Server during backup.
- ◆ Temporarily store the data coming from the NetWorker Server during restore. Sharepoint service picks the data from this area and updates the Sharepoint databases.

To specify the staging area for SharePoint granular backups by using the NetWorker SharePoint Service Configuration dialog box:

1. In **Temporary Storage Location**, specify the path for the staging area for SharePoint granular backups.

The **Temporary Storage Location** must be a valid drive. A new folder or an existing folder can be specified in that drive.

Note: Specifying a value in the Size of File field does not have any effect on the configuration process.

2. Click **OK** to save your changes.

The NetWorker SharePoint Service Configuration saves the staging location to the Windows Registry.

Specifying the restore lock type

You can specify the restore lock type in the NetWorker SharePoint Service Configuration dialog box. The options are:

- ◆ Read unlocked/Write unlocked
- ◆ Read unlocked/Write locked
- ◆ Read locked/Write unlocked
- ◆ Read locked/Write locked

After restore, depending on the option selected, the read/write locks are enabled for restored site collections. The option specified here is used as the default setting throughout. However, the option can be changed from the NMM GUI using the Recovery Options tab just before restore. The *EMC NetWorker Module for Microsoft Applications Release 2.2 Administration Guide* provides details about the Recovery Options tab.

Configuring Windows firewall settings

NMM automatically configures Windows firewall settings during installation. There is no need to run the Security Configuration Wizard to create firewall exceptions for the NMM client. The previous version of NMM, NetWorker VSS Client, required running the SCW, and then saving the SCW settings to the configuration file NetWorkerEXT.xml, which is no longer needed.

NMM settings can also be modified after installation:

1. Select **Start**, and then select **Control Panel > Add or Remove Programs**.
2. Select **NetWorker Module for Microsoft Applications**, and then click **Change**.

Windows firewall exception error for irccd.exe

Occasionally, the following error message is displayed during installation:

```
"Unable to create a Windows Firewall exception for C:\Program Files\EMC\rmagentps\client\bin\irccd.exe. File not found."
```

If this occurs, manually configure the firewall setting, and then validate the configuration.

To configure the firewall:

1. Select **Start**, and then select **Control Panel > Add or Remove Programs**.
2. Select **NetWorker Module for Microsoft Applications**, and then click **Change**.
3. In the **Welcome to NetWorker User Module for Microsoft Applications Maintenance** dialog box, click **Next**.
4. In the **Windows Firewall** window, select **Configure the Windows Firewall**.
5. Click **Next** until you finish the configuration wizard.
6. Click **Start**, and then click **Control Panel**.
7. Open **Windows Firewall**.
8. Click the **Exceptions** tab.
9. In the **Programs and Services** list, verify that **EMC Replication Manager Client for RMAgentPS** appears and is selected:
 - If the checkbox is not selected, select it.
 - If there is no entry for **EMC Replication Manager Client for RMAgentPS**, manually add it:
 - a. Click **Add Program**.
 - b. Click **Browse**.
 - c. Type **C:\Program Files\EMC\rmagentps\client\bin\irccd.exe**.
If NMM was installed on an another drive letter other than C:\, specify the correct path to irccd.exe as needed.
 - d. Click **OK**.

Manually creating NMM firewall exceptions

When NMM is installed on a NetWorker storage node, NMM firewall exceptions are not created. This option is not provided by the installer. When the NetWorker Client is used as a data mover, backups fail. If you are using Windows firewall and installing NMM 2.2 on an existing storage node, create and manually add the firewall exceptions listed in [Table 6 on page 65](#).

Table 6 Windows firewall exceptions

Display name	Program name
EMC NetWorker PowerSnap Service	nsrpsd.exe
EMC NetWorker PowerSnap Mover Agent	nsrsnapagent.exe
EMC NetWorker PowerSnap SnapCopy Agent	nsrbragent.exe
EMC NetWorker NSRSnapBwrAgent process	nsrsnapbwragent.exe
EMC NetWorker VSS Client Save Process	nsrsnap_vss_save.exe
EMC NetWorker VSS Client Recover Process	nsrsnap_vss_recover.exe
EMC NetWorker Client Configuration Server	nsrscsd.exe
EMC NetWorker User	winworkr.exe
EMC Replication Manager Client for RMAgentPS	irccd.exe

To manually add the exceptions:

1. Select **Start**, and then select **Control Panel** and **Add or Remove Programs**.
2. Select **NetWorker Module for Microsoft Applications**, and then click **Change**.
1. When the **Welcome to NetWorker User Module for Microsoft Applications Maintenance** dialog box appears, click **Next**.
2. In the **Windows Firewall** window:
 - For Windows Server 2008, click **Allow a program through Windows Firewall**.
 - For Windows Server 2003, click **Exceptions**.
3. For both Windows Server 2008 and Windows Server 2003, type the pathname of the program. All programs are located in C:\Program Files\Legato\nsr\bin, except for irccd.exe, which is located in C:\Program Files\Legato\nsr\rmagentps\client\bin.

For example, the pathname for:

 - **winworkr.exe** is C:\Program Files\Legato\nsr\bin\winworkr.exe.
 - **irccd.exe** is C:\Program Files\Legato\nsr\rmagentps\client\bin\irccd.exe.
4. Click **Add Program**.

A

add-on enablers 38
authorization code 41

B

base enablers 38
BCVs 51

C

CLARiiON array configuration 48
CLARiiON configuration file 48
copy protection violation error 39
create device group 51

D

device group 51
duplicate enablers 39

E

enabler certificate 40
establishing mirrors 51
evaluating NetWorker software 39
Exchange server 60

H

-help option 51

I

install_nmm_silent_sample.cmd 33

L

License Manager software 42
licensing process 42

M

Microsoft System Center Configuration Manager 2007
server 34

N

new authorization code 42
NMC 47
NMM Firewall exceptions 65
nwexinfo.exe utility 60

P

PowerSnap NetWorker security 47
production host 47
proxy host 47
purchased edition 39

R

registration period 40
Replication Manager port settings 61
rmagentps service 61

S

sample commands 32
sample configuration file 48
stand-alone method 30
SYMCLI 51

T

temporary enabler 39

U

uninstall_nmm_silent_sample.cmd 35
utility 60

W

Windows E_ACCESSDENIED error 62

