

Dell EMC NetWorker Module for Microsoft

Version 19.2

Administration Guide

REV 01

November 2019

Copyright © 2007-2019 Dell Inc. or its subsidiaries. All rights reserved.

Dell 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.” DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Figures	7
Tables	9
Preface	11
Chapter 1	Overview of Product Features 15
	Overview of NetWorker Module for Microsoft 16
	Volume Shadow Copy Service technology..... 16
	Resilient Change Tracking technology..... 16
	Block based backup technology..... 17
	Virtual Device Interface technology..... 19
	NMM architecture..... 19
	Changes in underlying architecture in NMM 9.0 and later..... 20
	Supported backup and recovery types..... 21
	NetWorker backup levels and corresponding NMM backup levels..... 22
	NMM binaries..... 23
	Using NMM 9.0.x to recover NMM 8.2.x VSS backups..... 25
	Granular level recovery..... 26
	Performing a granular level recovery for data backed up on a tape device..... 27
	Directed recovery..... 27
	NMM backup and recovery requirements..... 28
	Access privileges for backup and recovery..... 28
	Adding Microsoft Windows groups and NetWorker administrative privileges..... 29
	Setting AES data encryption..... 30
	Synchronizing NMM client and NetWorker server clocks..... 31
	Identifying and back-translating computer names through name resolution..... 31
	NMM Support Tools for recovery..... 32
Chapter 2	NMM Client Graphical User Interfaces 35
	Overview of NMM graphical user interfaces..... 36
	NetWorker User for Microsoft user interface..... 36
	User interface views..... 36
	Display conventions..... 38
	Connecting to a NetWorker server..... 38
	Specifying recovery browse times in the NetWorker User for Microsoft GUI 39
	Searching for items..... 39
	Selecting items for recovery..... 40
	Marked objects..... 40
	Viewing required volumes for recovery..... 41
	Selecting backup versions for recovery..... 41

Chapter 3	NetWorker Client Management	43
	Configuring Microsoft application server.....	44
	Configuring NetWorker privileges manually.....	46
Chapter 4	Restricted Data Zone	47
	NMM support for NetWorker Restricted Datazone.....	48
	Recommendations.....	49
	Providing required privileges for RDZ support in NMM.....	49
Chapter 5	VSS-Based Scheduled Backups	51
	Configuring a client resource.....	52
	Considerations when using the Client Backup Configuration wizard for NetWorker server 8.2.3 or later and NMM 19.2.....	52
	Creating a client resource by using the Client Backup Configuration wizard.....	53
	Manually creating a client resource by using the Client Properties dialog box...	53
	Editing a client resource that is created with NMM 9.0 or later.....	54
	Editing a client resource that was created with NMM 8.2.x after you upgraded to NMM 9.0 and later.....	55
	Editing existing client resources through the NMC bulk edit feature...	55
	Considerations and recommendations for application backups.....	55
Chapter 6	Data Deduplication with Data Domain	59
	Overview of deduplication support with Data Domain.....	60
	Client Direct data deduplication backup and recovery.....	60
	Backup support.....	61
	Recovery support.....	61
	Data Domain and NetWorker server configuration.....	61
	Data Domain Boost data deduplication capabilities.....	62
	Enabling Client Direct backups over Fibre Channel.....	62
	Configuring data deduplication for Data Domain clients.....	62
	Recovering deduplicated data.....	64
Chapter 7	Multihomed Setup for Backups and Recoveries	65
	Overview of a multihomed environment.....	66
	Sample network topology of multihomed environment for backup.....	66
	Requirements for a multihomed environment.....	67
	NIC and IP requirements.....	67
	Network configuration requirements for the NMM client.....	68
	Network configuration requirements for NetWorker server.....	69
	Network configuration requirements for NetWorker storage node.....	69
	Configuring a multihomed client resource.....	70
	Validating configuration of a multihomed environment.....	72
Chapter 8	Active Directory Backups and Recoveries	73
	Supported and unsupported Active Directory backup and recovery types and configurations.....	74
	Supported Active Directory objects for granular backup and recovery.....	74
	Improvement in NMM GUI browsing performance of Active Directory backups with large number of objects.....	74
	Performing Active Directory granular backups.....	76
	Recommendations for Active Directory granular backups.....	76
	Configuring a pool for backup operations.....	76

	Configuring a client resource.....	77
	Performing an Active Directory granular recovery.....	78
	Recovery restrictions for Active Directory.....	78
	Recovering an Active Directory object or object attribute.....	79
	Recovering Active Directory backups created with NMM 8.2.x	80
Chapter 9	Cloning Backups and Recoveries	83
	Overview.....	84
	Cloning with NMM.....	84
	Concurrent cloning.....	85
	Recovering cloned data with NMM.....	86
	Identifying the required save time range.....	86
	Recovering NMM data from recoverable or recycling save sets.....	86
	Generating the media database list of the save sets.....	87
	Recovering recoverable save sets to the client file index.....	87
	Recovering recyclable save sets to the client file index.....	89
	Save set media database.....	90
	Performing recovery.....	92
	Restriction on cloning BBB incremental backups that reside on AFTD or CloudBoost.....	93
Chapter 10	Windows Bare Metal Recovery Solution	95
	Overview.....	96
	System requirements.....	96
	Microsoft BMR requirements.....	96
	CPU requirements.....	96
	Hard disk requirements.....	96
	NIC driver requirements.....	97
	Critical and noncritical volume requirements.....	97
	System Reserved Partition requirements.....	97
	Supported operating systems.....	98
	Supported Microsoft applications.....	98
	NetWorker software version requirements.....	98
	Protecting an environment before a disaster.....	98
	BMR by using NetWorker and NMM.....	99
	Backing up an Active Directory for BMR.....	99
	Performing BMR of an Active Directory.....	100
Chapter 11	Troubleshooting	101
	NMM Configuration checker.....	102
	The EMCReports tool.....	102
	NMM client error messages.....	102
	General NMM client error messages.....	102
	Microsoft Exchange client error messages.....	103
	Microsoft SharePoint Server client error messages.....	106
	Microsoft SQL Server client error messages.....	107
	Checking log files.....	108
	NMM client log files.....	108
	Active Directory log files.....	109
	NetWorker server log files.....	109
	GLR mount service log file.....	109
	Other troubleshooting resources.....	109

Glossary

111

FIGURES

1	Architecture in NMM 8.2.x and earlier	19
2	Architecture in NMM 9.0 and later.....	20
3	Save sets that are written to the tape.....	27
4	Encryption directive for SQL VSS client resource configuration.....	31
5	Recover view of the NetWorker User for Microsoft GUI main page	37
6	Monitor view of the NetWorker User for Microsoft GUI main page.....	37
7	Selected and partially selected items.....	40
8	Configure Options dialog box.....	44
9	Client Direct data deduplication environment.....	61
10	Apps & Modules tab with the deduplication attribute.....	63
11	Sample network topology of NetWorker multihomed backup.....	67
12	Advanced Settings dialog box.....	69
13	Globals (1 of 2) tab for multihomed client resource configuration.....	71
14	Globals (2 of 2) tab for multihomed client resource configuration.....	71
15	Browse tab.....	75
16	Search tab with Enable direct search option.....	75
17	Enable concurrent cloning in the Policy Action Wizard.....	86


TABLES

1	Revision history.....	12
2	Style conventions.....	12
3	Types of supported backups.....	21
4	Types of supported recoveries.....	21
5	Support for backup and recovery	22
6	NetWorker backup levels and corresponding NMM backup levels.....	22
7	NMM binaries and their description.....	23
8	GLR of Microsoft application backups.....	26
9	Pull-and push-directed recovery support	27
10	Access privileges for backup and recovery.....	29
11	Icons used in the NetWorker User for Microsoft GUI.....	38
12	User group privileges for NMM operations.....	46
13	Privileges options for RDZ.....	49
14	Best practices for application backups.....	55
15	Configuration details for Data Domain and NetWorker	62
16	System-only attributes that are not backed up	78
17	Attributes retained after object is deleted.....	79
18	Parent and the child save sets.....	85

Preface


As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

 **Note:** This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website <https://www.dell.com/support>.

Purpose

This guide contains information about using the NetWorker Module for Microsoft (NMM) 19.2 software and is intended for use by system administrators during the setup and maintenance of the product.

 **Note:** The **NetWorker Administration Guide** supplements the backup and recovery procedures described in this guide. Download a copy of the **NetWorker Administration Guide** from the Support website at (<https://support.emc.com>) before using this guide.

Audience

This guide is part of the NMM documentation set and is intended for use by system administrators during the setup and maintenance of the product. Readers should be familiar with the following technologies used in backup and recovery operations:

- NetWorker software
- Microsoft Volume Shadow Copy Service (VSS) technology
- Microsoft Virtual Device Interface (VDI) technology (if using NMM to backup and recover SQL Server VDI)

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	November, 2019	First release of this document for the NetWorker Module for Microsoft 19.2 release.

Related documentation

The NMM documentation set includes the following publications:

- *NetWorker Module for Microsoft Release Notes*
- *NetWorker Module for Microsoft Administration Guide*
- *NetWorker Module for Microsoft Installation Guide*
- *NetWorker Module for Microsoft for SQL and SharePoint VSS User Guide*
- *NetWorker Module for Microsoft for SQL VDI User Guide*
- *NetWorker Module for Microsoft for Exchange VSS User Guide*
- *NetWorker Module for Microsoft for Hyper-V User Guide*
- *ItemPoint for Microsoft SQL Server User Guide*
- *ItemPoint for Microsoft Exchange Server User Guide*
- *ItemPoint for Microsoft SharePoint Server User Guide*
- NetWorker documentation set

Special notice conventions that are used in this document

The following conventions are used for special notices:

ⓘ **NOTICE** Identifies content that warns of potential business or data loss.

ⓘ **Note:** Contains information that is incidental, but not essential, to the topic.

Typographical conventions

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options

Table 2 Style conventions (continued)

<i>Monospace italic</i>	Used for variables.
Monospace bold	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- <https://www.dell.com/support>
- <https://community.emc.com>

Where to get support

The Support website <https://www.dell.com/support> provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to <https://www.dell.com/support>.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:


1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to <https://www.dell.com/support>.

2. On the **Support** tab, click **Service Requests**.

 **Note:** To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To find the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network <https://community.emc.com>. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Overview of Product Features

This chapter includes the following sections:

• Overview of NetWorker Module for Microsoft	16
• NMM architecture	19
• Supported backup and recovery types	21
• NMM binaries	23
• Using NMM 9.0.x to recover NMM 8.2.x VSS backups	25
• Granular level recovery	26
• Directed recovery	27
• NMM backup and recovery requirements	28
• NMM Support Tools for recovery	32

Overview of NetWorker Module for Microsoft

The NetWorker Module for Microsoft (NMM) software uses the following technologies to provide backup and recovery for Microsoft applications:

- Microsoft Volume Shadow Copy Service (VSS) technology: NMM uses this Microsoft technology to provide snapshot backup and recovery support for Microsoft applications. The NMM client creates point-in-time snapshot data, which can then be recovered from the backup media. You can perform backup and recovery operations of the following applications:
 - SQL Server
 - Exchange Server
 - SharePoint Server
 - Hyper-V Server
- Resilient Change Tracking (RCT) technology: NMM uses this Microsoft technology to back up and recover the Hyper-V Server 2016 data.
- Block Based Backup (BBB) technology: NMM uses this technology to back up and recover the Exchange Server data and the Hyper-V Server data.
- Virtual Device Interface (VDI) technology: NMM uses this Microsoft technology to communicate with the SQL Server to back up and recover the SQL Server data. The *NetWorker Module for Microsoft for SQL VDI User Guide* provides specific backup and recovery information for a SQL Server using VDI technology.

Note: Any references to the Data Domain systems and the Data Domain devices in the product also apply to the PowerProtect Data Domain systems.

Volume Shadow Copy Service technology

The Volume Shadow Copy Service (VSS) coordinates the activities among the three components that create, modify, back up, and recover data.

- Requester—The application that requests that a shadow copy is created. Typically, the requester is a backup application, such as NMM.
- Writer—The writer is an application-specific software that ensures that the application data is ready for shadow copy creation. Writers provide information about the data to back up and specific methods for handling components and applications during backup and recovery. Writers also identify the type of application or service that is being backed up. If a service or application is present on a system but is inactive, information from its writer is unavailable.
- Provider—The provider captures snapshots. The Microsoft Software Shadow Copy provider is a host-based provider that works with any type of storage hardware and is included in all Windows versions.

The Microsoft TechNet website provides information about the VSS process.

Note: NMM VSS only supports Windows disk manager. Other volume manager software, such as Veritas, is not supported.

Resilient Change Tracking technology

Windows Server 2016 has built-in system of Resilient Change Tracking (RCT). This RCT feature of Hyper-V 2016 enables easier and faster incremental backups. With this feature, backup vendors do not need to create and support their own file system filter drivers, which you need for the previous Hyper-V versions that do not have any native Change Block Tracking (CBT).

The Change Block Tracking (CBT) feature stores the blocks that are tracked in a memory bitmap on the host. In the case of virtual machine migration or power outage, if anything happens to the

memory, the whole bitmap is lost. You cannot identify the changed blocks, and must spend time and resources to perform a full rescan. The RCT feature solves this problem. It creates three bitmaps: one in memory and two on disk.

In RCT, the bitmap that is present in the memory functions in the same way as in CBT. It is the most granular of the three bitmaps. As long as the virtual machine runs, the backup operation looks at this bitmap, and copies the changed blocks only when an incremental backup is requested.

When you migrate the virtual machine, or there is a sudden power outage, the backup operation looks for the following bitmaps on the disk:

- **Modified Region Table (MRT) file:** Use this file when you migrate the virtual machine and lose the bitmap that is present in the memory. The extension of this file is `.mrt`.
- **RCT file:** Use this file when there is a sudden power outage or a similar event. The extension of this file is `.rct`.

NMM supports image-level full and incremental RCT backups of Hyper-V 2016 standalone and federated virtual machines to the AFTD, Data Domain, or CloudBoost storage device that you configure.

To configure RCT backups:

- Consider the following notes:
 - RCT backups do not include VSS writers because they do not use VSS framework.
 - Create and maintain separate policies and groups for RCT and VSS backups. Configure and schedule either RCT backups or VSS backups at a time. Do not mix RCT backups with VSS backups.
 - RCT backups of the virtual machines that contain any user checkpoints or recovery checkpoints fail. Before you back up such virtual machines, merge the checkpoints by running the following PowerShell command:
`Get-VM -name VMname | Get-VMSnapshot | Remove-VMSnapshot`
 RCT backups of the virtual machines that do not contain any checkpoints proceed.
 - When you switch from the VSS-based backup to the RCT-based backup, merge all the checkpoints of the virtual machines for the RCT backups to succeed.
 - You can back up together the virtual machines that are configured on CSV and SMB.
 - You cannot back up the virtual machines with a configuration version earlier than 6.2.
 - You cannot back up the virtual machines that are present on the local storage node, and added to a cluster.
 - You cannot back up the virtual machines that contain shared disks.
- Use one of the following applications:
- **Client Backup Configuration** wizard of NMC
- **Client Properties** dialog box of the NetWorker Administration program

Block based backup technology

This section provides an overview of the Block based backup (BBB) method, which is the only backup option for Exchange Server and Hyper-V Server in NMM 9.0 and later.

The Block Based Backup and Recovery chapter in the *NetWorker Administration Guide* provides information about BBB. The *NetWorker Module for Microsoft for Exchange VSS User Guide* and the *NetWorker Module for Microsoft for Hyper-V User Guide* provide details about how to perform BBB for Exchange Server and Hyper-V Server respectively.

During BBB, the backup client analyzes the volume and backs up only the changed or new blocks for a file since the previous backup. Using BBB instead of file-based backup can reduce backup

storage requirements and minimize the recovery point objective (RPO) when backing up and restoring files.

BBB provides the following advantages over file-based backup:

- For BBB volume backups, BBB does not require a backup of all the files in the volume. BBB copies the used blocks in the volume for level full or incremental backups. Performing a file-by-file search and copy can be time consuming.
- During backup, BBB copies only those blocks that have changed since the last backup, while file-based backup copies complete files that have changed within a file. By copying only the changed blocks, BBB backups complete faster than file-based backups.
- BBB provides backup in native VHDx or VHD format based on operating system support. VHDx or VHD backup format has advantages such as instant backup access, fast search, incremental forever, synthetic full, and granular level recovery.

When using BBB for Exchange, consider the following:

- BBB is the only supported backup technology for NMM 9.0 and later.
- Select BBB when you configure a client resource, and select a Data Domain device or an Advanced File Type Device (AFTD) as the target device, otherwise the backup fails. Direct File Access (DFA) must be enabled for the target devices.
- Cloning for incremental backup is not supported on AFTD.
- When you use Data Domain, the resulting backup on the target device is a full backup because NMM uses Data Domain virtual synthetics technology to create a synthetic full backup.
- If the database moves to another node, an Exchange Server incremental backup is promoted to BBB full.
- The backup is always VSS full backup regardless of the backup level that the protection policy passed.

When using BBB with NMM Hyper-V, consider the following:

- BBB is the only supported backup technology for NMM 9.0 and later.
- BBB for Hyper-V does not use the BBB Change Block Tracking, but uses the Microsoft Native Change Block Tracking for incremental backups.
- Select BBB when you configure a client resource, and select a Data Domain device or an Advanced File Type Device (AFTD) as the target device, otherwise the backup fails. Direct File Access (DFA) must be enabled for the target devices.
- Cloning for incremental backup is not supported on AFTD.
- When you use Data Domain, the resulting backup on target device is a full backup because NMM uses Data Domain virtual synthetics technology to create a synthetic full backup.
- The VSS backup level follows the NetWorker backup level.

BBB does not support the following:

- Encrypted, compressed, or deduplicated files.
- Persistent snapshots and hardware providers.
- Recovery of backups created by using NMM 8.2.x or earlier releases.
- Junction points.
- Local AFTD or file type device (without share type). The device must be in the UNC path, for example `\\Hostname\Device_Name\`.

Virtual Device Interface technology

Virtual Device Interface (VDI) technology is used to back up and recover Microsoft SQL data. The *NetWorker Module for Microsoft for SQL VDI User Guide* provides details.

NMM architecture

In 9.0 and later releases, NMM uses the VSS Common Requester for all VSS framework-related operations and all workflows. Data roll-over is performed using the NetWorker Save for SQL Server (VSS) and SharePoint VSS, and the BBB framework for Hyper-V and Exchange Server.

NMM 9.0 and later architecture provides the following benefits:

- Improved backup and recovery performances
- Reduced complexity in configuring backups
- Removed complex and time-consuming maintenance of different layers
- Removed restrictions on workflows for addition of new features
- Simplified backup and recovery logs

All NMM 8.2.x and earlier features are supported by the simplified NMM 9.0 and later architecture and there are minimal changes to the graphical user interfaces.

The following diagrams show the architectural differences between NMM releases earlier than 9.0 and NMM 9.0 and later.

Figure 1 Architecture in NMM 8.2.x and earlier

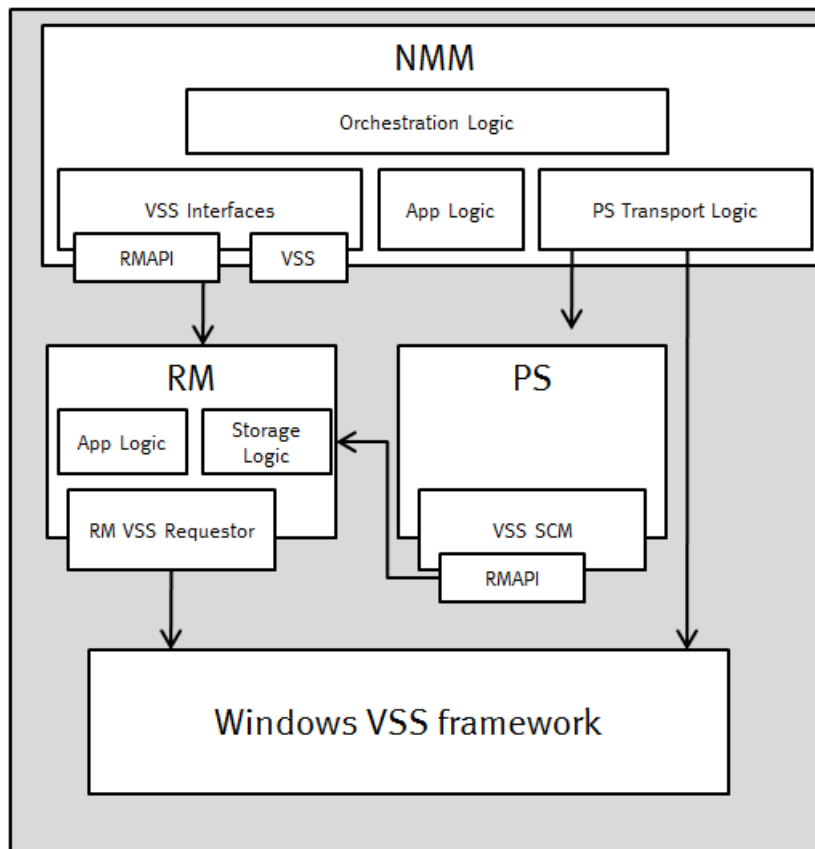
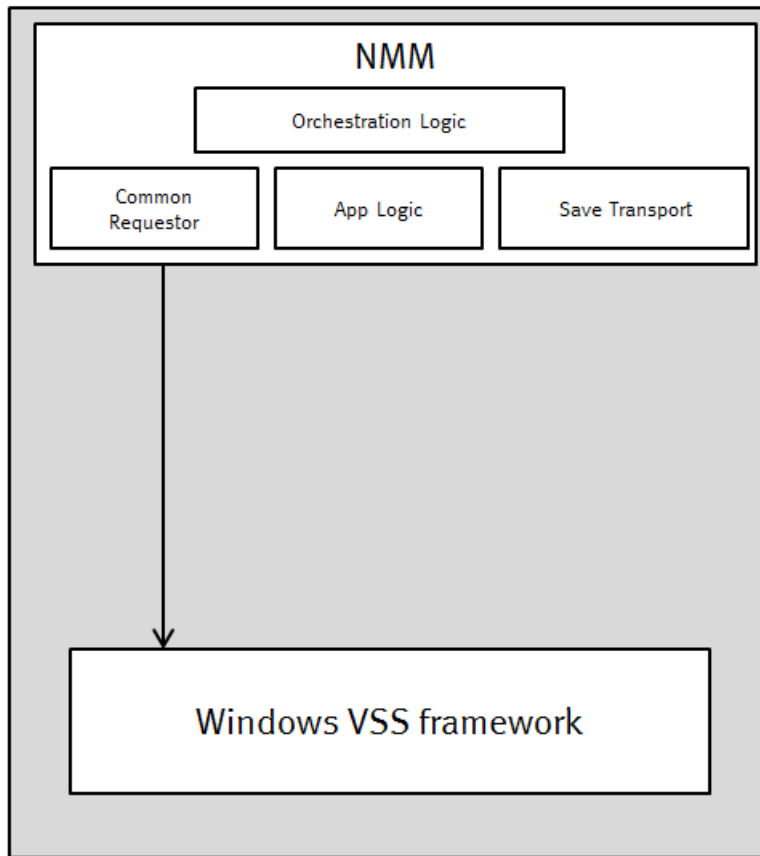


Figure 2 Architecture in NMM 9.0 and later




Changes in underlying architecture in NMM 9.0 and later

The changes in the underlying architecture in NMM 9.0 and later are as follows:

- Persistent snapshots are no longer supported.
- The logging model is reduced to a single log file for save operations and a single log file for recover operations.
- The backup command is `nsrnmmsv` and the recovery command is `nsrnmrc`. The `nsrsnap_vss_save` and `nsrsnap_vss_recover` commands are no longer used.
- The installation and implementation process is simpler because NMM backup and recovery operations require fewer software components. The *NetWorker Module for Microsoft Installation Guide* provides details.
- The snapshot policy that NMM 8.2.x and earlier releases used is replaced by data protection policy. The *NetWorker Administration Guide* provides details about the data protection policy.
- NMM 8.2.x and earlier backups and NetWorker backups shared a common namespace, which posed technical challenges during browsing and restoring the backup. A separate backup namespace is now available for NMM backups.

Supported backup and recovery types

NMM can back up data automatically or manually, as required. The backed-up data can be recovered as specific items or an entire volume. You can also fully recover a disabled computer.

 **Note:** NMM does not support backup and recovery of Windows Server 2012 and later deduplication volumes.

The following table lists the types of supported backups by NMM.

Table 3 Types of supported backups

Types	Description
Scheduled backup	Scheduled backups are available for all Microsoft applications. The NetWorker server backs up client data regularly through scheduled backups. You can schedule a backup to start at any time.
Manual backup	Manual, or ad-hoc, backups are available for Microsoft SQL Server when using the VDI technology. You can start a manual backup at any time from the command line or GUI. Manual backups from the NetWorker User for Microsoft SQL Server GUI are always full backups. Manual backups from the command line or the NMM Microsoft SQL Server Management Studio plugin can be any level.
Federated backup	Federated backup is an internal backup architecture that is available for SharePoint Server, Hyper-V Server, Exchange Server, and SQL Server (VDI). Refer to the list of application-specific guides in the <i>Related documentation</i> section of the Preface for details.
Granular backup	Granular backups are available for Active Directory. A granular backup does not use snapshot technology (non-VSS). Instead, the backup is routed directly to a granular backup medium. A traditional granular Active Directory backup enables you to recover individual objects and object attributes.

The following table lists the types of supported recoveries by NMM.

Table 4 Types of supported recoveries

Types	Description
Conventional recovery	The entire volume, database, or virtual machine is recovered as a whole.
Granular level recovery	Granular level recovery (GLR) lets you recover specific items, such as files and folders. The "Granular level recovery" section provides more details.
Flat file recovery	The "NMM Support Tools for recovery" section provides details.
Bare metal recovery	The "Windows Bare Metal Recovery" chapter provides details.

 **Note:** For all types of Exchange and Hyper-V Server backups and recoveries:

- The backup device must be AFTD or Data Domain, and must have client direct access. You can then clone to other backup devices, such as tape or CloudBoost, or even AFTD and Data Domain that have no direct client access.

- The recovery must be from AFTD, Data Domain, or CloudBoost and the client must have a direct access. If the device, for example tape device is ineligible, you can clone to AFTD, Data Domain, or CloudBoost and ensure that client-direct access is possible before performing recovery.

For SharePoint Server and SQL Server VSS granular level recovery, the recovery must be performed from AFTD, Data Domain, or CloudBoost device and the client must have a direct access.

The following table lists the types of backups and restores that NMM supports for different Microsoft applications.

Table 5 Support for backup and recovery

Backup and recovery types	Active Directory	SQL Server (VSS)	Exchange Server (VSS)	SharePoint Server (VSS)	Hyper-V (VSS)	SQL Server (VDI)
Scheduled backup	Yes	Yes	Yes	Yes	Yes	Yes
Manual backup	NA	NA	NA	NA	NA	Yes
Federated backup	NA	NA	Yes	Yes	Yes	Yes
Conventional recovery	NA	Yes	Yes	Yes	Yes	Yes
Granular level recovery	Yes	NA	Yes	Yes	Yes	Yes
Flat file recovery	NA	Yes	Yes	Yes	Yes	Yes
Bare metal recovery	NA	Yes	Yes	Yes	Yes	Yes

NetWorker backup levels and corresponding NMM backup levels

The following table lists the NetWorker backup levels and corresponding NMM backup levels.

Note: The "Supported NetWorker server and client versions" section in the *NetWorker Module for Microsoft Installation Guide* provides the NMM support matrix for NetWorker server and client versions. For more specific details, see the individual NMM release sections of the *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/eln/elhome>.

Table 6 NetWorker backup levels and corresponding NMM backup levels

Microsoft applications	NetWorker backup level	Corresponding NMM backup level
All Microsoft applications	Full	Full
Hyper-V and Exchange Server	Incremental	Performs incremental but the resulting save set is synthesized and full

Table 6 NetWorker backup levels and corresponding NMM backup levels (continued)

Microsoft applications	NetWorker backup level	Corresponding NMM backup level
SQL Server (VDI)	<ul style="list-style-type: none"> Logs only for NetWorker 9.2 and later Incremental for NetWorker 8.2.3 and later 	Logs only <i>i</i> Note: In addition to full and logs-only backups, you can perform cumulative, incremental backups for SQL VDI. The <i>NetWorker Module for Microsoft for SQL VDI User Guide</i> provides detailed information about the types of backup and recovery supported for SQL VDI.
SQL Server (VSS) and SharePoint Server (VSS)	Incremental	Full

i **Note:** NetWorker backup level, synthetic full, is not supported in NMM.

NMM binaries

The following table lists the NMM binaries and their description.

Table 7 NMM binaries and their description

Binary name	Description
nsradsave.exe	This binary is used to perform Active Directory backups.
nsradrecov.exe	This binary is used to recover Active Directory objects.
nsrnmmv.exe	This is a common binary used to perform VSS based backups for Exchange Server, SharePoint Server, SQL Server, and Hyper-V Server. The save set name passed to the binary determines the type of application being backed up. <i>i</i> Note: This binary cannot be used for adhoc backups from the client side based Command Line Interface (CLI) backup.
nsrnmmrc.exe	This is a common binary used for flat-file VSS restores of Exchange Server, SharePoint Server, SQL Server, and Hyper-V Server. The restore objects and the recover options passed to the binary determines the type of application being recovered. This binary is used only through the NMM client GUI and cannot be used for client side based Command Line Interface (CLI) VSS recovery.
nsrnmmhypervra.exe	This binary is used to get save set information for a Hyper-V Server. This binary is used during NMM Hyper-V client configuration using the Client Backup Configuration wizard and provides information on all virtual machines on a Hyper-V host or cluster.

Table 7 NMM binaries and their description (continued)

Binary name	Description
	The save set list is displayed in Client Backup Configuration wizard > Save set field.
nsrnmra.exe	This binary is primarily used for the Hyper-V file-level recovery (FLR) GUI. It runs on Windows as a Windows service and is used when the FLR GUI requests for browsing of Hyper-V virtual machines or mounting and unmounting of Hyper-V virtual machines from a selected backup. This binary mounts the VHDs on the required server and provides information on the VHDs and data.
nsrscsd.exe	This binary is started on demand on the NMM client as a remote host when remote host environment information is needed, and is used by backup and recovery programs.
nsrnm_glr_recover.exe	This binary is used for Hyper-V granular-level recovery when started from the WinClient. This binary copies selected files from mounted VHD to the destination path.
nsrnmexchra.exe	<p>This binary is used to get save set information for a Exchange Server. This binary is used during NMM Exchange client configuration using the Client Backup Configuration wizard and provides information on the databases on the Exchange Server or DAG.</p> <p>The save set list is displayed in Client Backup Configuration wizard > Save set field.</p>
nsrnmmspra.exe	<p>This binary is used to get save set information for a SharePoint Server farm. This binary is used during SharePoint Server client configuration using the Client Backup Configuration wizard and provides information on all SharePoint farm components.</p> <p>The save set list is displayed in Client Backup Configuration wizard > Save set field.</p>
nsrnmsqlra.exe	<p>This binary is used to get save set information for a SQL Server. This binary is used during NMM SQL Server client configuration using the Client Backup Configuration wizard and provides information on all available SQL instance and database information.</p> <p>The save set list is displayed in Client Backup Configuration wizard > Save set field.</p>
nsrxchmbrc.exe	This binary is used by native Exchange GLR solutions for NMM Exchange Server granular recovery of mailboxes.
nsrsqlsv.exe	This binary is used for SQL Server backup using VDI technology, and is independent of the NMM backup save binary for VSS based backup. This binary can be used for adhoc backup of SQL Server using CLI.

Table 7 NMM binaries and their description (continued)

Binary name	Description
nsrsqlrc.exe	This binary is used for SQL Server backup using VDI technology, and is independent of the NMM backup save binary for VSS based backup. This binary can be used to perform SQL data restore using CLI.
nwmssql.exe	<p>This binary is used by the NetWorker User for SQL Server GUI for client initiated backups and recovery using VDI technology.</p> <p>Note: You are recommended to use the SQL Server Management Studio Plugin GUI for all SQL VDI related tasks because the NetWorker User for SQL Server GUI is deprecated. The <i>NetWorker Module for Microsoft for SQL Server VDI User Guide</i> provides information about the SQL Server Management Studio Plugin GUI.</p>
userConfigUI.exe	This binary is used by the NMM Exchange Admin Configuration tool to configure user account with required permissions for NMM to manage backup and recovery in Exchange environments. It is mandatory that you use this tool to configure a user account prior to performing Exchange backup and recovery with NMM.
winclient.exe	This binary is used by the NetWorker User for Microsoft recover GUI. This GUI is common to all VSS based backups for Exchange Server, SharePoint Server, SQL Server, and Hyper-V Server. The GUI distinguishes the applications based on the plugins being loaded with the GUI and the application running on the host.

Using NMM 9.0.x to recover NMM 8.2.x VSS backups

You can use NMM 9.0.x to recover VSS backups that are created with a NMM 8.2.x release for Exchange Server, SQL Server, SharePoint Server, and Hyper-V.

Note: The information in this section is not required for users who use NMM 8.2.x release for SQL Server VDI or Active Directory backup and recovery and who upgrade to NMM 9.0 or later.

- Select the **Restore of NMM 8.2.x and Earlier Backups (VSS workflows)** option in the installer to install the required recovery GUI on your system. The *NetWorker Module for Microsoft Installation Guide* provides information about this option.
- Use the **Restore previous NMM release backups** shortcut on the **Start** menu to recover backups that were created with NMM 8.2.x releases. The application-specific user guides provide information about this feature.
- Edit the client resources that were created with the NMM 8.2.x release before performing the recovery. The "Scheduled Backup" chapter provides information about editing a client resource and the bulk edit feature.
- Ensure that the Snapshot attribute of the NetWorker group that a client resource belongs to is clear, or create a new group that does not have the snapshot option selected.

Note: NMM 9.0 and later do not support:

- Exchange Server node-level backups. Node-level backups that are configured with NMM 8.2.x or earlier releases fail after you upgrade NMM to NMM 9.0 or later. The error message is documented in the log file.
- Snapshot backups that are configured with NMM 8.2.x or earlier releases.
- Avamar client for deduplication.

Granular level recovery

You can perform granular level recovery (GLR) of Exchange Server, Hyper-V Server, SQL Server, and SharePoint Server backups that are created with NMM. GLR enables you to recover specific items, such as files and folders, from a single full backup without having to recover the full backup. This feature reduces the space requirements on local system storage and might reduce recovery time depending on the size of data and target storage.

The following table provides the descriptions for GLR of SharePoint Server, Hyper-V Server, Exchange Server, and SQL Server VSS.

Table 8 GLR of Microsoft application backups

Microsoft application	Description
GLR for SharePoint	To perform GLR for SharePoint, use the Granular level recovery tab in the NetWorker User for Microsoft GUI and the ItemPoint™ for SharePoint software. The GLR plug-in uses NetWorker Virtual File System (NWFS). This plug-in exposes files from a list of save sets within a single full backup as a virtual file system on an NMM client. The <i>NetWorker Module for Microsoft for SQL and SharePoint VSS User Guide</i> provides specific details for SharePoint GLR.
GLR for Hyper-V	To perform GLR for Hyper-V Server, use the GLR option in the NetWorker User for Microsoft GUI. The GLR operation for Hyper-V is performed using a Block Based Backup mount. The "Block Based Backup and Recovery" chapter in the <i>NetWorker Administration Guide</i> provides information about BBB, and the <i>NetWorker Module for Microsoft for Hyper-V User Guide</i> provides specific details for Hyper-V GLR.
GLR for Exchange Server	To perform GLR for Exchange, use the Granular level recovery tab in the NetWorker User for Microsoft GUI and the ItemPoint for Exchange software. The GLR operation for Exchange is performed using a Block Based Backup mount. The "Block Based Backup and Recovery" chapter in the <i>NetWorker Administration Guide</i> provides information about BBB, and the <i>NetWorker Module for Microsoft for Exchange VSS User Guide</i> provides specific details for Exchange GLR.
GLR for SQL Server	To perform GLR for SQL Server, use the Table Restore tab in the NMM SQL Studio Management plugin GUI and the ItemPoint for SQL Server software. The <i>NetWorker Module for Microsoft for SQL VDI User Guide</i> provides information about SQL GLR.

Note: To perform GLR of Exchange Server, Hyper-V Server, SQL Server, or SharePoint Server, the device from which recovery is performed must be AFTD, Data Domain, or a CloudBoost device with direct client access. Because recoveries from a device like tape cannot be performed, you must first clone the backup to AFTD, Data Domain or CloudBoost and ensure that client-direct access is possible, and then perform recovery.

Performing a granular level recovery for data backed up on a tape device

Perform the following steps for GLR of data that is backed up on a tape device:

Procedure

1. Identify the save sets that are cloned to the tape device by running the `mminfo` command. The output consists of separate lists of the save sets that are cloned to a tape device, AFTD, or DD device.
 - When using DD, you must identify the BBB full backup (each backup is a BBB full).
 - When using AFTD, you must identify the series of BBB incremental and base BBB full backups.
 - When using a tape device, you must identify the save sets that are written to the tape.

For example, the following figure displays the save sets that are written to the tape.

Figure 3 Save sets that are written to the tape

volume	type	client	date	time	size	ssid	fl	lvl name
000191L3	LTO Ultrium-4	dag01.benettongroupqas.org	12/08/11	12:40:01	139 MB	1776329237	cE	full APPLICATIONS:\Microsoft Exchange 2010
000191L3	LTO Ultrium-4	dag01.benettongroupqas.org	12/08/11	12:40:05	6157 KB	1759552024	cE	full APPLICATIONS:\Microsoft Exchange 2010
000191L3	LTO Ultrium-4	dag01.benettongroupqas.org	12/08/11	12:40:06	967 MB	1742774809	cE	full APPLICATIONS:\Microsoft Exchange 2010
000191L3	LTO Ultrium-4	dag01.benettongroupqas.org	12/08/11	12:40:07	251 MB	1725997593	cE	full APPLICATIONS:\Microsoft Exchange 2010

2. Run the `nsrclone` command to clone the save sets on the tape device to an AFTD or DD device. Ensure that these save sets are placed in the same group policy as the original backup.

The *NetWorker Administration Guide* provides information on the `nsrclone` command.

3. Perform GLR of the cloned save sets on the AFTD or DD device.

Directed recovery

The *NetWorker Administration Guide* provides details about directed recovery and requirements.

There are two types of directed recovery:

- Pull-directed recovery—The control role and destination role are run on the same computer. The control role that runs on the destination computer pulls the recovery data to itself. Backup data from the source client is restored to the destination client.
- Push-directed recovery—The control role can run on the source client or on a different client. The control client computer pushes the backup data to the destination client, which resides on a different computer from either the source client or the control client.

The following table lists the pull-and push-directed recovery support that NMM provides.

Table 9 Pull-and push-directed recovery support

Application	Pull-directed recovery	Push-directed recovery
Exchange Server	Yes	Yes

Table 9 Pull-and push-directed recovery support (continued)

Application	Pull-directed recovery	Push-directed recovery
	Only for DAG-based recovery	
Hyper-V	No	No
SharePoint Server	Yes	No
SQL Server VSS	Yes	No
SQL Server VDI	Yes	No

For pull-directed recovery for the applications listed in the preceding table, you can perform the following tasks:

- Run NMM recovery on the same server that the data is being backed up to but to a different location.
- Specify the alternate server to recover to.

Note: You can perform a SQL Server directed recovery (flat file recovery) to either of the following destinations:

- A different computer
- The original computer but a different location

The *NetWorker Module for Microsoft for SQL and SharePoint VSS User Guide* provides details.

Note: When you perform a directed recovery of Exchange Server, ensure that the following elements are the same for both the source and destination servers:

- The operating system and service packs
- Exchange Server 2019 and its CU levels
- Exchange Server 2016 and its CU levels
- Exchange Server 2013 and its CU levels
- Exchange Server 2010 and its RU levels

NMM backup and recovery requirements

This section provides information about NMM backup and recovery requirements.

Access privileges for backup and recovery

When installing NMM, you can run the System Configuration Checker from the installer. It is recommended that you run the System Configuration Checker to ensure that the setup is correctly configured for backup and recovery operations.

Before you perform backup and recovery operations, ensure that you enable the following privileges:


- To enable user access for NMM when User Access Control (UAC) is used, grant the "Log on as a batch job" privilege to the remote user who performs NMM operations. This act allows the user to log on with a privileged security token. Perform the following steps to grant the "Log on as a batch job" privilege:

1. On the client, open the Local Security Policy (`secpol.msc`) on the client.
 2. Click **Local Policies > User Rights Assignment**.
 3. Ensure that the Windows user or associated group has the **Log on as a batch job** privilege.
- The backup user is a part of the required Windows user groups on the application hosts.
 - The correct NetWorker user role is assigned to the backup user on the NetWorker server. The following table describes the backup user, the required Windows user groups on the application hosts, and the NetWorker user role.

The following table lists the access privileges for NMM backup and recovery.

Table 10 Access privileges for backup and recovery

Backup user type	Windows user groups on application host	NetWorker user roles
Exchange Server	<ul style="list-style-type: none"> • Backup Operators • Domain Users • Exchange Servers • Remote Desktop Users • Organization Management • Log on as Service 	Operators
Hyper-V Server	<ul style="list-style-type: none"> • Backup Operators • Domain Users • Remote Desktop Users 	Operators
SharePoint Server	<ul style="list-style-type: none"> • Backup Operators • Domain Users • Remote Desktop Users 	Operators
SQL Server (both VSS and VDI)	<ul style="list-style-type: none"> • Backup Operators • Domain Users • Remote Desktop Users 	Operators

 **Note:** Ensure that the *Operate NetWorker* privilege is set on the NetWorker server before you perform federated backups because the *Operate NetWorker* privilege is required to create additional backup and recovery jobs on remote hosts. The *Operate NetWorker* privilege is a part of the *Operators* role.

Adding Microsoft Windows groups and NetWorker administrative privileges

About this task

The NetWorker server recognizes domain names and Microsoft Windows groups, both local and global.

For example:

- Administrators group
- Domain Admins group

If you are logged in to a domain, the NetWorker server recognizes only the global group. You can discover the group name by running the Windows findgrp.exe utility, which is available with the Windows Resource Kit.

If you are logged in to an individual Windows computer, the NetWorker server recognizes only the local group, because no global group exists.

In cases where a user belongs to a domain that the server cannot contact, and therefore cannot verify the username, you can use a more specific user description to guarantee that the user has administrative rights to the server. The syntax for this user description is as follows:

- Single user:


```
user=user_name, domain=domain_name
```

- Group:

```
group=group_name, domainsid=domain_id
```

Setting AES data encryption

To use data encryption, you must use the NetWorker Administration GUI to set the datazone pass phrase for the NetWorker server. After the pass phrase is assigned, you can configure directives within NetWorker to use Advanced Encryption Standard (AES) encryption. AES data encryption is not recommended for Data Domain targets because it reduces deduplication efficiency.

 **Note:** Block Based Backup (BBB) for Exchange Server and Hyper-V Server does not support AES encryption.

- When you configure the client resources for VSS backups, in the **Create Client** window, on the **General** tab, in the **Directive** field, select **Encryption directive**. Complete this task for all applications for which AES encryption must be implemented. For example, in the following figure the Encryption directive is selected in the Directive field when configuring the client resource for SQL VSS backup.

Figure 4 Encryption directive for SQL VSS client resource configuration

The screenshot shows the 'Create Client' dialog box with the 'Backup' tab selected. The 'Identity' section on the left contains fields for 'Name:', 'Comment:', 'Tag:', and 'Backup type:'. The 'Checkpoint Restart' section has a 'Checkpoint enabled:' checkbox. The 'Backup' section on the right includes a 'Block based backup:' checkbox, a 'Directive:' dropdown menu set to 'Encryption directive', a 'Save set:' dropdown menu set to 'All', and a 'Protection group list:' section with checkboxes for 'Server Protection' and 'policy_sqlamr_wf_sqlamr'. At the bottom are 'OK', 'Reset', and 'Cancel' buttons.

- The *NetWorker Module for Microsoft for SQL VDI User Guide* provides information on how to implement AES encryption for a SQL VDI client resource.

Synchronizing NMM client and NetWorker server clocks

About this task

The clock times for the NMM client and NetWorker server must match for backups to work without any issues. If the clock times are not synchronized and differ by more than five minutes, problems occur when you try to recover full and incremental backups.

Identifying and back-translating computer names through name resolution

About this task

The NetWorker server and the NMM client need proper name resolution to identify and back-translate computer names.

For example:

- name-to-IP address
- IP address-to-name

Also, the NMM client uses the host server NETBIOS or short name when it connects to the NetWorker server to browse backups. If the NETBIOS name is not found, NMM cannot display backups.

Complete the required steps to ensure clear communication of computer names.

Procedure

1. Add the NetWorker server name to either of the following:


- The local hosts file, which is in the following location:
%SystemRoot%\system32\drivers\etc
 - The Domain Name System that contains the names of all servers on the network.
2. When you configure a client resource for solutions like Exchange, SharePoint, and so on, specify the NETBIOS name for the client in the Aliases attribute.

NMM Support Tools for recovery

NMM 9.0 and later does not support the `nsrnmmsstool` and `nsrsnap_vss_ssrecover` tools that are used for recovery in NMM 8.2.x.

In NMM 8.2.x, backups with browse policies that expire before the retention policy cannot be restored through the NetWorker User for Microsoft GUI. Index entries of the backups must exist to recover backups using the GUI. The `nsrnmmsstool` tool in NMM 8.2.x helps in recovering the client file indexes for the save sets whose browse policy has expired before the retention policy.

The `nsrnmmsstool` tool is not supported with NetWorker server 9.0 and later because the browse and retention policy are the same in NetWorker 9.0 and later. The `nsrsnap_vss_ssrecover` tool cannot be used in NMM 9.0 or later releases because NetWorker 9.2 and later backups are differently stored from NetWorker 8.2.x backups.

 **Note:** The NMM packaging support tools are unavailable for use with SQL Server VDI.

Using the `mminfo` command with NetWorker 8.2.3 or later server, NetWorker 19.2 client, and NMM 19.2 client

When you use a NetWorker server 8.2.3 or later with version 19.2 of the NetWorker and NMM clients, you can use the `mminfo` command to list and filter save sets.

In the following example configuration, NMM has two virtual machines, `vm1-windows7` and `vm2-windows7`. Each virtual machine has two virtual hard disks, and backups were performed on December 13, 2015 and December 14, 2015.

To recover the virtual machine `vm2-windows7` backups that were performed on December 13:

1. Get the save sets of the applications that were backed up on December 13.

```
mminfo -v -q "savetime>12/13/2015,savetime<12/14/2015" -r name
```

APPLICATIONS:\Microsoft Hyper-V

APPLICATIONS:\Microsoft Hyper-V\Host Component

APPLICATIONS:\Microsoft Hyper-V\Host Component\ConfigFiles

APPLICATIONS:\Microsoft Hyper-V\vm1-windows7

APPLICATIONS:\Microsoft Hyper-V\vm1-windows7\9D8F71EF-1B49-4237-BCFE-6179DB1323DB

APPLICATIONS:\Microsoft Hyper-V\vm1-windows7\A3231C45-7AD2-4C9E-9E5C-0D3D36015FA2

APPLICATIONS:\Microsoft Hyper-V\vm1-windows7\ConfigFiles

APPLICATIONS:\Microsoft Hyper-V\vm2-windows7

APPLICATIONS:\Microsoft Hyper-V\vm2-windows7\0EB90A1E-4095-4DC8-B85C-6CC210E80FBC

APPLICATIONS:\Microsoft Hyper-V\vm2-windows7\5E499BC1-8737-4331-9445-5AE4CF63867D

APPLICATIONS:\Microsoft Hyper-V\vm2-windows7\ConfigFiles

2. Get the SSID of vm2-windows7 of December 13:

```
mminfo -v -q "savetime>12/13/2015,savetime<12/14/2015" -N
"APPLICATIONS:\Microsoft Hyper-V\vm2-windows7" -r ssid
3631036106
```

3. Restore client file indexes for the vm2-windows7 of December 13 using the scanner command.

```
scanner -i -v -S 3631036106 \\pwsrv002\MyDev
```

Using the nsrnmrc.exe command with NetWorker 19.2 server, NetWorker 19.2 client, and NMM 19.2 client

You can perform flat file recovery of a Hyper-V or Exchange Server backups by using the nsrnmrc.exe command at the command prompt.

1. Use the mminfo command to generate a list of save sets:

```
mminfo -avot -q client=<client_name>
```

Where <client_name> is the name of the client where the backup resides.

2. Review the output and locate the save set ID (SSID) of the backup you must recover.

3. Type the following command with the SSID to generate the nsavetime for the backup:

```
mminfo -q ssid=<SSID> -r "name(50),ssid,savetime,nsavetime"
```

4. Review the output and note the nsavetime value.

5. Use the nsrinfc command to obtain the index path for the save set item:

```
nsrinfc -n [nmm | nmm_bbb] -s <server name> -t <nsavetime> <client name>
```

6. Use the nsrnmrc.exe command to restore the backup:

```
nsrnmrc.exe -s <server name> -c <client name> -A NSR_BBB_TRANSPORT=<yes/no>
-x <recovery_folder_path> -t <nsavetime> "APPLICATIONS:\Microsoft
<application_host>\<index_path>\\"
```

Where:

- The -x option is the directory for the flat file restore.
- NSR_BBB_TRANSPORT=Yes is the default option for Exchange Server and Hyper-V Server.

The following examples display sample commands for Hyper-V and Exchange Server:

- Hyper-V Server:


```
nsrnmrc.exe -s vmmsrv -c fmpcluster.aqua.local -A NSR_BBB_TRANSPORT=yes -x
c:\recover -t 1474605441 "APPLICATIONS:\Microsoft Hyper-V\vm1\\"
```

- Exchange Server with IP DAG:

```
nsrnmrc.exe -s nsr_server -c jetsdag -A NSR_BBB_TRANSPORT=yes -x
c:\recover -t 1474585250 "APPLICATIONS:\Microsoft Exchange 2013\Mailbox
Database 1\\"
```

- Exchange Server without IP DAG (IP-less DAG):

```
nsrnmrc -s NMMserver.demo.com -c nmmnode1.demo.com -x c:\pst -A
NSR_BBB_TRANSPORT=yes -t 1521248048 "APPLICATIONS:\Microsoft Exchange
2016\testmailbox\\"
```

 **Note:** For the -c option in this command, specify the node name, with which alias is associated, as the value. Do not specify the IP-less DAG name.

Refer to the following knowledge base article for more information:

https://emcservice--c.na16.visual.force.com/apex/KB_How_To?id=kA5j00000008VAJ

CHAPTER 2

NMM Client Graphical User Interfaces

This chapter includes the following sections:


- [Overview of NMM graphical user interfaces](#)..... 36
- [NetWorker User for Microsoft user interface](#).....36


Overview of NMM graphical user interfaces

The following user interfaces are available for NMM backup and recovery of Microsoft applications:

- NetWorker User for Microsoft GUI: This user interface uses the Hyper-V virtual machine recover APIs for RCT-based backups, and the VSS technology to recover all supported versions of the following Microsoft applications:
 - SQL Server
 - Exchange Server
 - Hyper-V Server
 - SharePoint Server
 - Active Directory

[NetWorker User for Microsoft user interface](#) on page 36 provides more information.
- Data Protection Add-in for System Center Virtual Machine Manager (SCVMM): The *NetWorker Module for Microsoft for Hyper-V User Guide* provides details.
- NMM Hyper-V File Level Recovery (FLR) GUI: The Hyper-V FLR GUI is fully web-based and runs in a web browser. The *NetWorker Module for Microsoft for Hyper-V User Guide* provides more information.

 **Note:** NMM does not support the Hyper-V FLR GUI from the next release. The NetWorker User for Microsoft GUI and the Data Protection Add-in for SCVMM provide the entire functionality that the Hyper-V FLR GUI provides.
- NMM Microsoft SQL Server Management Studio (SSMS) plug-in GUI: This user interface uses the VDI technology to back up and recover the supported versions of SQL Server. The *NetWorker Module for Microsoft for SQL VDI User Guide* provides more information.
- NetWorker SQL Ad-hoc plug-in: You can install the NetWorker SQL Ad-hoc plugin during the NMM installation. This plugin enables the user to perform manual backups and recoveries from the Microsoft SQL Server Management Studio GUI. The *NetWorker Module for Microsoft for SQL VDI User Guide* provides more information.

 **Note:** NetWorker SQL Ad-hoc plugin support is unavailable for SQL Server 2005 (x86).

NetWorker User for Microsoft user interface


The NetWorker User for Microsoft user interface has specific views and display conventions that enable you to perform basic tasks.

To start the GUI, select **Start > Programs > NetWorker Modules > NetWorker User for Microsoft** on the host where NMM is installed.

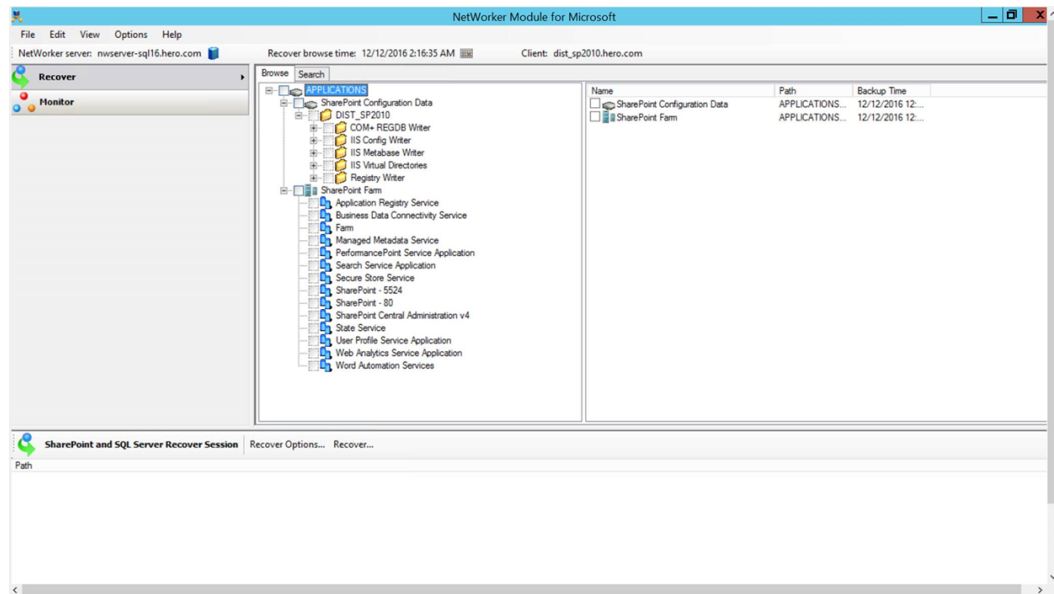
User interface views

The NetWorker Module for Microsoft GUI has two views, as described in the following topics.

Recover view


All recoveries are performed from the Recover view by selecting the Recover icon  on the left of the NetWorker User for Microsoft GUI main page.

The following figure displays the Recover view.

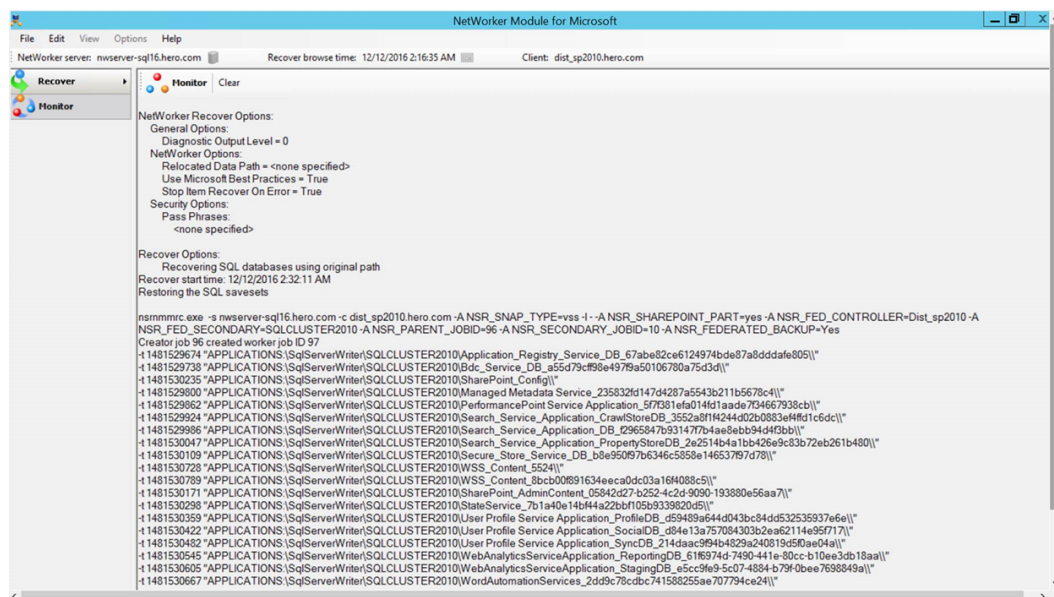
Figure 5 Recover view of the NetWorker User for Microsoft GUI main page

The summary of selected items can also display exclusions, which are those items that are not selected for recovery. This view can be helpful when many items are selected for recovery.

Monitor view

Recovery and snapshot management operations can be monitored in the Monitor view by selecting the Monitor icon  on the left of the NetWorker User for Microsoft GUI main page.

The following figure displays the Monitor view.

Figure 6 Monitor view of the NetWorker User for Microsoft GUI main page







Most messages that are displayed in the Monitor view are also written to log files. The Troubleshooting chapter provides more information about log files. You can also copy and paste text from the Monitor view to another application.

Display conventions

The NetWorker User for Microsoft GUI uses specific icons to identify various tasks and operations.

The following table outlines the main conventions used in the NetWorker User for Microsoft GUI.

Table 11 Icons used in the NetWorker User for Microsoft GUI

Icon	Name	Description
	NetWorker server	Displays the NetWorker server that is installed.
	Recover	Displays the Recover view to perform recoveries.
	Exchange Recover Session	Enabled when the Recover icon is selected. Allows you to continue with recovery.
	Monitor	Displays the Monitor view to monitor recovery and provides snapshot management options.
	Log files	Displays the log files that contain backup and recovery details.
	Database	Displays available databases.

Connecting to a NetWorker server

About this task

This topic provides information about launching the NetWorker User for Microsoft GUI.

 **Note:** You can also click **Options > Configure Options** to connect to a NetWorker server.

Procedure

- From the **Start** menu, open the NetWorker User for Microsoft GUI:
 - If you have opened the NetWorker User for Microsoft GUI before, go to the next step.
 - If this is the first time you have opened the NetWorker User for Microsoft GUI, the **Change NetWorker Server** dialog box appears. Continue to [step 3](#).
- From the **Main** toolbar, click **NetWorker Server**.
The **Change NetWorker Server** dialog box appears.
- Click **Update Server List** to browse for NetWorker servers. The discovery process might take a few minutes.
- When the list is updated, perform one of the following tasks:
 - Select a server. The selection appears in the **Server** field.
 - In the **Server** field, type the name of the server.
- Click **OK**.

Specifying recovery browse times in the NetWorker User for Microsoft GUI

About this task

The NetWorker User for Microsoft GUI navigation tree displays backup items from the specified date and earlier.

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. On the application toolbar, click the icon beside the **Recover browse time** field.
3. In the **Change Time** dialog box, select the arrows to select the date and time, and then click **OK**.

Searching for items

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. To search for items, perform one of the following steps:
 - In the middle panel, click the **Search** tab.
 - In the middle panel, on the **Browse** tab, perform any of the following steps:
 - To search at root-level, right-click the Microsoft application, and then select **Search for**.
 - To search at a save set-level, expand the Microsoft application, right-click the save set, and then select **Search for**.
3. In the **Path** field, type a folder path.
4. (Optional) In the **Name** field, type the name of the search item. You can refine the search by using the any of the following types of search:
 - Literal match (case-insensitive): Type `abc` to return `abc`, `ABC`, or `AbC` but not `abcd` or `ABCD`.
 - Literal match (case-sensitive): Type `"abc"` to return `abc`, but not `ABc` or `abcd`.
 - Name contains (case-insensitive): Type `%abc%` to return `abc`, `abcd`, `ABCD`, or `xyzABCde`.
 - Name starts with (case-insensitive): Type `abc%` to return `abcd` or `ABCde`, but not `xyzABCde`.
 - Name ends with (case-insensitive): Type `%abc` to return `xyzAbc`, but not `ABCde`.
 - Single-character match search by using the `?` wildcard:
 - Type `?` to return single character entries and drive volumes, such as `C` or `D`.
 - Type `WMI?Writer` to return `WMI Writer`.
 - Multiple-character match search by using the `*` wildcard:
 - Type `*.txt` to return all entries with a `.txt` extension.
 - Type `*` to return all items within the selected container.
 - Type `*writer*` to return all writers.
 - Search by using the `*` and `?` wildcards: Type `????*writer*` to return `WMI Writer`.
5. Click **Search**.

The **Result** panel displays the search results.

Selecting items for recovery

About this task

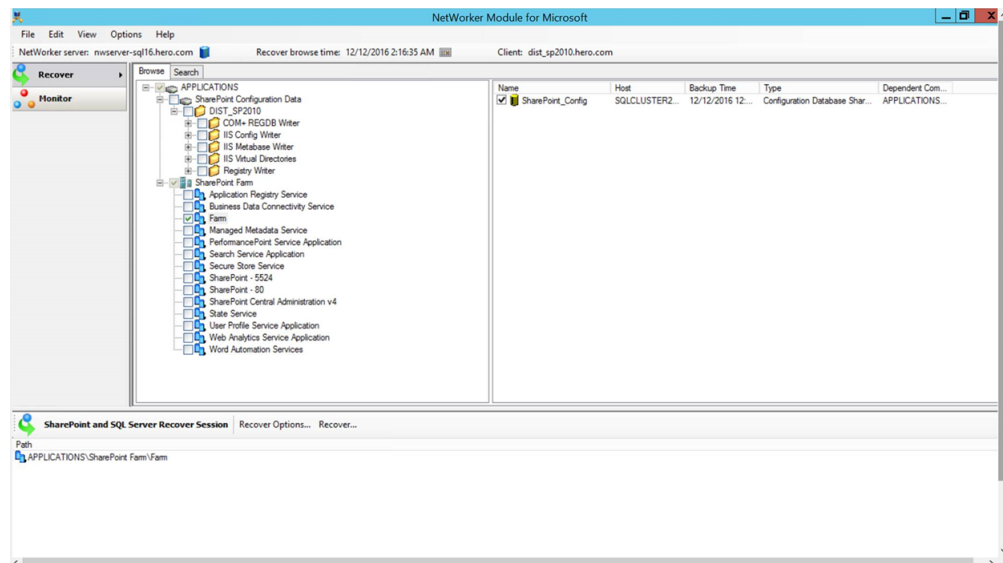
To select items for recovery, select the checkbox beside a node in the navigation tree. A check mark indicates that the node is selected. By default, all items that are contained in the node, such as folders and files, are also selected for recovery.

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. Expand the node that you must back up in the navigation tree.
3. To eliminate an item from the recovery process, clear the checkbox beside the item.

The following figure depicts one selected node and several partially selected nodes in the navigation tree.

Figure 7 Selected and partially selected items



Marked objects

About this task

This topic describes the meaning of marked objects.

- **Unmarked**—An unmarked item is one that is not selected for backup or restore. An empty checkbox appears to the left of an unmarked item.
- **Marked**—A marked item is one that is selected for backup or restore. A check mark appears in the checkbox to the left of an marked item.
- **Partially marked**—A partially marked item is one that has marked descendants, but the item itself is not marked. A partially marked item is not backed up or restored. A check mark appears in a gray checkbox to the left of a partially marked item.

Viewing required volumes for recovery

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. In the middle panel, on the **Browse** tab, expand the Microsoft application, and then select the save set that you want to recover.
3. Right-click the selected save set, and then select **Required volumes**.
4. In the **Required NetWorker Volumes** dialog box, review the list of volumes, and then click **OK**.

Selecting backup versions for recovery

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. In the middle panel, on the **Browse** tab, expand the Microsoft application, and then select the save set that you want to recover.
3. Right-click the selected save set, and then select **Versions**.
4. In the **NetWorker Versions** dialog box:
 - a. Select the backup time.
 - b. Select **Use selected item backup time as new browse time**.
 - c. Click **OK**.

CHAPTER 3

NetWorker Client Management

This chapter includes the following sections:

- [Configuring Microsoft application server](#)44
- [Configuring NetWorker privileges manually](#)46

Configuring Microsoft application server

About this task

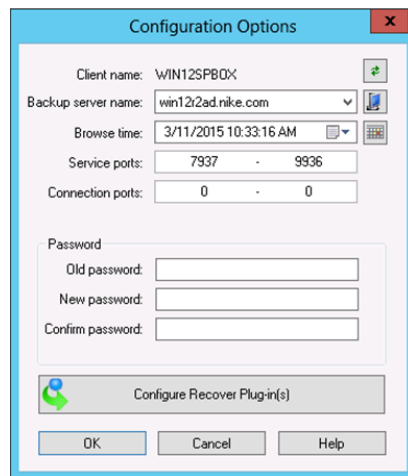
This procedure describes how to configure Microsoft application server by using the NetWorker User for Microsoft GUI.

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. From the **Options** menu, select **Configure Options**.

The **Configuration Options** dialog box appears.

Figure 8 Configure Options dialog box



3. To specify the Microsoft application server that you want to back up, click the icon beside the **Client name** list.

In the **Select Viewable Clients** dialog box:

- a. From the **Available clients on <NetWorker_server_name>** list, select the Microsoft application server, and then click **Add**.
The selected server appears in the **Clients to list on menu bar** list.
 - b. Click **OK**.
4. In the **Configuration Options** dialog box, from the **Backup server name** list, select the NetWorker server, to which you want to connect the Microsoft application server.

To specify a NetWorker server that is not available in the list:

- a. Click the icon beside the **Backup server name** list.
The **Change NetWorker Server** dialog box appears.
- b. To obtain the list of all available NetWorker servers, click **Update Server List**.
- c. Select the NetWorker server.
- d. Click **OK**.

The NetWorker server name appears in the **Backup Server Name** field.

NOTICE You can also connect to a NetWorker server by clicking the NetWorker server icon on the application toolbar.


5. In the **Browse time** list, select the recovery browse time.

To specify a browse time that is not available in the list, click the icon beside the **Browse time** list, and then specify the required recovery browse time.

6. In the **Service ports** field, type the range of the available ports.

A service port is a listener port that provides services to NMM client hosts. The default range of service ports is 7937 - 9936.

To implement an enhanced security environment, it is recommended that you reduce the range of available ports. The *NetWorker Administration Guide* provides more information about determining the range of the ports.


 **Note:** If a firewall exists between the NetWorker client and any NetWorker servers, ensure that the firewall is configured to accept the port ranges that you type in this field.

The *Configuring TCP Networks and Network Firewalls for NetWorker technical note*, which is available on Online Support website, provides more information about how to identify and configure the required ports for NetWorker hosts that must communicate across a packet filtering or stateful inspection firewall.

7. In the **Connection ports** field, type the range of the available ports.

A connection port is used to contact a service on a NetWorker server, a storage node, or a client. The default range of connection ports is 0 - 0.

To implement an enhanced security environment, it is recommended that you reduce the range of available ports. The *NetWorker Administration Guide* provides more information about determining the range of the ports.

 **Note:** If a firewall exists between the NetWorker client and any NetWorker servers, ensure that the firewall is configured to accept the port ranges that you type in this field.

The *Configuring TCP Networks and Network Firewalls for NetWorker technical note*, which is available on Online Support website, provides more information about how to identify and configure the required ports for NetWorker hosts that must communicate across a packet filtering or stateful inspection firewall.

8. To change the PW1 password, a protection for the items or files that you back up:

- a. In the **Old password** field, type the password that is in effect.
- b. In the **New password** field, type the new password.
- c. In the **Confirm password** field, retype the new password.

The new password is applied to future scheduled backups of the NMM client, where password-protection is enabled on the NetWorker server with a global or local directive.

Changing the password does not change the password for the backed-up files.

To recover PW1 or PW2 password-protected files, provide the password that was in effect at the time of the backup.

The *NetWorker Administration Guide* provides more information about PW1 and PW2 password-protection.

9. To select the required recover plug-ins for Microsoft applications, click **Configure Recover Plug-in(s)**.
10. In the **Configure Recover Plug-in(s)** dialog box:

- a. From the **Active Plug-in(s)** list, select the recover plug-in that you do not require, and then click the right-arrow to move the plug-in to the **Disabled Plug-in(s)** list.

Repeat this step for all the plug-ins that you do not require.

To move a plug-in from the **Disabled Plug-in(s)** list to the **Active Plug-in(s)** list, select the plug-in in the **Disabled Plug-in(s)** list, and then click the left-arrow.

When you perform a recovery, only the recover plug-ins that are listed in the **Active Plug-in(s)** list appear.

- b. Click **OK**.
11. In the **Configuration Options** dialog box, click **OK**.

Configuring NetWorker privileges manually

NMM requires that user groups have specific privileges to perform certain operations.

About this task

The following table outlines the user group privileges that are required for NMM backup operations.

Table 12 User group privileges for NMM operations

Operation	Required user group privilege
Federated backup	Operate NetWorker
Backup deletion	Changed Application Settings

Complete the following steps to configure NetWorker user group privileges manually.

Procedure

1. Open the NetWorker Administration GUI.
2. Click **Server**.
3. In the expanded left pane, click **User Groups**.
4. Right-click the appropriate user group, and then select **Properties**.

The **Properties** dialog box appears.

5. In the **Users** field, add the following values for the NMM client host. Type each value on a separate line:

```
user=NMM_Exchange_backup_admin_user,host=NMM_client_host
user=system,host=NMM_client_host
```

where *NMM_client_host* is the DNS hostname of the NMM client.

6. Click **OK**.
7. Configure the user group privilege as described in the application-specific user guides.

CHAPTER 4

Restricted Data Zone

This chapter includes the following sections:

- [NMM support for NetWorker Restricted Datazone](#)..... 48
- [Recommendations](#)..... 49
- [Providing required privileges for RDZ support in NMM](#)..... 49

NMM support for NetWorker Restricted Datazone

NMM includes the NetWorker support for the Restricted Datazone (RDZ) feature. The *NetWorker Administration Guide* provides an introduction to RDZ feature, which is under the multi-tenancy support provided by NetWorker.

The RDZ feature enables a privileged administrator to define restrictions for a datazone and to segment existing resources (called Restricted Datazone resources) into sub segments. An RDZ resource contains a list of users and privileges with a restriction on the number of clients, storage nodes, jukeboxes, and devices that are allowed to be associated with the RDZ. To create detailed permissions, you can set up multiple RDZ resources with different user lists and permission sets for the same RDZ.

 **Note:** NMM does not support external roles for RDZ for SQL Server.

An RDZ can be associated with the following resources:

- Protection groups
- Policy
- Clients
- Devices
- Directives
- Jukeboxes
- Labels
- Media pools
- Data protection policies
- Storage nodes
- Operation status

Resource association allows resources to be visible not only to the NetWorker administrator, but to anyone through the RDZ resources user lists. These associations are dependent on when the RDZ counts are checked. If the counts are lower than the number of resources that are associated with it in the relative field, an error message is displayed and the resource is not created or modified.

Two kinds of association, restricted users and restricted owners, exist between RDZ and other resources. If a user is associated with the Restricted Owner setting, all the permissions that the user has in the RDZ are applied to the resource. There is one exception; an associated Restricted Owner cannot modify either the Restricted Owners or Restricted Users list to prohibit the people on those lists from seeing the resource. Restricted Users and Restricted Owners are similar except Restricted Users cannot make direct changes to the resource. They can operate the resource and cause indirect updates to occur as a result of operating the resource.

If the Restricted Owner who creates the resource is part of an RDZ, resource associations occur automatically. Otherwise, resource association occurs through manual change by a NetWorker administrator. When a resource that is associated to other resources (such as a group is associated with clients) is associated with an RDZ resource, it is also modified to match the Restricted Users or Restricted Owners.

A resource can be associated with one or more RDZ. If a resource is associated with an RDZ, it is not a resource that the main datazone can use as a normal resource. The *NetWorker Administration Guide* provides information about configuring a restricted datazone.

The RDZ resource is created either in the **Server** tab of the NetWorker Administration GUI or through the `nsradmin` application. A privileged administrator creates RDZ resources.

Recommendations

Follow these recommendations when you use the RDZ support in NMM:

- Create an additional device for the main datazone for client bootstrap and index backup. This requirement is the same as RDZ backup and recovery of NetWorker file systems.
- Provide system permission, not group permission if you have provided group permission, do not provide system permission.
- A user in an RDZ does not require any additional permission to perform an operation. The permission for a user in an RDZ and a main zone are the same for NMM operations.

Providing required privileges for RDZ support in NMM

About this task

This procedure provides the steps to configure privileges for RDZ.

The *NetWorker Administration Guide* provides information about configuring an RDZ and the complete list of privileges.

Procedure

1. Open the NetWorker Administration GUI.
2. Click **Server**.
3. In the expanded left pane, select **Restricted Datazones**.
4. In the list that appears in the right pane of the window, right-click the RDZ and select **Properties**.
5. In the **Restricted Datazone Properties > General** tab, under **User Configuration**, type the following information in the **Users** field for each node that is part of the backup and recovery process:

```
user=name,host=client name
user=system,host=client name
```

6. In the **Privileges** field, select the options that are listed in the following table, and then click **OK**.

Table 13 Privileges options for RDZ

Environment	Task	Privileges option
All setups	Backup	<ul style="list-style-type: none"> • Monitor NetWorker • Backup Local Data • When creating a client resource, you must also select the higher-level permission, Create Application Settings.
	Recovery	<ul style="list-style-type: none"> • Monitor NetWorker • Recover Local Data

Table 13 Privileges options for RDZ (continued)

Environment	Task	Privileges option
Cluster (Exchange DAG, Hyper-V CSV, or Hyper-V SMB)	Backup	<ul style="list-style-type: none"> • Monitor NetWorker • Backup Local Data • Backup Remote Data • Remote Access All Clients • When creating a client resource, you must also select the higher-level permission, Create Application Settings.
	Recovery	<ul style="list-style-type: none"> • Monitor NetWorker • Recover Local Data • Recover Remote Data • Remote Access All Clients

CHAPTER 5

VSS-Based Scheduled Backups

This chapter includes the following sections:

- [Configuring a client resource](#).....52
- [Considerations when using the Client Backup Configuration wizard for NetWorker server 8.2.3 or later and NMM 19.2](#).....52
- [Creating a client resource by using the Client Backup Configuration wizard](#).....53
- [Manually creating a client resource by using the Client Properties dialog box](#).....53
- [Considerations and recommendations for application backups](#).....55

Configuring a client resource

A NetWorker client (client resource) is a resource that is configured on the NetWorker server.

About this task

For each client resource, the NetWorker server performs the following operations:

- Maintains the client resource information, including entries in the online client file index and media database.
- Performs the scheduled backups when a client request is received.
- Restores the data when a client request is received.

You can create multiple client resources for the same NMM client host. With this strategy, you can apply different backup attributes to different types of information on the same host. However, the **Remote access** field in the Client Properties page for all instances of the same client contain the same information. Any change in the **Remote access** field for any one instance is reflected in all the instances of the same client resource.

Although the general process for configuring a client resource is the same for all applications or systems and is performed through the NetWorker Administration GUI, some applications might have differences in their specific settings and requirements. These settings and requirements are described in the scheduled backup chapter of each application user guide.


Before you create the client resources, set the appropriate attribute values for the Policy and Group resources. You must be an administrator to perform this task. The *NetWorker Administration Guide* provides detailed information.

Configure a client resource by using either of the following methods:

- Using the Client Backup Configuration wizard (the recommended method)
- Typing the details manually on the Client Properties page

Considerations when using the Client Backup Configuration wizard for NetWorker server 8.2.3 or later and NMM 19.2

If you are using NetWorker server 8.2.3 and NMM 19.2:

- For the Client Backup Configuration wizard to function properly, ensure that JRE 8 or later is installed on the host, where the NetWorker Management Console (NMC) is used. However, NMC of NetWorker 8.2.3 requires JRE 7.
- Before you run the NMM 19.2 Client Backup Configuration wizard to modify a client resource that was created with NMM 8.2.x, ensure that the Snapshot attribute of the NetWorker group that this client resource belongs to is clear. If the Snapshot attribute is selected, the NetWorker group cannot be selected in the wizard and you are prompted to create or select another group.
 **Note:** This requirement does not apply to SQL Server VDI and Active Directory.
- NetWorker server 8.2.3 and later use a different procedure to create client resources than NetWorker server 19.2. Follow the procedure provided in the Scheduled Backup chapter of each application user guide.

Creating a client resource by using the Client Backup Configuration wizard

You can use the Client Backup Configuration wizard in the NetWorker Management Console (NMC) to create client resources for VSS-based backups of Hyper-V Server, SharePoint Server, and Exchange Server. The wizard fetches the required information from the configuration setup and configures the client resources.

About this task


You cannot use the Client Backup Configuration wizard to create client resources for VSS-based backups of SQL Server and Active Directory.

Procedure

1. Open the NetWorker Administration GUI.
2. Click **Protection**.
3. In the expanded left pane, select **Clients**.
4. Select **File > New > Client Backup Configuration**.

The **Client Backup Configuration** wizard appears.

5. On the **Specify Client Information** page, in the **Client Name** field, type either the hostname or the Fully Qualified Domain Name (FQDN) of the client.


 **Note:** Do not type the IP address of the client.

6. Specify the other fields on the **Specify Client Information** page, and the other pages of the wizard according to the Microsoft application that you use, and your requirements.

Each application-specific user guide provides detailed information about how to create a client resource.

Manually creating a client resource by using the Client Properties dialog box

About this task

 **NOTICE** The procedure to create a client resource when you use NetWorker server 8.2.3 or later is different from the procedure to create a client resource when you use NetWorker server 19.2. When you use NetWorker server 8.2.3 or later and NMM 19.2, ensure that you perform the following steps:

- Configure a regular NetWorker backup group instead of configuring a data protection policy. Do not enable the **Snapshot** option in the **Group Properties** dialog box.
- Type `nsrnmmsv.exe` in the **Backup Command** field in the **Client Properties** dialog box.

To manually create a client resource by using the **Client Properties** dialog box, perform the following steps:

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left panel, select **Clients**.

3. Click **View > Diagnostic Mode**.


4. Click **File > New**.

The **Client Properties** dialog box appears.

5. On the **General** tab:

- a. In the **Name** field, type either the hostname or the FQDN of the client.

The client must be a fully qualified host to be a NetWorker client.

 **Note:** In this field, do not type the IP address of the client.

- b. In the **Comment** field, type a description.

- c. In the **Tag** field, type one or more tags to identify this client resource for the creation of dynamic client groups for data protection policies.

Dynamic client groups automatically generate a list of clients for a data protection policy that is based on the tags that are assigned to the client and group.

- d. To perform Hyper-V and Exchange Server backups, select **Block based backup**. Do not select this option for option for SQL Server VDI, SQL Server VSS, and SharePoint Server.

- e. From the **Directive** list, select an option.

A directive is an instruction to take special actions on a specified set of files for a specified client during a backup. The *NetWorker Administration Guide* provides information about directives.

- f. In the **Save set** field, specify the save set name of the application that you want to back up.

- g. From the **Protection group list**, select the required protection group.

The *NetWorker Administration Guide* provides details about protection groups.

6. On the **Apps & Modules** tab.

- a. In the **Access** area, leave the **Remote user** and **Password** fields empty.

- b. In the **Backup command** field, type the backup command:

```
nsrnmmsv.exe
```

- c. In the **Application Information** field, specify application information variables according to your requirement.

- d. Under **Deduplication**, specify the relevant deduplication fields.

- e. Specify the other fields according to your requirement.

7. Specify the fields on the other tabs according to your requirement.

8. Click **OK**.

Editing a client resource that is created with NMM 9.0 or later

You can edit a client resource after it has been created by completing the following steps.

Procedure

1. In the Administration window, click **Protection**.

2. Right-click **Clients** in the navigation tree or right-click the required client in the **Clients** table.
3. Select **Modify Client Properties**.
4. Make the required changes for the client resource.
5. Click **OK**.

Editing a client resource that was created with NMM 8.2.x after you upgraded to NMM 9.0 and later

After you upgrade to NMM 9.0 and later, you must modify all the client resources to recover the NMM 8.2.x backups.

Procedure

1. In the Administration window, click **Protection**.
2. Right-click **Clients** in the navigation tree or right-click the required client in the **Clients** table.
3. Select **Modify Client Properties**.
4. In the **Backup Command** field, delete the `nsrnsnap_vss_save` command and type the `nsrnmmsv.exe` command. This change must be performed for all the existing client resources.
5. Make other changes, if required.
6. Click **OK**.

Editing existing client resources through the NMC bulk edit feature

You can edit all the client resources at once with the bulk edit feature. The NMC bulk edit feature must be used on a group of client resources that use the same backup command and options. For example, you must use the bulk edit option for all the client resources where the backup command uses the `-D` option.

Considerations and recommendations for application backups

The following table provides detailed information.

Table 14 Best practices for application backups

Consideration	Best practice
Define different schedules for protecting the following: <ul style="list-style-type: none"> • The operating system • The application that is to be backed up 	For application servers, such as SQL Server or Exchange Server, back up the server application data under a schedule that is different than the backup made of host operating system data and attached volumes. Typically, application data is backed up several times a day while operating system data and volumes are backed up less frequently.
Move an NMM client to a different NetWorker server	An NMM client should be protected by only one NetWorker server. Do not set up scheduled backups for an NMM client on multiple NetWorker servers. If the NMM client is configured with a different NetWorker server from the NetWorker server that is set up for

Table 14 Best practices for application backups (continued)

Consideration	Best practice
	<p>scheduled backups, you can move the NMM client by performing the following steps:</p> <ol style="list-style-type: none"> 1. On the NetWorker server that you are moving from, disable or delete the client resources that are set up for the NMM client. You can disable a client resource for scheduled backup by clearing the Scheduled backup attribute in the client resource. 2. On the NetWorker server that you are moving to, set up scheduled backups for the NMM client.
Installation path for application server program	Do not install application server program files on the same volume as the application's database files and the log files.
Enable SQL Server data recovery	<p>If the SQL Server Writer service is disabled, perform the following steps to enable the recovery of all SQL data:</p> <ol style="list-style-type: none"> 1. Re-enable the SQL Server Writer service. 2. Back up the SQL Server.
Perform a full backup	<ul style="list-style-type: none"> • For the Exchange database that was recovered (not all databases). • For Exchange Server if an Exchange Service Pack was installed.
When database names contain French and Spanish characters, successful backups of database are possible when you type the database name in the save set.	<p>Unicode characters are not printed in the Command Prompt on Windows.</p> <p>This is a Windows operating system issue.</p> <p>A backup that contains databases with unicode characters in their names fails when you run the <code>nsrnmmsv.exe -?</code> command. The backup fails because the output is not a valid component.</p>
Backing up a clustered NMM client	<ul style="list-style-type: none"> • Configure a client resource: Configure a client resource for each virtual server that is being backed up and for each physical node in the cluster on which the virtual server can run. In each client resource, type the names of the physical nodes of the cluster in the Remote Access attribute. • Configure NetWorker administrator privileges: Configure NetWorker administrator privileges for each physical node in the cluster and for each proxy client in the cluster. • Configure a proxy client: Configure a proxy client for a clustered NMM client. • Do not use the pathownerignore functionality: NMM does not enforce this restriction. <p>Ensure that a <code>nsr\bin\pathownerignore</code> file is not used or set. In some circumstances, during a backup,</p>

Table 14 Best practices for application backups (continued)

Consideration	Best practice
	<p>NMM might ignore the path owner and the data from a clustered disk is backed up in the physical node indexes. However, the recovery of the data fails. Clustered disks must be backed up under a virtual cluster client.</p> <ul style="list-style-type: none">• Cluster failover and backups: If a node within a cluster fails during a backup, the backup fails. The next scheduled backup operation is the next valid backup.

CHAPTER 6

Data Deduplication with Data Domain

This chapter includes the following sections:

• Overview of deduplication support with Data Domain.....	60
• Client Direct data deduplication backup and recovery.....	60
• Data Domain and NetWorker server configuration.....	61
• Data Domain Boost data deduplication capabilities.....	62
• Configuring data deduplication for Data Domain clients.....	62
• Recovering deduplicated data.....	64

Overview of deduplication support with Data Domain

NMM supports deduplicated backups and restores with a Data Domain system. You can configure the Data Domain system as NetWorker AFTDs, virtual tape library (VTL) devices, or DD Boost devices.

A Data Domain deduplication backup to an AFTD, VTL, or DD Boost device can be a manual backup or a scheduled backup.

The first Data Domain backup backs up all the specified data and achieves the least amount of data deduplication, referred to as compression or global compression in Data Domain documentation. Subsequent Data Domain backups achieve improved deduplication rates as the backups identify more and more redundant data blocks.

For information on software requirements, supported operating systems, and Microsoft application versions that are supported in NMM for deduplication with Data Domain, see the *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/elb/elbhome>.

 **NOTICE** Client Data Domain Boost deduplication support is unavailable for Active Directory.

The *NetWorker Data Domain Boost Integration Guide* provides information about the Data Domain server and NetWorker server setup and configuration, and is available at <http://support.emc.com>.

Client Direct data deduplication backup and recovery

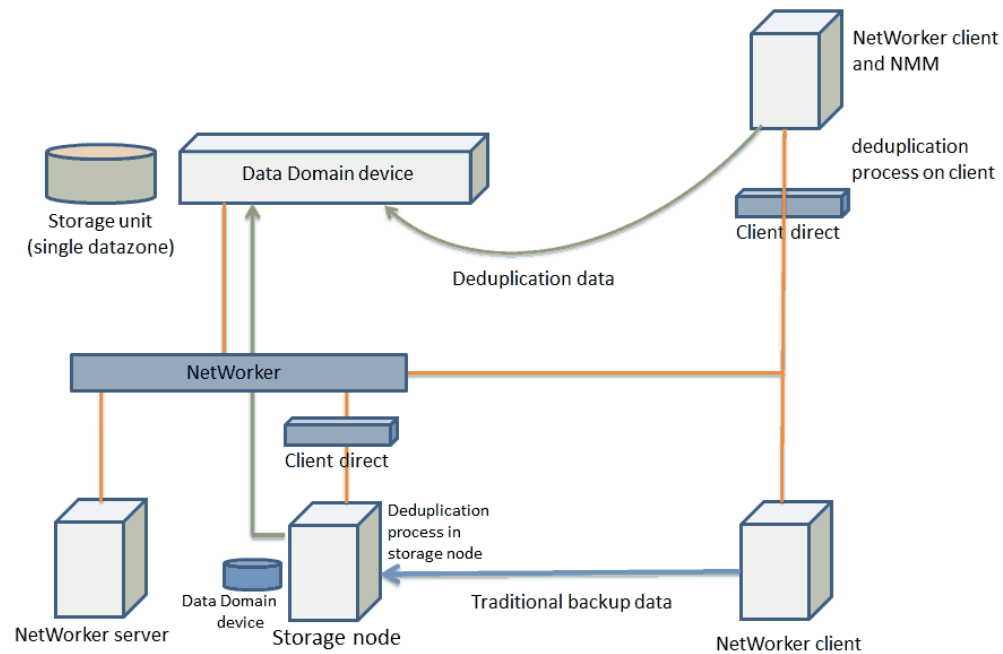
For some types of data, Data Domain devices support Client Direct, which enables client-side data deduplication backup and recovery.

This Client Direct deduplication method has the following advantages:

- The client directly writes to a Data Domain device, eliminating the need for a dedicated storage node configuration.
- Data deduplication on the client host reduces the bandwidth for the data transfer.

Client Direct data deduplication enables multiple hosts to share a Data Domain device. Multiple sessions on a single device can improve performance.

The following figure shows an example environment where Client Direct with distributed segment processing (DSP) is used to send deduplicated backup data directly from the client to a NetWorker Data Domain device. The same environment can also be used to send deduplicated data from the storage node to the Data Domain device during the data deduplication backup.

Figure 9 Client Direct data deduplication environment

Backup support

The Client Direct feature enables supported NetWorker clients to deduplicate their backup data locally and to store it directly on a Data Domain device, thereby bypassing the NetWorker storage node and reducing network bandwidth usage. Because multiple clients with Client Direct backup support can share a device by using multiple sessions, Client Direct can reduce the number of devices used, which reduces the impact on the Data Domain system performance and maintenance.

Recovery support

If a supported Client Direct client has access to its NetWorker Data Domain storage device, the client recovers data directly from the device, regardless of whether Client Direct was used for the backup. Because Client Direct bypasses the storage node, performance is improved.

If the Client Direct client cannot access the data, the recovery process reverts to the traditional method that uses the storage node. The Data Domain system converts the stored data to its original non-deduplicated state for the recovery.

Data Domain and NetWorker server configuration

The NMC provides configuration, monitoring, and reporting of backup and restore operations on NetWorker Data Domain devices. The NMC is accessible from any supported remote internet browser.

The Client Configuration Wizard simplifies the configuration of storage devices, backup clients, storage (target) pools, volume labeling, and save set cloning.

The following table provides the configuration details for Data Domain and NetWorker.

Table 15 Configuration details for Data Domain and NetWorker

Feature	Consideration
Optimized cloning	No special procedures or considerations are required for Data Domain optimized cloning by NMM.
Data Domain storage node	No special procedures or considerations are required when using Data Domain storage node with NMM.
Client IO optimization (Data Domain Boost)	The topic, Configuring client resources , provides more information.

Data Domain Boost data deduplication capabilities

The NetWorker integration with Data Domain Boost logical storage devices on Data Domain systems enables backup data to be deduplicated on a NetWorker storage node before the data is sent for storage on a Data Domain system. This feature dramatically reduces the amount of data that is sent and stored on the Data Domain system and reduces the bandwidth that the storage process uses.

The DD Boost software enables multiple concurrent storage and recovery operations, unlike conventional virtual tape library (VTL) and CIFS or NFS AFTD interfaces on Data Domain systems.

DD Boost software consists of the following two components:

- The DD Boost library API enables the NetWorker software to communicate with the Data Domain system.
- The DSP feature enables data deduplication to be performed on a NetWorker storage node or other supported host before the data is sent to the Data Domain system for storage.

Deduplicated data backups are stored on special Data Domain (DD Boost) storage devices on the Data Domain system that are accessed by the NetWorker storage nodes and server.

Enabling Client Direct backups over Fibre Channel

NMM supports backups to DD Boost devices over Fibre Channel.

To enable Client Direct backup to a DD Boost device over Fibre Channel, ensure that the database-specific operating system user has the correct device permissions as described in the following article:

Fibre Channel Devices with Products using DD Boost in Windows Environment (Document ID dd95005)

Use the document ID to search for this article on the Online Support website.

The *NetWorker Data Domain Boost Integration Guide* provides client and device configuration instructions for NetWorker backup and recovery operations.

Configuring data deduplication for Data Domain clients

About this task

After the Data Domain server and NetWorker server have been configured for deduplication, configure a client resource to use deduplication. A storage node, which is configured with at least

one Data Domain device, must exist for client IO optimization. For a Data Domain Boost backup, ensure that the device is a Data Domain device and that the enabler has been applied.

Procedure

1. Create a client resource.
2. In the **Clients** table, right-click the client and select **Properties** to edit the client resource.

The **Client Properties** window appears.

3. Click the **General** tab, and then ensure that the **Client direct** checkbox is selected to use the client direct functionality.

Note: The Client Direct functionality is available only when you use a Data Domain device or an AFTD device.

4. Click the **Apps & Modules** tab. In the **Deduplication** group, select the **Data Domain Backup** checkbox.

The **Client Properties** page with the **Apps & Modules** tab appears, as shown in the following figure.

Figure 10 Apps & Modules tab with the deduplication attribute

The screenshot shows the 'Client Properties - SHP2013SP1.WOW.COM' window with the 'Apps & Modules' tab selected. The window is divided into several sections:

- Access:** Fields for 'Remote user:' and 'Password:'.
- Backup:** Fields for 'Backup command:' (nsrnmmsv), 'Pre command:', 'Post command:', 'Save operations:', 'NAS device:' (checkbox), 'NDMP:' (checkbox), 'NDMP array name:', 'Application information:', and 'Backup config:'.
- Deduplication:** Fields for 'Data Domain backup:' (checkbox), 'Data Domain interface:' (dropdown menu showing 'IP'), 'Avamar deduplication backup:' (checkbox), and 'Avamar deduplication node:' (dropdown menu).
- Probe:** Field for 'Probe resource name:' (dropdown menu).
- Proxy Backup:** Radio buttons for 'None' (selected), 'SCSI', and 'VMware'. Below each radio button is a 'Proxy host:' field.

5. Click the **Globals (2 of 2)** tab, provide the remote storage node name where the Data Domain device is configured.

This name should be the only entry.

During the backup, the NMM client performs the following tasks:

- Contacts this storage node to obtain the Data Domain device credentials.
- Establishes a connection by using these credentials.

- Sends data directly to the Data Domain system.
6. Click **OK**.
 7. (Optional) To verify that a backup is successful by typing the following command:

```
mminfo -avot -s server_name -c client_name  
where:
```

- *server_name* is the name of the NetWorker server.
- *client_name* is the name of NMM client.

Recovering deduplicated data

About this task

The process for recovering data from a Data Domain deduplication system is basically the same as that for recovering from a traditional storage node. The backed-up data from a client is stored in a deduplicated state on the Data Domain device. Both the storage node and the Data Domain system must be online during the recovery of deduplicated data.

The same process applies for recovering data that was backed up using the client IO feature.

CHAPTER 7

Multihomed Setup for Backups and Recoveries

This chapter includes the following sections:

- [Overview of a multihomed environment](#)..... 66
- [Requirements for a multihomed environment](#)..... 67
- [Configuring a multihomed client resource](#).....70
- [Validating configuration of a multihomed environment](#)..... 72

Overview of a multihomed environment

NMM supports backup environments where there are separate networks for regular traffic and backup traffic. This chapter describes multihomed environment configuration requirements and instructions.

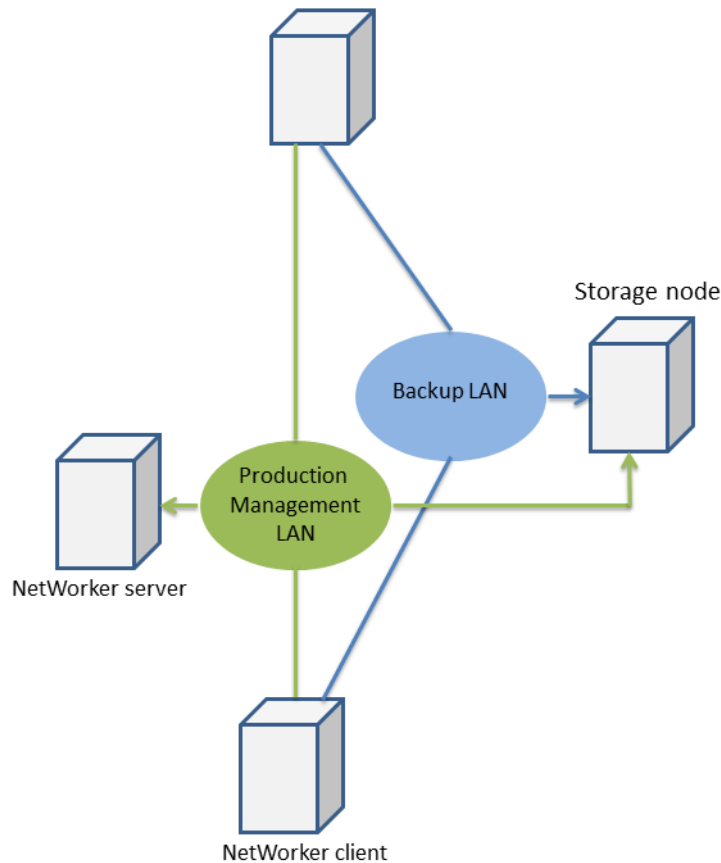
Note: Additional configuration steps may be required to complete the configuration of a client resource. Refer to the appropriate NMM user guide for the Microsoft application you are using for instructions on configuring a client resource for scheduled backup and recovery.

In a multihomed environment, NMM supports backup and recovery operations for the following Microsoft applications:

- Using VSS technology:
 - Exchange Server
 - Hyper-V Server
 - SharePoint Server
 - SQL Server
- Using VDI technology:
 - SQL Server

Sample network topology of multihomed environment for backup

You can set up a multihomed environment in several ways. The following figure demonstrates one way that you can set up a NetWorker multihomed environment for backup. In this example, the NetWorker server authenticates the client through the production network, but uses the backup LAN for the data transfer.

Figure 11 Sample network topology of NetWorker multihomed backup

For cluster virtual clients, the connection from the NetWorker server is started on the backup media production network, but the backup payload flows through the backup network.

Requirements for a multihomed environment

Before you set up a multihomed environment, you must meet the NIC and IP requirements and the network configuration requirements.

NIC and IP requirements

Ensure that the following requirements are met before you set up a multihomed environment:

- Each NIC should be configured with only one IP address.
- The IP address that belongs to any specific NIC resides in a separate subnet or VLAN. The IP subnet or VLAN through which the backup traffic is meant to pass is called the backup subnet.
- The IP resolves to one unique hostname per NIC.
- All the hosts, such as the following hosts that participate in the backup, have at least one NIC (called the backup NIC) configured with an IP address (called the backup IP) on the backup subnet:
 - NetWorker server
 - NetWorker storage node

- NetWorker client
- If you have an NMM client that is a cluster virtual server and is identified by an FQDN production domain, the NetWorker server must have access to the production subnet through another NIC.
This access is required because the NetWorker server must be able to resolve the FQDN of the cluster virtual server. In such cases, the NetWorker server needs at least two NICs: one on the backup subnet, and the other on the production subnet.
- The backup IP on any host must resolve to its FQDN on a backup LAN. This IP address to hostname mapping can be implemented in various ways:
 - By creating an entry for the backup IP on a backup domain. The backup domain offers a mechanism to identify backup IPs by name. Examples of where and how to configure a backup domain are as follows:
 - The backup domain can be a separate domain that is hosted on an exclusive DNS server on the backup subnet.
 - The backup domain zone can be configured on an existing DNS server that is accessible from the NMM client.
 - This mapping method might require customized configurations in the DNS server depending on the DNS server status, on whether the DNS server is separate, and on whether the preexisting DNS server is used for a multi-NIC configuration.
 - By updating the `%SystemRoot%\system32\drivers\etc\hosts` file with the IP to FQDN mapping on the NMM client host.

Network configuration requirements for the NMM client

Ensure that the following requirements are met before you configure the NetWorker client's network in a multihomed environment:


- The bind order of network interfaces must be as follows:
 - Production NIC
 - Private NIC, if any, in the case of a Windows cluster
 - Backup NIC

If required, complete the following steps to modify the bind order:

1. Click **Start > Settings > Control Panel > Network Connections**.
2. In the **Network Connections** dialog box, select **Advanced > Advanced Settings**.
3. Reset the order of the connections.

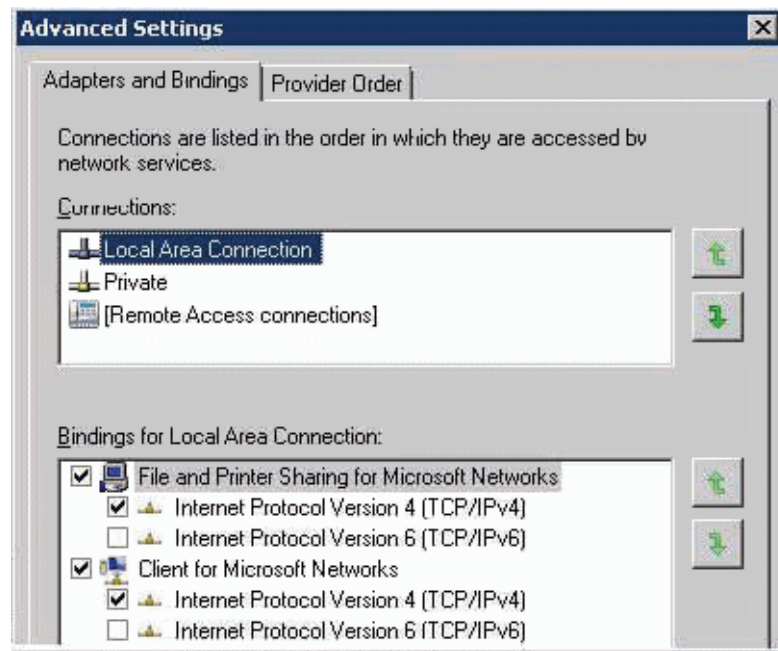
- For each NIC, set the following items:
 - DNS server address as the only corresponding DNS server IP address.
Each NIC should have one entry that is the same as the DNS server IP of the domain where this backup IP has an entry.

For example, if the DNS server of backup-domain.com is hosted on 192.168.8.5, the backup NIC on the NMM client should have only one entry, 192.168.8.5.
 - DNS suffix for this connection as the corresponding suffix.

 **NOTICE** Do not use the Append these DNS suffixes (in order) attribute.

The following figure displays the NIC settings.

Figure 12 Advanced Settings dialog box



Complete the following steps to configure the NIC settings:

1. Click **Start > Settings > Control Panel > Network Connections**.
2. Open the **Network Connections**.
3. Update the NIC settings for the environment.
4. Click **OK**.

Network configuration requirements for NetWorker server

Ensure that the following requirements are met before you configure the NetWorker server's network in a multi-homed environment:

- As the minimum requirement, the NetWorker server must have a backup IP, which is an IP address for a NIC on the backup subnet. This backup IP resolves to a unique FQDN on the backup domain.
- If an NMM client is a cluster virtual server and is identified by an FQDN in the production domain:
 - The NetWorker server must have access to the production subnet through another NIC.
 - The NetWorker server must be able to resolve the production FQDN of cluster virtual server. In such cases, the NetWorker server needs at least two NICs, one on the backup subnet and the other on the production subnet.

Network configuration requirements for NetWorker storage node


The only requirement for a NetWorker storage node is a backup IP, which is an IP address for a NIC on the backup subnet. This backup IP resolves to a unique FQDN on the backup domain.

Configuring a multihomed client resource

About this task

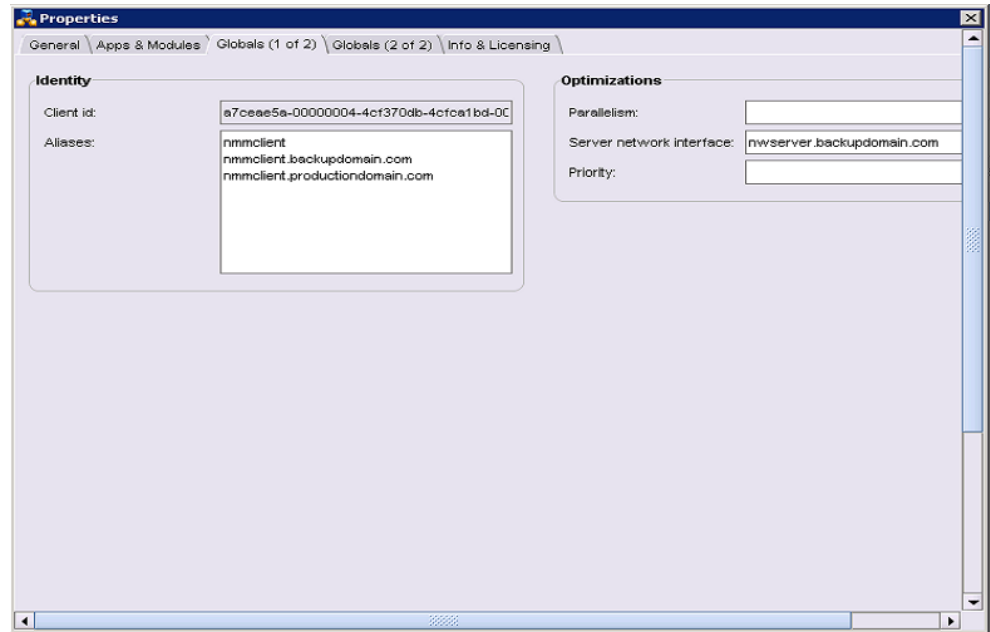
This procedure describes how to configure client resources in a multihomed environment.

Procedure

1. Open the NetWorker Administration GUI.
2. Create an NMM client resource:
 - For a stand-alone server, create an NMM client resource with the fully qualified domain name (FQDN) of the backup domain.
For example: `nmmclient.backupdomain.com`
 - For a cluster virtual server or Exchange DAG:
 - a. Create an NMM client resource for the cluster virtual server with either of the following names:
 - NetBIOS name
 - Production domain FQDN
 -  **Note:** If you are using the NetBIOS name, ensure that the **NetBIOS over TCP/IP** attribute is enabled for the production NIC on the NetWorker server.
 - b. (Optional) If you are manually configuring the cluster client resource by using the NMC Client Properties window, complete the following steps:
 - a. Create dummy clients for each of the physical nodes that are part of the SQL virtual server or Exchange DAG instance.
 - b. Update each dummy client resource to add the NMM client hostname to the **Alias** attribute on the **Globals (1 of 2)** tab in the client **Properties** window.
3. Open the client **Properties** window for the NMM client in NMC and ensure that the following settings are made:
 - a. Ensure that the NMM client has the **Server network interface** attribute set as the backup domain FQDN of the NetWorker server in the **Globals (1 of 2)** tab.

The **Client Properties** page with the **Globals (1 of 2)** tab appears, as shown in the following figure.

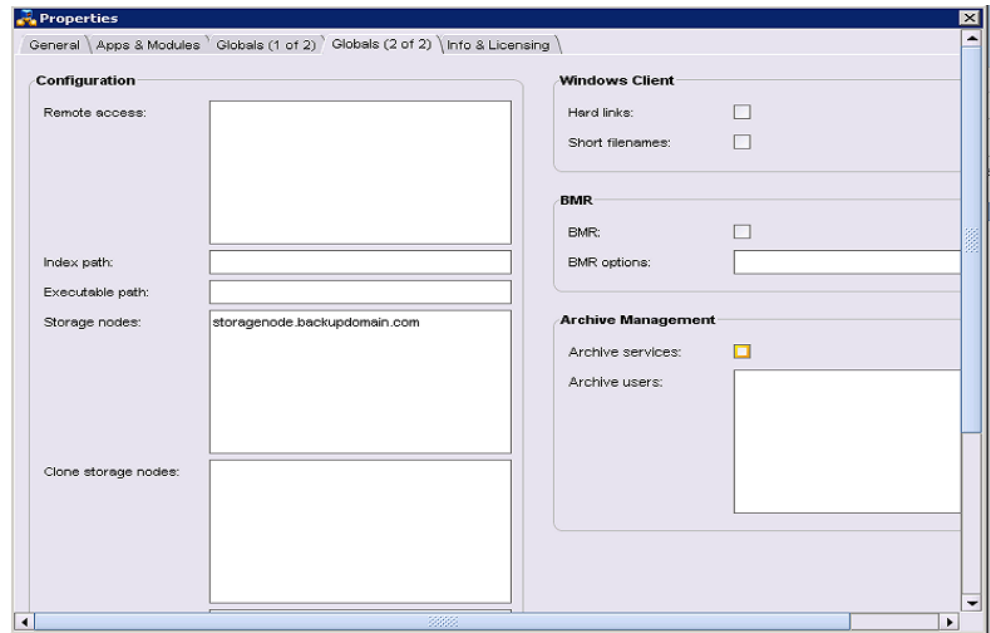
Figure 13 Globals (1 of 2) tab for multihomed client resource configuration



- b. Ensure that all NMM and dummy clients have the **Storage Nodes** attribute on the **Globals (2 of 2)** tab in the properties of the client resource set to the backup domain FQDN of the storage node that receives the client data.

The **Client Properties** page with the **Globals (2 of 2)** tab appears, as shown in the following figure.

Figure 14 Globals (2 of 2) tab for multihomed client resource configuration



Validating configuration of a multihomed environment

Perform the following configuration checks to verify that the multihomed environment is correctly configured with NMM.

- To resolve and reach the correct IP address from one host to another, you must ping for the following FQDNs corresponding to NICs participating in the backup:
 - NetWorker server
 - NetWorker storage node
 - NetWorker client

The FQDNs should resolve and reach the correct IP address from one host to another.

- Ensure that there is always a one-to-one mapping of the FQDN to an IP address in the DNS server's record for each multi-NIC FQDN. Review the DNS server records to verify that the required mapping is present.

CHAPTER 8

Active Directory Backups and Recoveries

This chapter includes the following sections:


- [Supported and unsupported Active Directory backup and recovery types and configurations](#) 74
- [Supported Active Directory objects for granular backup and recovery](#) 74
- [Improvement in NMM GUI browsing performance of Active Directory backups with large number of objects](#) 74
- [Performing Active Directory granular backups](#) 76
- [Performing an Active Directory granular recovery](#) 78
- [Recovering Active Directory backups created with NMM 8.2.x](#) 80

Supported and unsupported Active Directory backup and recovery types and configurations

Supported Active Directory backup and recovery types and configurations

NMM supports:


- Granular backups, which are performed at full and incremental levels.
- Granular recoveries, which are recoveries of individual Active Directory objects or object attributes.

 **NOTICE** To back up and recover file system, and recover system state backups, use NetWorker.

Unsupported Active Directory backup and recovery types and configurations

NMM does not support:

- Client parallelism for Active Directory. Backups proceed regardless of the parallelism that you set.
- Backup of the Active Directory Application Mode (ADAM) writer.
- Backups in an environment, in which domain migration has been performed.

 **NOTICE** It is not recommended to perform an Active Directory backup with deduplication.

Supported Active Directory objects for granular backup and recovery

NMM supports granular backup and recovery of the following Active Directory objects:

- Users
- Groups
- Organizational units
- Computer
- Contact
- InetOrgPerson
- Shared folder
- MSMQ queue alias

Improvement in NMM GUI browsing performance of Active Directory backups with large number of objects

To improve the browsing performance of Active Directory backups with large number of objects in the NMM GUI, the following enhancements are made:

About this task

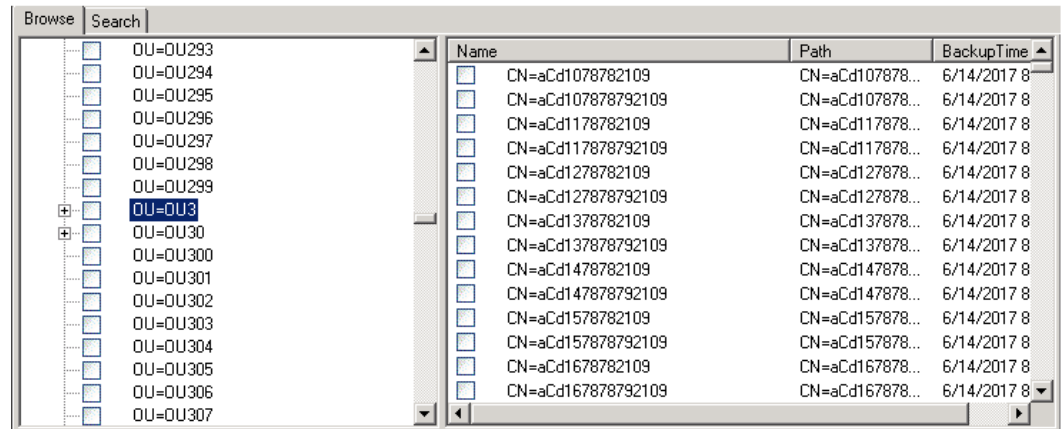
- Browse optimization in GUI: The recovery GUI browsing performance is faster by 30% to 40%.
- Search enhancement: The enhanced Active Directory search functionality called "Enable direct search" now enables you to enter the specific path of an Active Directory object and search for the specific object in a Windows Active Directory deep hierarchical environment. You can now

search directly in the backup index with the search operation starting directly from the specified path to the child object, instead of the search operation starting at root level. You can then perform restore directly from the Search Result pane without browsing the entire path. This eliminates the need to browse the paths of the objects in the NMM Recovery GUI.

Procedure

1. Start the NetWorker User for Microsoft GUI.
2. In the **Browse** tab, browse for the object under the root. The following figure displays the **Browse** page and the example root level that is selected for the object.

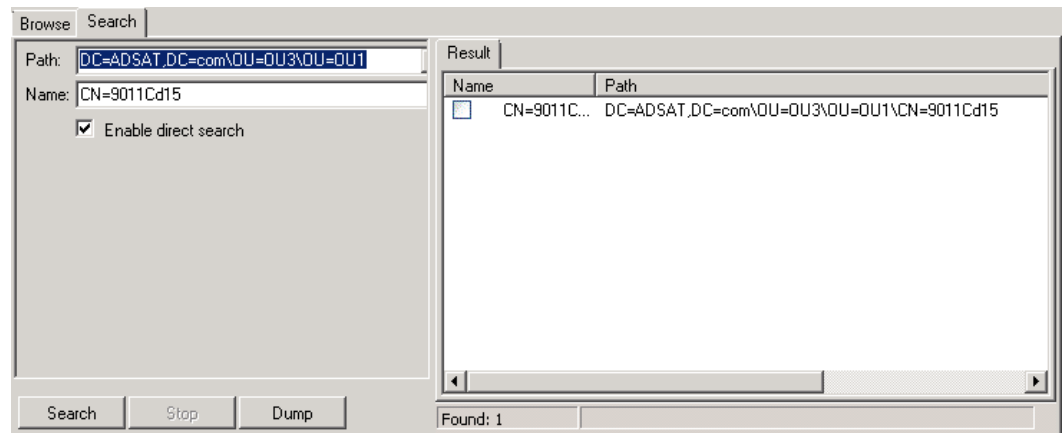
Figure 15 Browse tab



3. Select the **Search** tab.

As shown in the following figure, the root path OU=OU3 selected in the Browse tab is displayed in the **Path** field.

Figure 16 Search tab with Enable direct search option



4. Select the **Enable direct search** option.

This enables the **Path** field and you can now type the entire path of an object in the Path field.

Note: If the path of an object contains special characters, ensure to use URL encode in place of the special characters.

For example, OU=OU1 is added to the object path to specify the entire path of the object.


5. Type the name of the object on the **Name** field.
6. Click **Search** to view the relevant indexes.

7. Click **Dump** to copy the search item(s) to a text file.

Performing Active Directory granular backups

About this task

A traditional granular backup of Active Directory backup enables you to recover individual objects and object attributes. The backup is routed directly to a granular backup medium.

 **NOTICE** Perform a full-level backup after performing either of the following operations:

- Changing the properties or main attributes of an object.
- Deleting and then re-creating a security group.

Recommendations for Active Directory granular backups

Consider the following guidelines before performing an Active Directory granular backup:


- System-only attributes are not backed up with Active Directory objects. These attributes are recovered through tombstone reanimation.
- NMM 9.x and later do not support backing up Active Directory Application Mode (ADAM) writer. However, you can back up the ADAM writer by backing up the Active Directory for Bare Metal Recovery (BMR). [Backing up an Active Directory for BMR](#) on page 99 provides the information.
- Changing the system date and time to an earlier date in the domain controller is not recommended.
Each item in Active Directory is marked by a time. Active Directory uses the time to resolve any data conflicts. Recovery of a deleted object by the NMM client will fail if the date and time are changed after the object has been backed up. If a change in the system date or time is necessary, immediately perform a full backup of the domain.
- A restored user account is automatically disabled, and, for security, the pwdLastSet attribute is not recovered. A new password must be set after a user account is recovered.
- A change to an object'smemberOf attribute is reflected in the owner object of that group and not in the object itself.
For example, if a user is added to the Guests group, the Guests group object is modified, not the user object. If an incremental backup is performed, the Guests object, not the user object, is in the backup.
- Many configuration settings are stored in Active Directory, but LDAP cannot always be used to modify them. Also, some items that are stored in Active Directory are references to objects that are managed by other applications. The APIs must be used to modify the objects.

Configuring a pool for backup operations

About this task

When you use NetWorker server 19.2 with NMM 19.2, review the *NetWorker Administration Guide* for the procedures about performing the following tasks:

- Configuring a device
- Configuring a label template
- Configuring a backup pool
- Labeling the device

 **Note:** When you use NetWorker server 8.2.3 or later with NMM 19.2, review the information in the "Backup Groups and Schedules" chapter in the *NetWorker Administration Guide*.

Configuring a client resource

About this task

This procedure describes the steps to configure a client resource from the NetWorker Administration GUI.

Procedure

1. Open the NetWorker Administration GUI.
2. Click **Protection**.
3. In the expanded left pane, select **Clients**.
4. From the **File** menu, select **New**.
5. Click the **General** tab.
6. In the **Name** field, type the fully qualified hostname of the NetWorker client.
7. In the **Comment** field, type a description. If you are creating multiple client resources for the same NetWorker client host computer, use this attribute to differentiate the purpose of each resource.
8. In the **Save Set** field:
 - Specify the components to be backed up.
 - Specify domain objects in the following format:
`CN=common name,U=OU name,DC=domain name,C=suffix`
 - Example 1: When `CN=testuser1,OU=OU1,DC=corp,DC=xyz,DC=com` is used, the backup saves testuser1.
 - Example 2: When `DC=corp,DC=xyz,DC=com` is used, the backup saves the entire domain named corp.xyz.com from its root level.
9. On the **Apps & Modules** tab:
 - In the **Backup command** field, type the following command `nsradsave.exe`.
Active Directory domain objects cannot be backed up in the same client resource.
 - Clear the **Data Domain backups** option. An NMM backup of an Active Directory object fails when you select the Data Domain option in the client properties.
10. Click the **Globals (1 of 2)** tab.
11. In the **Aliases** field, ensure that the NETBIOS name for the client is present. This is automatically populated by NetWorker when name resolution is configured. If the NETBIOS name is not present, add the NETBIOS name for the client.

 The NMM client uses the host server NETBIOS, or short name, when connecting to the NetWorker server to browse backups. If the NETBIOS name is not found, NMM cannot display backups.
12. Complete the other attributes as required.
13. On the **Globals (2 of 2)** tab, leave the **Remote Access** field blank.
14. Click **OK**.

Performing an Active Directory granular recovery

You can select individual deleted Active Directory objects and their attributes for recovery.

NOTICE Microsoft recommends that you have a secondary Active Directory server that can be promoted to the primary Active Directory server if a disaster occurs.

If you do not have a secondary Active Directory server that can be promoted to the primary Active Directory server, complete the steps in this section to recover from a Active Directory server disaster.

Recovery restrictions for Active Directory

The following restrictions apply when recovering Active Directory objects and attributes:

Note: After starting an Active Directory recovery, view the Monitor page to verify the status of the recovery.

- **Tombstone lifetime restriction**—When an Active Directory object is deleted, the object is retained in a Deleted Objects container or tombstone. If you need the deleted object, you should recover the tombstone object instead of creating a new object because data, such as the Security Identifier (SID) and the Globally Unique Identifier (GUID), are stored with the tombstone object. This data is critical for additional data recoveries, such as reclaiming assigned group permissions.
For example, Access Control Lists (ACLs) use a security identifier objects SID to store the object's permissions. If you create a new group, it is assigned a new SID and GUID, so the permissions assigned to the old group are lost. If you recover the group from the tombstone object, the group retains its permissions. Similarly, the SID and GUID are both used to recover a user profile. A user's profile becomes unusable if you create a new user profile with the same name because the new profile is assigned a new SID and GUID, which makes the permissions in the original profile inaccessible.

Objects in tombstone are deleted when they reach the tombstone lifetime age for the domain. The lifetime age is 180 days for Windows. After an object is deleted from the tombstone, it cannot be recovered. This is an Active Directory restriction. The tombstone lifetime is a configurable attribute of a Windows domain. Refer to the *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/eln/elhome> for supported Windows versions.

- **System-only attributes cannot be recovered**—Object attributes that are system-only cannot be backed up or recovered. This is an Active Directory restriction.
The following table provides a sample of system-only attributes that are not backed up.

Table 16 System-only attributes that are not backed up

badPwdCount	lastLogon	uSNChanged
badPasswordTime	logonCount	uSNCreated
distinguishedName	objectCategory	userAccountControl
dSCorePropagationData	objectClass	whenChanged
instanceType	objectGUID	whenCreated
lastLogoff	sAMAccountType	

- Attributes that are retained for a deleted object—The following table provides a sample of attributes that are retained for an Active Directory object when it is deleted and moved to the tombstone database.

Table 17 Attributes retained after object is deleted

attributeID	mSMQOwnerID	subClassOf
attributeSyntax	name	systemFlags
distinguishedName	nCName	trustAttributes
dNReferenceUpdate	objectClass	trustDirection
flatName	objectGUID	trustPartner
governsID	objectSid	trustType
groupType	oMSyntax	userAccountControl
instanceType	proxiedObjectName	uSNChanged
IDAPDisplayName	replPropertyMetaData	uSNCreated
legacyExchangeDN	sAMAccountName	whenCreated
mS-DS-CreatorSID	securityIdentifier	

These attributes are restored when deleted objects from the tombstone database are restored. Objects that do not retain all their mandatory attributes cause a constraint violation error during a restore operation.

For example, a published shared printer has mandatory attributes (printerName, serverName, shortServerName, uNCName, and versionNumber), which are not retained in the tombstone database.

- Object password attributes—An object's password cannot be recovered. After recovering an object with a password attribute, the Windows administrator must reset the password.
- Moved or renamed objects—If objects are moved or renamed, but not deleted from Active Directory, those objects cannot be restored even if they are successfully backed up. Those objects are not stored in the deleted storage database (tombstone) so they cannot be restored.
However, the attributes for these objects can be restored from the Context menu of the Active Directory interface, which restores the objects with the specific attribute sets.
- Attributes with null values—Attributes with null values are not backed up and therefore are not recovered. For example, if the attribute Phone Number is empty (null), the null Phone Number attribute is not backed up.
This is an Active Directory restriction and is intended to prevent the unintentional overwriting of valid attribute values.
For example, if a Phone Number attribute is null when a snapshot is taken, but later a valid phone number is added, subsequent recovery operations will not overwrite the valid phone number with a null value.
- Schema objects—Schema objects cannot be recovered so they cannot be backed up. They should never be deleted.

Recovering an Active Directory object or object attribute

About this task

The following procedure describes how to recover an Active Directory object or object attribute.

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. On the application toolbar, click the **NetWorker Server** icon to select the NetWorker server on which the NetWorker client was configured for backup.
3. In the left pane, select **Recover > Active Directory Recover Session**.
4. In the navigation tree, select the Active Directory objects to be recovered. By default, the objects that are displayed in the navigation tree are from the most recent backup:
 - To search for an item, click the **Search** tab.
 - To recover objects from a previous backup:
 From the application toolbar, click the **Browse Calendar** icon and select an earlier browse time.
 To view all versions of a backup object before the selected browse time, select an object in the navigation tree, right-click, and select **Versions**.
5. To determine whether any volumes must be mounted for a selected object, right-click an object and select **Required Volumes**.
6. Recover the entire object or selected object attributes:
 - To recover the entire object:
 - a. Select the object.
 - b. From the Active Directory Recover Session toolbar, click **Start Recover** to begin the recovery operation.
 An entire object can be restored if it is deleted. The attributes are restored to an existing object.
 - To recover the selected attributes of an object:
 - a. Right-click an object and select **Restore Item Attributes**.
 The **Active Directory Recover Attributes** dialog box appears.
 - b. Select each attribute to be recovered.
 - c. Click **OK**.
7. Click **Start Recovery**.
8. From the left pane, select **Monitor** to view the progress of the recovery.

Recovering Active Directory backups created with NMM 8.2.x

About this task

NMM 9.0 and later are compatible with the following NetWorker versions for Active Directory backup and recovery that were created with NMM 8.2.x:

- Backup and restore with NetWorker server 9.0 or later, NetWorker client 8.2, and NMM 8.2.
- Backup and restore with NetWorker server 9.0 or later, NetWorker client 8.2.x, and NMM 8.2.x.

Procedure

1. Back up the data with NetWorker server 8.2 or 8.2.x, NetWorker client 8.2 or 8.2.x, and NMM 8.2 or 8.2.x.
2. Upgrade the NetWorker server from 8.2 or 8.2.x to 9.0 or later, the NetWorker client from 8.2 or 8.2.x to 9.0 or later, and NMM from 8.2 or 8.2.x to 9.0 or later.

3. Data that is backed up with NMM 8.2 or 8.2.x is browsable in NMM 9.0 or later. To perform restore browse the data.
4. Restore the data through the NetWorker User for Microsoft 19.2 GUI.

CHAPTER 9

Cloning Backups and Recoveries

This chapter includes the following sections:

• Overview	84
• Cloning with NMM	84
• Concurrent cloning	85
• Recovering cloned data with NMM	86
• Restriction on cloning BBB incremental backups that reside on AFTD or CloudBoost	93

Overview

A clone action creates a copy of one or more save sets. Cloning allows for secure offsite storage, transfer of data from one location to another, and verification of backups. You can configure a clone action to occur after a backup in a single workflow. You can also use save set and query groups to define a specific list of save sets to clone in a separate workflow.

You can perform manual, scripted cloning using the `nsrclone` command or set up scheduled cloning by configuring data protection policies.

The simplification process has changed the NMM 9.0 cloning procedure from previous releases. The "NMM architecture" section provides details about NMM 9.0.1 and later.

If you use NetWorker server 19.2 with NetWorker client and NMM 19.2, review the information in the "Data Protection Policies" chapter and the "Backup Data Management" chapter in the *NetWorker Administration Guide* to supplement the information in this chapter.

- The Data Protection Policies chapter describes how you can schedule cloning by configuring data protection policies.
- The Backup Data Management chapter describes how you can clone save sets manually by using the `nsrclone` command.

If you use NetWorker server 8.2.3 with NetWorker client and NMM 19.2, review the information in the "Backup Groups and Schedules" chapter and "Cloning" chapter in the *NetWorker Administration Guide* to supplement the information in this chapter.

Review the following BBB restrictions for cloning and staging:

- Cloning is not supported for BBB incremental backup to an AFTD target.
- Only cloning of BBB full to AFTD is supported.
- NMM lacks save set consolidation. You may clone only every 38 backups, or you must perform full backups based on your cloning needs.
- Staging is not supported for BBB backups.

Note: The **Delete source save sets after clone completes** option, which instructs NetWorker to remove the source save set information from the client file index and mark the save set as recyclable in the media database during a Server expiration maintenance action, is not supported by Exchange Server and Hyper-V Server BBB backups.

Cloning with NMM

When performing manual, scripted cloning, run the `mminfo` command to list the save sets. In the listed save sets, select the ones that have the same Generation ID in attributes and clone all save sets together. These save sets must be part of a single backup.

When performing scheduled cloning, ensure that all the save sets are selected in the GUI. Run the `mminfo` command to verify that all the save sets have been selected.

Note: Cloning Exchange Server and Hyper-V Server BBB incremental backups to an AFTD device is not supported.

The following table lists the save sets that are available for cloning Microsoft applications. When you clone, include the parent and the child save sets.

Table 18 Parent and the child save sets

Application	Component	Child save sets	Parent save sets
Exchange	Database	APPLICATIONS:\Microsoft Exchange\db1\\DatabaseFiles	APPLICATIONS:\Microsoft Exchange\db1
	Logs	APPLICATIONS:\Microsoft Exchange\db1\LogFiles	
Hyper-V	VHD1(x)	APPLICATIONS:\Microsoft Hyper-V \VM1\Parent_GUID_VHD1	APPLICATIONS:\Microsoft Hyper-V \VM1
	VHD2(x)	APPLICATIONS:\Microsoft Hyper-V \VM1\Parent_GUID_VHD2	
	Config files	APPLICATIONS:\Microsoft Hyper-V \VM1\ConfigFiles	
SharePoint	Component	APPLICATIONS:\Microsoft Office Search\<SP primary node hostname> \IndexComponentGroup_8e49f4d4-b0bf-46fb-adcc-8556f4f7c56a	APPLICATIONS:\Microsoft Office SharePoint Services
SQL VSS	Database	APPLICATIONS:\SqlServerWriter\"<SQL hostname>%5C<SQL instance name> \db1\DatabaseFiles	APPLICATIONS:\SqlServerWriter\"<SQL hostname>%5C<SQL instance name>\db1
	Logs	APPLICATIONS:\Microsoft SQL Server \db1\LogFiles	
SQL VDI	Database	Databasel.mdf	MSSQL:Databasel
	Logs	Databasel.ldf	

Concurrent cloning

NMM supports concurrent cloning. When concurrent cloning is configured, the clone action runs in parallel with backup sessions. The clone job does not wait for the backup action to complete, but starts when the backup process starts. As the save session writes a save set to backup device, data gets written to the clone device.

To enable concurrent cloning, in the **Policy Action Wizard**, on the **Specify the Action Information** page, select the **Concurrent** option. The following figure shows an example.

Figure 17 Enable concurrent cloning in the Policy Action Wizard

Policy Action Wizard

Specify the Action Information

Specify information about the action and define the schedule for the action operation. Select an action type, and if applicable the select action sub-type. To associate this action with a different workflow in the p select the workflow from the Workflow drop down. If the new action should occur after another action that is associated with the policy, select an existing action from the Previous drop-down. To start the new action at the same time as the action defined in the Previous attribute, select Concurrent.

Identity

Name: clone

Comment:

Enabled: ☒

Action Type: clone

Workflow

Policy: policy579

Workflow: w579

Previous: backup

Concurrent: ☒

Period

☒ Weekly by day (For example Sunday, Friday, etc.)

☐ Monthly by day (For example 1st day, 5th day etc.)

Click on the day to schedule the action

Make All Execute

Sun	Mon	Tue	Wed	Thu	Fri	Sa
⚡	⚡	⚡	⚡	⚡	⚡	⚡

Recovering cloned data with NMM

This section provides the steps necessary to recover a save set that is in a recoverable state.

Identifying the required save time range

Run the `mminfo` command to identify the required save time range for the backup version that is being restored by querying the media database.

The save time range is the day before (date1) and the day after (date2) the date of the backup that is to be restored.

Recovering NMM data from recoverable or recycling save sets

To determine the status of a save set in the media database, use the `mminfo` command. The `ssflags` attribute provides a status summary for each save set.

When you generate the `ssflags` save sets summary report:

- An **R** in the `ssflags` output denotes that a save set is recoverable and has exceeded its defined browse policy.
- An **E** in the `ssflags` output denotes a save set that is eligible for recycling and has exceeded its defined retention policy. This is also referred to as an expired save set.

In the case of incremental or differential save sets, the `ssflags` value contains an **E** only when all dependent incremental, differential, or full backups have exceeded their defined retention policy periods. When all save sets on a volume are eligible for recycling, the volume can be overwritten.

Generating the media database list of the save sets

This section outlines the steps that are required to identify all the necessary save sets for a recover operation of a recoverable original backup or clone.

Procedure

1. From the command prompt on the NetWorker server, type the `mminfo` command to generate a list of NMM original or cloned save sets in the media database:

```
mminfo -S -s NetWorker_server_name -c NMM_client_name -
q "group=group_name, savetime>=date1, savetime<=date2 -ot 1>output.txt
2>&1
```

where:

- *NetWorker_server_name* is the name of the NetWorker server host.
 - *NMM_client_name* is the name of the NMM client host.
 - *group_name* is the name of the group that contained the NMM client when the backup occurred.
 - *date1* is at least one day before the date range of either the NMM original or clone that is to be restored.
 - *date2* is at least one day after the date range of either the NMM original or clone that is to be restored.
2. Edit the `output.txt` file, which resides in the same directory from which the `mminfo` command is run.
 3. If the output file contains the following message, the media database does not contain NMM save sets for the specified client or query options:

```
mminfo: no matches found for the query
```

Make adjustments to the query options that you specify in the `mminfo` command. If the query results are missing save sets, see the [Save set media database](#) on page 90 section for information on locating and adding save sets to the media database.

Recovering recoverable save sets to the client file index

If the backup save sets are recoverable, they can be made browsable for the length of time that is required to perform the recovery operation. For example: `sflags=vrF`


Procedure

1. For each save set in the `output.txt` file, type the following command:

```
nsrmm -s NetWorker_servername -e time1 -S ssid
```

where:

- *NetWorker_servername* is the name of the NetWorker server.
- *time1* is the new retention time.
- *ssid* is the save set value that is recorded for each metadata or rollover save set.


 **Note:** Ensure that the new browse and retention dates for the save sets are far enough in the future that the recovery has time to complete.

2. Repopulate the client file index on the NetWorker server with the save set information:

```
nsrck -L 7 -t date client 1>nsrck.txt 2>&1
```

where:

- *date* is a date after the completion of the latest save set that to be restored.
- *client* is the name of the NMM client.

 **Note:** Ensure that the volume that contains the index backup is available for mounting.

3. Review the output in `nsrck.txt` for errors after the command has completed.

For example:

- If any of the following errors are reported:

- 19779:nsrck: Please run ``nsrck clientname''
- 9348:nsrck: The index recovery for ' clientname ' failed.
- 39078:nsrck: SYSTEM error: The operation completed successfully.

Type the following command:

```
nsrck -L2client
```


where *client* is the name of the NMM client.

- Ignore file attribute messages such as the following; they do not impact the NMM recovery:
32222:uasm: Warning: Some file attributes were not recovered:
C:\Program Files\EMC NetWorker\nsr\index\clientname\db6\tmprecov
\C\Program Files\ EMC NetWorker \nsr\index\clientname\db6\
- If the `nsrck` command fails with the error `xxxxx`, the index backup might no longer be referenced in the media database. Use the following command to scan all ssids recorded for the save sets:

```
scanner -i -S ssid device
```

where:

- *ssid* is the save set ID of the save set that is to be restored.
- *device* is the device containing the volume for the save set that is to be restored.


 **Note:** Ensure that the NMM software is closed on the NMM clients before you run the scanner command. If the software is open while the scanner runs, the scanner command might fail with 'Index error, flush Failed'.

- If browse and retention times that the scanner sets are not long enough for recovery procedures to complete, for each save set, modify the browse times of the existing save sets:

```
nsrmm -s NetWorker_servername -w time2 -S ssid
```

where:

- *NetWorker_servername* is the name of the NetWorker server.
- *time2* is the new browse time.
- *ssid* is the save set value that is recorded for each save set, described in [Generating the media database list of the save sets](#) on page 87.

 **Note:** Ensure that the new browse dates for the save sets are far enough in the future that the recovery has time to complete.

- Open the NetWorker User for Microsoft GUI and start the recovery. [Performing recovery](#) on page 92 provides steps for recovery.

Recovering recyclable save sets to the client file index

Procedure

1. Reset the browse and retention times for all the save sets that were recorded as a result of the following the steps in the "Generating the media database list of the save sets" section, by typing the following command:

```
nsrmm -e time1 -S ssid
```

where:

- *time1* is the required retention time.
- *ssid* is the save set value that is recorded for each save set.

2. Type the following command for each save set in the output file:

```
nsrmm -o notrecyclable -S ssid/cloneid
```

3. Repopulate the client file index with the save set information by typing the following commands:

```
nsrck -L 7 -t MM/DD/YYYY client_name 1>nsrck.txt 2>&1
```

where:

- *MM/DD/YYYY* is a date after the completion of the latest save set that is restored.
- *client_name* is the name of the NMM client.

4. Review the output in the *nsrck.txt* file for errors after the command has completed.

For example:

- If the following messages are reported:

Messages:

```
19779:nsrck: Please run ``nsrck clientname``
```

```
9348:nsrck: The index recovery for ' clientname ' failed.
```

```
39078:nsrck: SYSTEM error: The operation completed successfully.
```

Type the following command:

```
nsrck -L2 client_name
```

where *client_name* is the name of the NMM client.

- Ignore file attribute messages such as the following; they do not impact the NMM recovery and can be safely ignored:

```
32222:uasm: Warning: Some file attributes were not recovered:
```

```
C:\Program Files\EMC NetWorker\nsr\index\clientname\db6\tmprecov  
C:\Program Files\EMC NetWorker\nsr\index\clientname\db6\
```

- If the *nsrck* command fails with the error *xxxxx*, the index backup might no longer be referenced in the media database. Use the following command to scan all *ssids* that are recorded for the save sets in the output file:

```
scanner -i -S ssid device
```

where:

- *ssid* is the save set ID of the save set that is to be restored.
- *device* is the device that contains the volume for the save set that is to be restored.

Note: Ensure that the NMM software is closed on the NMM clients before you run the scanner command. If the NMM software is open while the scanner runs, the scanner command might fail with the following error:

```
Index error, flush Failed
```

5. If browse and retention times that the scanner sets are not a long enough for recovery procedures to complete, for each save set, modify the browse times for the existing save set:

```
nssrmm -s NetWorker_server_name -w time2 -S ssid
```

where:

- *NetWorker_server_name* is the name of the NetWorker server.
- *time2* is the new browse time.
- *ssid* is the save set value that is recorded for each save set, described in the topic [Generating the media database list of the save sets](#) on page 87.

Note: Ensure that the new browse dates for the save sets are far enough in the future that the recovery has time to complete.

Save set media database

This section discusses recovering a save set that is not in the media database.

Determining the clone save sets that do not exist in the media database

If the NMM original or clone save sets that are required for a recovery operation are no longer in the media database, you must scan the original or clone volumes to regenerate the media and index database for these save sets. You can use the `scanner` command to scan the volumes.

Identifying volumes required for scanning

In the following scenarios, the scanning procedure can identify the required volumes for the backup that is being restored.

- Restoring from a full backup. The volumes from the date of the backup are required.
- Restoring from an incremental backup. The volumes from the day of the completed incremental backup to the most recent full backup are required.
- If other volumes must be scanned, review the following procedures to identify what save sets are missing, so the additional volumes can be retrieved.

Disabling idle device timeout

To prevent devices from being unloaded from the drives while the scanner is in use, you must temporarily disable the **Idle Device Timeout** attribute.

Procedure

1. Connect to the NetWorker server through the NMC.
2. Click the **Devices** button.
3. Click **View**, and then select **Diagnostic mode**.
4. Right-click the device that will scan the required volume.
5. Select **Properties** to modify the properties of the device.
6. Select the **Advanced** tab.

7. Set the **Idle Device Timeout** value to 0.
8. Click **OK**.

Scanning the required volume

Procedure

1. Mount the volume that contains the clone save sets onto the drive.
2. If the volume is no longer in the NetWorker media database, choose the option **Load without mount while loading the tape**.
3. From the command prompt on the NetWorker server, obtain a list of the save sets on the clone volume to generate a report of the save sets on the volume. Type the following command:

```
scanner -S ssid -i name of clone device
```

4. Open the `scanner_output.txt` file, which resides in the same directory from which the `scanner` command was run. If the `scanner_output.txt` file contains the following message:

```
scanner: SYSTEM error: Cannot start device_name: No such file or directory
```

Check the device name that is specified in the `scanner` command for errors and retry the `scanner` command with the correct device name.

Determining ssid of the required save sets

Procedure

1. Inspect the `scanner_output.txt` file to determine the ssids of the required save sets. The save sets can be identified by using the following attributes values for each save set in the output file:
 - Client name
 - Save time
 - Level
 - Save set name
2. Determine the ssids and save time of all save sets that are required to perform the recovery, including all the dependent full and incremental save sets.

Note: The ssid values are used later in the procedure to scan the save sets back into the media database. The save time values validate that the repopulation of the client file index was successful.

If the date of the point-in-time recovery was an incremental or differential backup level as denoted by the value in the level column, all save sets from the point-in-time recovery to the last full must be identified. The associated full backup might be on a different volume.

Scanning required save sets into media database and client file index

Procedure

1. Type the `scanner` command to scan save sets:

```
scanner -i -S ssid device 1>scanner1.txt 2>&1  
where:
```

- *ssid* is the ssid that is recorded for the save set.
- *device* is the device with media containing the save set.

Ensure that the NetWorker User software is closed on the NMM clients before you run the `scanner` command. If the NMM software is open while the scanner runs, the `scanner` command might fail with 'Index error, flush Failed'.

2. Review the output of the `scanneri.txt` file for errors.

Validating save sets in the client file index

For each save set that was scanned in, you can use the `nsrinfo` command to validate that the data has been repopulated in the client file index.

Procedure

1. To validate that the save sets are in the client file index, run the `nsrinfo` command against each savetime to confirm that the client file index was populated with the necessary save set details:

```
nsrinfo -t exact_savetime client
```

where:


- *exact_savetime* is the savetime recorded from the scanner output.
- *client* is the name of the NMM client.

2. Type the `nsrinfo` command for all save sets.

Performing recovery

The following procedure provides the general steps for performing an NMM recovery for Exchange Server, SharePoint Server, Hyper-V Server, and SQL Server VSS. Some applications might require additional steps or settings. The application-specific user guides provide the full application-specific recovery procedures.

About this task

 **Note:** For information on recovering SQL Server VDI backups, refer to the *NetWorker Module for Microsoft for SQL VDI User Guide*.


Procedure

1. On the NMM client, start the NetWorker User for Microsoft program.
2. In the **Client** listbox, select the NMM client.
3. If the NMM client is part of a cluster, select the virtual client.
4. In the left pane, select **Recover**, and then select the appropriate application:
 - Exchange
 - Hyper-V
 - SharePoint
 - SQL Server (listed as System)
5. Click the **Calendar** icon.
6. Select the required date and time.
7. In the **Browse** window, select all the required backups.

8. To ensure that the correct full and all other associated incremental or differential backups are selected:
 - a. Right-click one of the marked items.
 - b. Select **Version**.
 - c. Click **Cancel**.

If the required backup version is not displayed, ensure that all the save sets are scanned and are in a browsable state.

9. To ensure that the correct volume is selected:
 - a. Right-click one of the marked items.
 - b. Select **Required Volumes**.

 **Note:** The **Required Volumes** dialog box correctly displays all volumes that are needed for the currently browsed backup time, but if that backup is an incremental one, volumes from dependent incrementals or the full backup may not be displayed. To obtain an accurate list of required volumes for an incremental backup, repeat this procedure for each backup of the database, including the most recent full backup.

- c. Make note of all the listed volumes.
 - d. Click **OK**.
10. Start the recovery.

Restriction on cloning BBB incremental backups that reside on AFTD or CloudBoost

NetWorker does not support cloning BBB incremental backups that reside on an AFTD or CloudBoost. This restriction does not apply to DD backup targets because all backups to Data Domain are full backups (synthetic full backup using DD virtual synthetics).

The restriction is built into the `nsrclone` command, which returns an error when an attempt to clone BBB incremental for AFTD or CloudBoost target is made.

When a data protection policy (NetWorker server 9.x) or a scheduled clone (NetWorker server 8.x) is used, the cloning action fails and the action log displays:

```
6/17/2015 9:03:44 PM NSRCLONE failed for one or more save sets.
```

The full action log for the cloning action displays more detailed information:

```
6/17/2015 9:02:30 PM Save set 3263316649 is an incremental Block Based Backup save set and will not be included for cloning.
```

For policy-based cloning of BBB scenarios, you can adjust the action filters to filter BBB incremental backups.

When configuring backups, it is best practice to set the backup level to incremental for all days.

For an AFTD target, NMM automatically promotes the backup to full for the initial backup or after 38 incremental backups. With such a best practice setting, you would get a clone of the AFTD full backup only the first time an Exchange database or Hyper-VM is backed up or every 39 backups. To create additional clones, schedule more frequent full backups. You must be aware of the impact that running full backups has on the backup window.

CHAPTER 10

Windows Bare Metal Recovery Solution

This chapter includes the following sections:

• Overview	96
• System requirements	96
• Protecting an environment before a disaster	98
• BMR by using NetWorker and NMM	99
• Backing up an Active Directory for BMR	99
• Performing BMR of an Active Directory	100

Overview

Bare-metal recovery (BMR) is a technique in the field of data recovery and restoration where the backed up data is available in a form that allows you to restore a system from bare metal, that is, without any requirements as to previously installed software or operating system.

Typically, the backed up data includes the necessary operating system, applications, and data components to rebuild or restore the backed up system to an entirely separate piece of hardware. The hardware receiving the restore should have a similar configuration as that of the hardware that was the source of the backup.

The basic BMR is the process of bringing up a server after a disaster and ensuring that the system recovers with the operating system, the applications, and the data as they were at the time of the failure.

Restoring a server to the exact configuration that it had at the time of its destruction can be a difficult task. When this restoration is performed to another hardware, it can add to the complexity of the process and can be time-consuming. Windows BMR solution provides a flexible and reliable method of restoring a server after a disaster.

System requirements

The following sections list requirements to perform Windows BMR. However, the *NetWorker E-LAB Navigator*, which is available at <https://elabnavigator.emc.com/elab/elhome>, provides the latest information about the system requirements to perform Windows BMR by using NMM.

Microsoft BMR requirements

Perform BMR recoveries to the same or similar hardware, and physical to virtual environment.

The following Microsoft KB article provides the requirements to perform a BMR to similar hardware:

<http://support.microsoft.com/kb/249694>

CPU requirements

Consider the following CPU requirements:

- The operating system architecture and the processor architecture must match.
- Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) must match.
- You can treat AMD or Intel processors as being the same if they follow the same architecture. You can recover the operating system backup of an AMD x64 computer to an Intel x64 computer. The process is reversible.
- You can restore the backup of an x86 operating system version only to an x86 processor computer.
- You can restore the backup of an x64 operating system version only to an x64 processor computer.

Hard disk requirements

Consider the following hard disk requirements:

- The disk or RAID drivers that are used in the old system must be compatible with the disk or RAID controllers in the new system.
- For each critical disk on the BMR target system, the startup hard disk capacity on the new system must be greater than or equal to the capacity on the old system. BMR fails if the capacity is smaller by even a single byte.
- Windows BMR supports IDE, SATA, or SCSI hard disks. You can perform the backup on one type of hard disk and recover on another type. For example, SAS to SATA is supported.
- You must restore the backup to the same logical disk numbers as on the original server. You cannot use different logical disk numbers on the target system to recover the critical volumes such as the operating system volume.
- Ensure that the RAID setup on the destination computer does not interfere with the disk order of the hard disks.

NIC driver requirements

To use different Network Interface Card (NIC) after a Windows BMR recovery, install new NIC drivers that match the NIC in the new computer after Windows starts on the new server.

Critical and noncritical volume requirements

Consider the following critical and noncritical volume requirements:

- Windows BMR backs up only critical volumes, and can be used for offline disaster recovery. Use the NetWorker client to back up the non-critical volumes.
 - Note:** NetWorker considers only system volume as a critical volume. If you have installed a Microsoft application on a drive other than the system drive, the drive is not considered as critical. On Windows Server 2008 R2, a volume is critical if a Microsoft application has installed a Windows service on it, but on Windows Server 2012, a volume that has a Windows application service installed is not critical.
- To make a volume critical on Windows Server 2012, set the value of the `HKLM\System\CurrentControlSet\Control\SystemWriter\ReportWin32ServicesNonSystemState` registry key to 0. This ensures that BMR includes the Microsoft application binaries, and the volume on which they are installed is marked as critical.
 - Note:** This registry key may not be in the registry by default. If it is not in the registry, create the `HKLM\System\CurrentControlSet\Control\SystemWriter\ReportWin32ServicesNonSystemState` registry key.

System Reserved Partition requirements

Ensure that System Reserved Partition (SRP) is online before you perform a BMR backup. Otherwise, the backup fails and displays the following error messages:

```
84687:save: Unable to get volume information of file system '\\?
\Volume{245204f6-5ff7-11e2-a3ac-806e6f6e6963}\': The device is not
ready. (Win32 error 0x15). VSS OTHER: ERROR: VSS failed to process
snapshot: The shadow copy provider had an unexpected error while trying
to process the specified operation. (VSS error 0x8004230f)
```

```
90108:save: Unable to save the SYSTEM STATE save sets: cannot create the
snapshot.
```

```
86024:save: Error occurred while saving disaster recovery save sets.
```

If SRP is offline, perform the following steps to bring it online:

1. In the WinPE command prompt, type `diskpart` and press **Enter**.
2. Run the following command to display the list of volumes:
`DISKPART> list volume`
3. Run the following command to select the volume that is offline:
`DISKPART> select <volume_name>`
4. Run the following command to bring the selected volume online:
`DISKPART> online volume`

Supported operating systems

The *NetWorker E-LAB Navigator*, which is available at <https://elabnavigator.emc.com/elabinhome>, provides information about the operating systems and versions that NMM supports.

Supported Microsoft applications

The *NetWorker E-LAB Navigator*, which is available at <https://elabnavigator.emc.com/elabinhome>, provides information about the Microsoft applications and versions that NMM supports.

NetWorker software version requirements

The *NetWorker E-LAB Navigator*, which is available at <https://elabnavigator.emc.com/elabinhome>, provides information about the NetWorker software versions that NMM supports.

Use the NetWorker Windows BMR 32-bit ISO image to recover an x86 operating system on either an x86 or x64 computer.

Use the NetWorker Windows BMR 64-bit ISO image to recover only an x64 operating system on an x64 computer.

Protecting an environment before a disaster

To prepare for disaster recovery, back up application data and other necessary files.

Procedure

1. Use NetWorker client to back up non-application data.
The *NetWorker Administration Guide* provides details about using the NetWorker client to backup non-application files.
2. If you use a NetWorker server earlier than 9.0.x, create a NetWorker group without enabling the Snapshot option. Otherwise, create a policy.
3. Create a NetWorker client resource, and assign it to the group that you created in step 2.
4. Configure the NetWorker client resource by typing `ALL` in the **Save set** field, and clearing the **Backup command** and **Application information** fields.
5. Perform a backup.
6. Use NMM to perform a full backup of application data.
The NMM application specific user guides provide details about how to perform a full backup.

BMR by using NetWorker and NMM

Perform Windows file system backup and recovery by using the NetWorker client, and application-specific backup and recovery by using NMM.

Note: Specific information about how to backup and recover Microsoft applications in NMM 19.2 is provided in application-specific user guides.

NetWorker disaster recovery provides an automated BMR solution by using the Windows ASR writer and other VSS writers to identify critical volumes that are required to perform a disaster recovery on a disabled system. BMR is performed offline, that is, when the Windows operating system is inactive. This avoids the necessity to manually reinstall Windows, and the problems that occur when operating system files are being restored to an active Windows system.

NMM 19.2 is compatible with the NetWorker 19.2 client, which provides a true BMR capability for Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008. This capability is built into the NetWorker client and provides BMR support to the same or similar hardware. For Windows BMR, you should download the ISO recovery boot image file from the Online Support website (<https://support.emc.com>). The ISO image provides a wizard that allows you to format disks, recover Windows critical volumes from backup, and restart the server to bring it back online.

To support a NetWorker Windows BMR recovery, download the Windows BMR image from the Online Support website (<https://support.emc.com>). This download enables you to create a bootable Windows BMR ISO that contains NetWorker binaries and a wizard, which controls the recovery process.

The "Windows Bare Metal Recovery to Physical or Virtual Computers" section in the *NetWorker Administration Guide* provides detailed information about how to use the NetWorker Windows BMR image to perform a BMR recovery on protected hosts and VMware virtual machines.

NOTICE For all the Microsoft applications, after performing Windows disaster recovery and restarting the system, check all the disk and volume configurations. Usually, the disks and volumes appear as on the original system. However, it is possible, especially in BMR scenarios, that the volume or disk signatures do not match the original ones, and the non-critical volumes or disks are offline and not mounted. Use the Microsoft Disk Manager to bring the volumes and disks online, and then restart the system for drive letter reassignments. Assign the same drive letters that existed before the BMR. Non-critical volumes that the mount points access might have a similar issue.

Backing up an Active Directory for BMR

Procedure

1. By using the NetWorker Administration GUI, create a policy, a workflow, a group, and an action for Active Directory.

The Data Protection Policies chapter in the *NetWorker Administration Guide* provides information.

2. Create a client resource for Active Directory:
 - a. In the **NetWorker Administrator** window, click **Protection**.
 - b. In the expanded left panel, right-click **Clients** and select **New**.

The **Create Client** dialog box appears.

- c. In the **Name** field, type the name for the client resource.
 - d. Click **OK**.
3. In the right panel, right-click the client resource and select **Modify Client Properties**.
4. In the **Client Properties** dialog box:
 - a. On the **General** tab:
 - In the **Group** list, select the group that you created in step 1.
 - In the **Save set** field, type **ALL**.
 - b. On the **Apps & Modules** tab, ensure that the **Backup command** and **Application information** fields are clear.
 - c. Specify other fields according to the requirements.
 - d. Click **OK**.
5. Perform the backup.

Ensure that the backup successfully completes.

Performing BMR of an Active Directory

Procedure

1. Perform the procedures that the "Performing a Windows BMR recovery to physical or virtual computers" section in the *NetWorker Administration Guide* describes.

The "Performing post-recovery tasks for Active Directory services" section in the *NetWorker Administration Guide* provides information about how to perform an authoritative recovery of Active Directory.
2. Verify whether you can successfully log in as the domain administrator.
3. Verify whether all the Active Directory objects are present in both the Active Directory Users and the Computers and Domain Name System management.

CHAPTER 11

Troubleshooting

This chapter includes the following sections:

- [NMM Configuration checker](#) 102
- [The EMCReports tool](#)..... 102
- [NMM client error messages](#)..... 102
- [Checking log files](#)..... 108
- [Other troubleshooting resources](#)..... 109

NMM Configuration checker

The following configurations can be checked:

- Application Host—These tests are related to the operating system, software components, Volume Shadow Copy Service (VSS) subsystem, and generic conditions that NMM requires.
- Microsoft Exchange Server
- Microsoft SharePoint Server
- Microsoft SQL Server
- Microsoft Hyper-V Server

You can view the Configuration checker results either as an HTML document or a plain text file. NMM saves the `results.html` report in the `\NetWorker Module for Microsoft` folder in the local temporary folder directory of the user account that is running the NMM installation wizard. NMM also saves the configuration check log file as `cfgchk_log.txt` in this same folder. The report lists the number of checks that have passed, failed, or generated warnings.

Correct the checks that have failed and review the warnings to ensure that NMM does not encounter problems during data backup and recovery.

The EMCReports tool

EMCReports is a tool that collects system wide information, like Windows event logs, systems logs, hardware configuration information, NetWorker logs, and NMM logs. The tool generates a zip file of all the collected information. You can send the zip file to the Support team for troubleshooting.

To download the EMCReports tool:

1. Open a browser and navigate to the EMC Online Support website (<https://support.emc.com>).
2. Under **Tools & Sites**, select **EMC Reports for Windows**.
3. Download the version of EMCReports applicable to your operating system.

The *NetWorker Administration Guide* provides more information about the EMCReports tool.

NMM client error messages

Error messages help to identify the product component that is not functioning correctly.

General NMM client error messages

The following list describes the error messages that might occur on any NMM client.

Savegroup failed in scheduled backup

Problem

A notification appears on the **Monitor** page that a savegroup failed.

Solution

Check the savegroup details for the failed save set. The savegroup details provide an exact cause or a general error, which can indicate a client or server side issue. The *NetWorker Administration Guide* provides information about viewing group backup details. If the savegroup details do not provide enough information, check the NMM client log and the other client logs.

VSS_E_WRITERERROR_RETRYABLE error code 0x800423f3

Problem

This error occurs if a savegroup is rerun after it was stopped during a replication, which did not complete.

Solution

1. Stop and restart the Microsoft VSS service.
2. Restart the Exchange Information store if it was running and was backed up.

VSS CLIENT... Invalid Writer Selection... for APPLICATIONS

Problem

This error message might appear for one of the following reasons:

- There is a typographical error in writing the save set.
- Exchange Server services are not up.
- SQL Server databases are offline.

Solution

Perform the appropriate tasks:

- Retype the save set correctly, or use the `nsrnmmsv` command to view all the valid save sets for an application.
- If you use Exchange Server:
 - Start the Exchange services.
 - If Exchange services were already started, dismount and mount the databases, and then start the savegroup.
- If you use SQL Server applications, bring the databases online.

VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED

Problem

You can create no more than 64 shadow copies per volume. Because of this limitation, the `VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED` error occurs when you try to create the 65th volume shadow copy. When the storage limit is reached, older versions of the shadow copies are deleted and cannot be restored.

Solution

Ensure that the number of persistent shadow copies does not exceed 64 per volume.

Microsoft Exchange client error messages

The following list describes error messages that might occur for Microsoft Exchange Server clients.

NMM Exchange2010 Shell Exception State of runspace is not valid for this operation

Problem

This message appears if a recovery database (RDB) is not mounted when NMM performs an RDB restore of a database with many transaction logs. The following error messages appear in the client host Event Viewer:

Exchange Search Indexer failed to enable the Mailbox Database RDB3 (GUID = d8378f25-b070-40e8-ada3-bf88b23a0c7d) after 1 tries. The

```
last failure was: MapiExceptionMdbOffline: Unable to get CI
watermark (hr=0x80004005, ec=1142)
Diagnostic context:
Lid: 1494 ---- Remote Context Beg ----
Lid: 44215
Lid: 60049 StoreEc: 0x8004010F
Lid: 49469
Lid: 65341 StoreEc: 0x8004010F
Lid: 56125
Lid: 47933 StoreEc: 0x8004010F
Lid: 32829
Lid: 49213 StoreEc: 0x8004010F
Lid: 48573
Lid: 64957 StoreEc: 0x8004010F
Lid: 9518 StoreEc: 0x476
Lid: 1750 ---- Remote Context End ----
Lid: 8434 StoreEc: 0x476
Lid: 13362 StoreEc: 0x476. It will retry after 10 minutes.
```

Solution

Perform the following workaround to ensure that the RDB is mounted:

1. Restart the Microsoft Exchange Information Store service.
2. Use the NMM and Exchange Management Shell to mount the RDB.
3. Close the NetWorker User for Microsoft GUI.
4. Restart the NetWorker User for Microsoft GUI.
5. Browse the RDB browsing to ensure that the RDB is mounted.

Insufficient permission to access mailbox. See documentation for required permission settings. Server MBX is not capable of RSG operations

Problem

This error message appears if Recovery Storage Group (RSG) browsing permissions are not provided when NMM recovers a storage group to an RSG that was previously created.

Solution

Complete the required steps before you start the RSG recovery. Perform the same steps on both nodes of a cluster in a cluster continuous replication (CCR) or a single copy cluster (SCC) cluster environment.

1. Install MAPI Collaboration Data Objects.
2. Provide RSG browsing permissions. This step ensures that the error message does not appear, and the recovery is successful.

For example, run the following PowerShell command with appropriate arguments:

```
get-mailboxserver Exchange_Server_name | Add-AdPermission -user username
-accessrights ExtendedRight -extendedrights Send-As, Receive-As, ms-Exch-
Store-Admin
```

3. Set the registry to disable IPv6.
4. Complete the following steps to fix RSG browsing issues in the registry:
 - a. Open the registry and go to HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters.

- b. Edit or create the 32-bit DWORD value `DisabledComponents`, and specify the value `FFFFFFFF`. The public folder must be present on the Exchange Server for RSG browsing to succeed.

77108: nsrnmmsv

Problem

The following error message appears when you perform a passive node backup with only a single passive node client configured for Exchange deduplication backups in a CCR setup:

```
77108:nsrnmmsv:NMM .. Operation unit failed with error 'Traditional
save returned error. saverc :-Possible cause: 1)Unsupported file
system or 2)write-protected disc or 3)No space on disc
```

```
NMM .. Error backing up one or more of the file system savesets:
NMM .. Operation unit failed with error Traditional save returned
error. saverc :-1.
```

Solution

Complete the required steps whenever you perform a passive node backup for Exchange deduplication backups in a CCR setup.

1. Configure a virtual client in the same savegroup where the passive node is configured.
2. Ensure that you do not schedule this virtual client for a backup in the same group.
3. Enable deduplication settings for this virtual client. Although the client exists in the same savegroup, it will not be part of the backup operation.
4. Ensure that a backup device is configured correctly for the client.

Error starting Restore

Problem

In Exchange 2010 DAG, remote recovery to another DAG node might fail with an `Error starting Restore` error message due to either of the following reasons:

- The firewall is enabled on the remote node.
- The name resolution is not configured correctly.

Solution

Perform both of the following tasks to resolve the error:

- Disable the firewall on the remote node.
- Configure both forward and reverse lookup zones correctly, and ensure that name resolution works correctly for all DAG nodes.

Microsoft SharePoint Server client error messages

The following list describes error messages that might occur on Microsoft SharePoint Server clients.

88461: nsrnmrc: SharePointMgmt.cpp(431): Caught unexpected exception while retrieving SharePoint Server 2010 backup components details

Problem

An unexpected exception occurs when NMM retrieves details of SharePoint Server 2010 backup components. This problem is expected during a full SQL Server is restored when the server services are down and NMM Performs some queries are performed to retrieve data.

Solution

Ignore the error message because the recovery is successful.

The system cannot find the file specified. Dismounting the SP GLR backup CBFS error in cbfs_open_file()...

Problem

Error messages might appear in the NWFS log file and the **Monitor** window during NWFS unmount or shutdown operations at the end of GLR activities. These error messages could include the following text:

```
The system cannot find the file specified.
Dismounting the SP GLR backup CBFS error in cbfs_open_file()
nwfs_cbfs_event_handlers::cbfs_close_file(): CBFS exception
```

Solution

Ignore these messages.

Format string save set name %S is valid cannot be rendered correctly. 63778: nsrnmmsv: NMM .. ERROR NMM .. ERROR.. Writer

Problem

Intermittent backup failure is seen on the farm node where search services are hosted. Backup fails and the following error message appears:

```
Format string save set name %S is valid cannot be rendered correctly
63778: nsrnmmsv:NMM .. ERROR..Writer SharePoint Services Writer with
local dependent writer id { comp ContentIndex_SPSearch cannot be
found. CONTINUE PROCESSING.
```

This error is generally expected when search services or dependent services are not running. However, it is sometimes seen when all dependent services and search services are running.

Solution

Restart the search services to ensure a successful backup.

Microsoft SQL Server client error messages

The following list describes error messages that might occur on Microsoft SQL Server clients.

Point-in-time can only be changed for a transaction log backup, unless...

Problem

During a SQL VDI recovery, if a user selects a point-in-time but no transaction log backup or incremental backup is available after a full backup, the following message appears:

The point-in-time for a restore can only be changed for logs only backup. Unless the last backup time is specifically selected by the user, the active log backup option is set by default.

Solution

This message means that unless the restore is selected with the active log backup option, a point-in-time can be changed only for a transaction log backup. Click **OK** and make the required changes.

D:\views\nw\ntx64\fb_nmm24\nsr\vssclient\snapvsssave\ nsrnmmsv.h(202)

Problem

The following message appears in the `nsrnmmsv.raw` file and the NMM Event Viewer when NMM starts a backup for SQL Server 2012:

```
D:\views\nw\ntx64\fb_nmm24\nsr\vssclient\snapvsssave\
nsrnmmsv.h(202)
```

Solution

Ignore the error message because the backup is successful.

nsrnmmsrc: Cannot login to SQL Server SQLEXPRESS\ENGINEER...

Problem

The following messages appear in the NetWorker User for Microsoft GUI for a successful recovery when SQL services are in a stopped state:

```
nsrnmmsrc:Cannot login to SQL Server SQLEXPRESS\ENGINEER.
86397:nsrnmmsrc:Unable to connect to the SQL Server29085:
nsrnmmsrc:Microsoft SQL Server Provider error:
38006: nsrnmmsrc:Named Pipes Provider: Could not open a connection to
SQL Server [2]. .
38006: nsrnmmsrc:A network-related or instance-specific error has
occurred while establishing a connection to SQL Server. Server is
not found or not accessible. Check if instance name is correct and
if SQL Server is configured to allow remote connections. For more
information see SQL Server Books Online..
38006: nsrnmmsrc>Login timeout expired.
66212: nsrnmmsrc:Cannot login to SQL Server SQLEXPRESS\ENGINEER
```

Solution

Ignore the error messages because the recovery is successful.

Checking log files

NMM and its associated features generate many log files. These log files include errors that occur during the processes.

Check the log files in the following order:

1. NMM client log files
2. Active Directory log files
3. NetWorker server log files

Also, third-party providers generate their own logs in place of the Solutions Enabler log, `hwprov.log`. The third-party documentation provides more information.

NMM client log files

VSS client log files

For VSS-based processes, the NMM client generates the following log files:

- `Monitor.xml`
- `nsrnmra.raw`
- `nsrnmmsv.raw`
- `nsrnmmsv_<timestamp>.<process_id>.log`
- `nsrnmrc.raw`
- `nsrnmrc_<timestamp>.<process_id>.log`
- `nsrnmhypervra.raw`
- `nsrncsd.raw`
- `sharepointapi.log`
- `NWWMIclient.txt`

The VSS client log files are present in the `.. \nsr\applogs\` folder. For example, `C:\Program Files\EMC NetWorker\nsr\applogs\` folder.

The `nsrnmmsv.raw` and `nsrnmrc.raw` files are operational log files, which contain high-level and critical information about the backup and recovery operations respectively.

The `nsrnmmsv_<timestamp>.<process_id>.log` and `nsrnmrc_<timestamp>.<process_id>.log` files are debug log files, which contain detailed diagnostic information that includes operational logs. The debug log files are generated only if you specify the debug level when you perform backup and recovery operations. The amount of information that the debug log files contain depends on the debug level that you specify. High debug level generates detailed logs.

Examples of debug log files:

- `nsrnmmsv_2017_02_07.09_57_23.6288.log`
- `nsrnmrc_2017_02_07.12_17_41.6300.log`

The SharePoint search application related log files `<search application name>.xml` and `ssa_topology.xml` are available at the following location: `C:\Program Files\EMC NetWorker\nsr\tmp\TopologyMetadata\`.

Both the save and recover commands write to these files. The log files are cumulative and text is appended to them with each run. The logging level of each log file is controlled by the debug level set by the CLI attribute -D debug level.

VDI client log files

For VDI-based processes, the NMM client generates the following log files:

- nsrsqlsv.raw
- nsrnmmstv_<timestamp>.<process_id>.log
- nsrsqlrc.raw
- nsrnmmrc_<timestamp>.<process_id>.log
- xbsa.messages

The VDI client log files are present in the `.. \nsr\applogs\` folder. For example, `C:\Program Files\EMC Legato\nsr\applogs\` folder.

Active Directory log files

The Active Directory log files are named as follows:

- nsradsave.log
- nsradrecover.log

The Active Directory log files are located in the applogs folder, for example, `C:\Program Files\EMC NetWorker\nsr\applogs\`.

NetWorker server log files

The NetWorker server creates several log files, which are documented in the *NetWorker Administration Guide*.

GLR mount service log file

The `MountService_<timestamp>.log` file, which is present in the `C:\Program Files\EMC NetWorker\nsr\applogs` folder contains debug logs from the mount operation, which you perform during a GLR.

The mount service does not automatically create the `MountService_<timestamp>.log` file. To manually create this log file, perform the following steps:

1. Open the **Registry Editor** window.
2. Go to **HKEY_LOCAL_MACHINE > SOFTWARE > EMC**.
3. Create the `MOUNTSERVICE_DEBUG_LOG` key.
4. For the `MOUNTSERVICE_DEBUG_LOG` string value name, specify `MODE=FILE,LEVEL=TRACE,NATIVEDEBUGLEVEL=9` as the string value data.
5. Close the **Registry Editor** window.

Other troubleshooting resources

If the problem appears to be related to the NetWorker server, check that the NetWorker server is installed and configured correctly. Also, check the log files and error message documentation for the NetWorker server.

- *NetWorker Installation Guide*
- *NetWorker Administration Guide*
- *NetWorker Error Message Guide*

You can also go to the following resources for troubleshooting information:

- <http://support.microsoft.com>
- <http://social.technet.microsoft.com/search/en-US>

GLOSSARY

This glossary contains terms related to the NetWorker Module for Microsoft. Many of these terms are used in this manual.

A

active-passive cluster	Type of cluster configuration where the data server runs on the active physical node, and other nodes are passive nodes that maintain data updates and wait to take over if the active node fails.
administrator	Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.
Administrators group	Microsoft Windows user group whose members have the rights and privileges of users in other groups, plus the ability to create and manage the users and groups in the domain.
advanced file type device (AFTD)	Disk storage device that uses a volume manager to enable multiple concurrent backup and recovery operations and dynamically extend available disk space.
application specific module (ASM)	Program that is used in a directive to specify how a set of files or directories is to be backed up or recovered. For example, compressasm is a NetWorker directive used to compress files.
archive	Process that backs up directories or files to an archive volume to free up disk space for regular backups. Archived data is not recyclable. See groom.
archive request	NetWorker resource used to schedule and manage archiving.
archive volume	Volume used to store archive data. Archive data cannot be stored on a backup volume or a clone volume.
autochanger	See library.
auto media management	Feature that enables the storage device controlled by the NetWorker server to automatically label, mount, and overwrite a volume it considers unlabeled.

B

backup	<ol style="list-style-type: none">1. Duplicate of database or application data, or an entire computer system, stored separately from the original, which can be used to recover the original if it is lost or damaged.2. Operation that saves data to a volume for use as a backup.
backup cycle	Full or level 0 backup and all the subsequent incremental backups that are dependent on that backup.

Backup Operators group	Microsoft Windows user group whose members have the capability to log in to a domain from a workstation or a server, whose data they may back up and restore. Backup Operators can also shut down servers or workstations.
backup volume	A volume used to store backup data. NetWorker backup data cannot be stored on an archive volume or a clone volume.
BMR	Windows Bare Metal Recovery, formerly known as Disaster Recovery. For more information on BMR, refer to the Windows Bare Metal Recovery chapter in the <i>NetWorker Administration Guide</i> .
bootstrap	Save set that is essential for disaster recovery procedures. The bootstrap consists of three components that reside on the NetWorker server: the media database, the resource database, and a server index.
browse policy	NetWorker policy that specifies the period of time during which backup entries are retained in the client file index. Backups listed in the index are browsable and readily accessible for recovery.
C	
carousel	See library .
client	Host on a network, such as a computer, workstation, or application server whose data can be backed up and restored with the backup server software.
Client Direct	Feature that enables clients to deduplicate backup data and send it directly to AFTD or DD Boost storage devices, bypassing the NetWorker storage node. The storage node manages the backup devices but does not handle the backup data.
client file index	Database maintained by the NetWorker server that tracks every database object, file, or file system backed up. The NetWorker server maintains a single index file for each client computer. The tracking information is purged from the index after the browse time of each backup expires.
client-initiated backup	See manual backup .
Client resource	NetWorker server resource that identifies the save sets to be backed up on a client. The Client resource also specifies information about the backup, such as the schedule, browse policy, and retention policy for the save sets.
clone	<ol style="list-style-type: none"> 1. Duplicate copy of backed-up data, which is indexed and tracked by the NetWorker server. Single save sets or entire volumes can be cloned. 2. Type of mirror that is specific to a storage array.
clone-controlled replication (CCR)	Creation of a replica of deduplicated data copied from one DD Boost device to another, which can be scheduled by the NMC clone feature and is indexed and tracked by the NetWorker server.
clone volume	Exact duplicate of a backup or archive volume. NetWorker software can index and track four types of volumes (backup, archive, backup clone, and archive clone). Save sets of these different types may not be intermixed on one volume. Clone volumes may be used in exactly the same way as the original backup or archive volume.

cloud	Configuration of backup disks that uses Atmos.
cluster	Group of linked virtual or physical hosts, each of which is identified as a node, with shared storage that work together and represent themselves as a single host.
cluster client	A NetWorker client within a cluster; this can be either a virtual client, or a NetWorker Client resource that backs up the private data that belongs to one of the physical nodes.
cluster nodes	A group of linked virtual or physical hosts with shared storage in a cluster, which work together and represent themselves as a single host called a virtual cluster host.
Cluster VSS Writer	In a Windows Server 2012 or 2012 R2 cluster with virtual machine storage on CSV, the Cluster VSS Writer reports components for backup for virtual machines that are owned by nodes other than the proxy or local node.
command prompt	Line on a screen, also known as shell prompt, where you type software commands.
common internet file system (CIFS)	Formerly known as Server Message Block (SMB). Message format used by Microsoft DOS and Windows to share files, directories, and devices.
components metadata document	See metadata document .
connection port	Port used to perform functions through a firewall.
Console application administrator	Console server user role whose members can configure features, except security features, in the Console sever application.
Console security administrator	Console server user role whose members can add Console users and assign them to Console roles.
Console server	See NetWorker Management Console (NMC) .
control zone	Group of datazones managed by the NetWorker software.
conventional storage	Storage library attached to the NetWorker server or storage node, used to store backups or snapshot backups. Also known as secondary storage. See primary storage .
copy restore	Create a copy of a database by restoring a SQL Server 7.0 or later database backup to a new location or to a new database name. The copy restore type replaces the directed recovery operation, which existed in versions of the NetWorker Module before release 3.0.
critical volume	Any volume containing system state files or files for an installed service, including volumes mounted as NTFS directories which contain such files. The volume where a critical volume is mounted is also considered to be critical. This is required to perform an offline restore, however maybe optional for this release depending upon the difficulties of implementing this feature.
CSV Shadow Copy Provider	The VSS provider that performs the snapshot for virtual machines that are owned by nodes other than the proxy node in a Windows Server 2012 or 2012 R2 cluster with virtual machine storage on CSV.

D

database	<ol style="list-style-type: none"> 1. Collection of data arranged for ease and speed of update, search, and retrieval by computer software. 2. Instance of a database management system (DBMS), which in a simple case might be a single file containing many records, each of which contains the same set of fields.
Data Domain device	Logical storage device created on a Data Domain system, used to store deduplicated NetWorker backups. Each device appears as a folder on the Data Domain system and appears with a storage volume name in NMC. A Data Domain device is also known as a DD Boost device.
data mover (DM)	Client system or application, such as NetWorker software, that moves data during a backup, recovery, snapshot, or migration operation. See proxy host.
datazone	Group of clients, storage devices, and storage nodes that are administered by a NetWorker server.
deduplication backup	Type of backup in which redundant data blocks are identified and only unique blocks of data are stored. When the deduplicated data is restored, the data is returned to its original native format.
destination client	Computer to which database files are restored in a directed recovery.
device	<ol style="list-style-type: none"> 1. Storage folder or storage unit that can contain a backup volume. A device can be a tape device, optical drive, autochanger, or disk connected to the server or storage node. 2. General term that refers to storage hardware. 3. Access path to the physical drive, when dynamic drive sharing (DDS) is enabled.
DFS component	<ol style="list-style-type: none"> 1. A namespace for files and DFS links, called a DFS root. 2. A connection to a shared file or folder, called a DFS child node. <p>See distributed File System (DFS).</p>
directed recovery	Method that recovers data that originated on one client host and re-creates it on a different client host, known as the destination client.
directive	Instruction that directs NetWorker software to take special actions on a given set of files for a specified client during a backup or recovery operation. Directives are ignored in manual (unscheduled) backups.
disaster recovery	Restore and recovery of data and business operations in the event of hardware failure or software corruption.
distributed File System (DFS)	Microsoft Windows add-on that creates a logical directory of shared directories that span multiple hosts across a network.
drive	Hardware device through which media can be read or written to. See device.
dynamic drive sharing (DDS)	Feature that allows NetWorker software to recognize and use shared drives and when they are available.

E

event-based backup See [probe-based backup](#).

expiration date Date when a volume changes from read/write to read-only.

F

failover A means of ensuring application availability by relocating resources in the event of a hardware or software failure. Two-node failover capability allows operations to switch from one cluster node to the other. Failover capability can also be used as a resource management tool.

failover cluster Windows high-availability clusters, also known as HA clusters or failover clusters, are groups of computers that support server applications that can be reliably utilized with a minimum of down-time. They operate by harnessing redundant computers in groups or clusters that provide continued service when system components fail.

federated backup During federated backups, NMM detects the SQL Server preferred backup setting for the Availability Group and performs the backup at the preferred node.

file system

1. Software interface used to save, retrieve, and manage files on storage media by providing directory structures, data transfer methods, and file association.
2. Entire set of all files.
3. Method of storing files.

firewall Security software designed to prevent unauthorized access to or from a private network.

full backup Type of backup that backs up all data objects or files, including the transaction logs contained in databases, regardless of when they last changed. See [level](#).

G

granular recovery Granular recovery provides the ability to recover specific files in seconds from a single backup. This dramatically reduces the recovery time and the footprint of the backup on storage resources.

groom Process that removes the original files from a local disk after a successful archive operation.

group One or more client computers that are configured to perform a backup together, according to a single designated schedule or set of conditions.

H

high-availability system System of multiple computers configured as cluster nodes on a network that ensures that the application services continue despite a hardware or software failure. Each cluster node has its own IP address with private resources or disks that are available only to that computer.

host Computer on a network.

hostname Name or address of a physical or virtual host computer that is connected to a network.

I

incremental backup See [level](#).

instance A copy of SQL Server running on a computer.

Internationalization (I18N) Process of adapting software to accept input and output of data in various languages and locales.

J

Java plug-in JVM that can be used by a web browser to run Java applets.

jukebox See [library](#).

L

label Electronic header on a volume used for identification by a backup application.

legacy method Use of special-case Microsoft APIs to back up and recover operating system components, services, and applications.

level Backup configuration option that specifies how much data is saved during a scheduled or manual backup:

- A full backup backs up all data objects or files, regardless of when they last changed.
- An incremental backup backs up only data objects or files that have changed since the previous backup.

library Hardware device that contains one or more removable media drives, as well as slots for pieces of media, media access ports, and a robotic mechanism for moving pieces of media between these components. Libraries automate media loading and mounting functions during backup and recovery. The term library is synonymous with autochanger, autoloader, carousel, datawheel, jukebox, and near-line storage.

library sharing Shared access of servers and storage nodes to the individual tape drives within a library. The drives are statically assigned to hosts.

Lightweight Directory Access Protocol (LDAP) Set of protocols for accessing information directories.

local cluster client NetWorker client that is not bound to a physical machine, but is instead managed by a cluster manager. It is also referred to as a logical or virtual client.

localization (L10N) Translation and adaptation of software for the user language, time formats, and other conventions of a specific locale.

M

manual backup	Backup that a user performs from the client, also known as an unscheduled, on-demand, or ad hoc backup.
media	Physical storage, such as a disk file system or magnetic tape, to which backup data is written. See volume .
media index	Database that contains indexed entries of storage volume location and the life cycle status of all data and volumes managed by the NetWorker server. Also known as media database.
media pool	See pool .
metadata document	VSS Information stored in an XML document that is passed from the writer to the requester. Metadata includes the Writer name, files, and components to back up, a list of components to exclude from the backup, and the methods to use for recovery. See shadow copy set .
mount	To make a volume physically available for use, such as the placement of a removable disk volume or tape into a drive for reading or writing.
mount host	Host in a network that is used to mount storage array snapshot volumes to perform snapshot restore and rollover operations.
mount point	See volume mount point .
multiplex	To simultaneously write data from more than one save set to the same storage device.

N

named instance	An installation of SQL Server that is given a name to differentiate it from other named instances and from the default instance on the same computer. A named instance is identified by the computer name and instance name.
NetWorker administrator	NetWorker server user who may add, change, or delete NetWorker server users.
NetWorker application administrator	NetWorker server user who may operate NetWorker software, configure the NetWorker server, and create and modify NetWorker resources.
NetWorker Management Console (NMC)	Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.
NetWorker security administrator	NetWorker server user who may add, change, or delete NetWorker server user groups.
NetWorker server	Computer on a network that runs the NetWorker server software, contains the online indexes, and provides backup and restore services to the clients and storage nodes on the same network.

NetWorker Snapshot Management (NSM) Technology that provides point-in-time snapshot copies of data. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.

NetWorker User for SQL Server The graphical user interface for the NetWorker Module for Microsoft software. From this interface you can initiate manual backups as well as recoveries.

NetWorker Windows BMR image A bootable image that contains NetWorker binaries and a wizard to control the Windows BMR process.

node See [cluster](#).

non-critical volume A volume that contains files that are not part of the system state or an installed service.

notification Message sent to the NetWorker administrator about important NetWorker events.

O

offline backup Backup of database objects performed while the corresponding database or instance is shut down and unavailable to users. Also known as a cold backup.

offline restore Automated restore that does not require the manual installation of an operating system. A bare metal recovery (BMR) is an offline restore.

online backup Backup of database objects performed while the corresponding database or instance is running and available to users. Also known as a hot backup.

online indexes Databases located on the NetWorker server that contain all the information pertaining to the client backups (client file index) and backup volumes (media index).

online restore Restore operation that is performed from a NetWorker recover program. An online restore requires that the computer has been booted from an installed operating system. See also offline restore.

operator Person who performs day-to-day data storage tasks such as loading backup volumes into storage devices, monitoring volume locations and server status, verifying backups, and labeling volumes.

override A NetWorker feature that allows you to configure a different backup level for a specific date listed in a Schedule resource.

P

parallelism Feature that enables a maximum number of concurrent streams of data during backup or restore operations. For example, parallelism values can be set for the NetWorker server, clients, pools, and groups.

pathname	Set of instructions to the operating system for accessing a file: <ul style="list-style-type: none"> • An absolute pathname indicates how to find a file by starting from the root directory and working down the directory tree. • A relative pathname indicates how to find a file by starting from the current location.
physical cluster client	Backup client that is bound to a physical host in the cluster and can have its own resources (private or local).
physical host	Node or host that forms part of a cluster.
point-in-time copy (PIT copy)	Fully usable copy of a defined collection of data, such as a consistent file system, database, or volume that contains an image of the data as it appeared at a specific point in time. A PIT copy is also called a snapshot or shadow copy.
policy	Set of defined rules for client backups that can be applied to multiple groups. Groups have dataset, schedule, browse, and retention policies.
pool	<ol style="list-style-type: none"> 1. NetWorker sorting feature that assigns specific backup data to be stored on specified media volumes. 2. Collection of NetWorker backup volumes to which specific data has been backed up.
primary storage	Server storage subsystem, such as a disk array, that contains application data and any persistent snapshots of data.
probe-based backup	Type of scheduled backup, also known as an event-based backup, where the NetWorker server initiates the backup only when specified conditions are met, as determined by one or more probe settings.
provider	Software component defined by Microsoft VSS, that plugs in to the VSS environment. A provider, usually produced by a hardware vendor, enables a storage device to create and manage snapshots.
proxy client	Surrogate client that performs the NetWorker save operation for the client that requests the backup. A proxy client is required to perform a serverless backup.
proxy host	Surrogate host computer that performs backup or clone operations in place the production host by using a snapshot copy of the production data. See mount host .

Q

quiesce	State in which all writes to a disk are stopped and the file system cache is flushed. Quiescing the database prior to creating the snapshot provides a transactionally consistent image that can be remounted.
----------------	--

R

recover	To restore data files from backup storage to a client and apply transaction (redo) logs to the data to make it consistent with a given point-in-time.
----------------	---

recyclable save set	Save set whose browse and retention policies have expired. Recyclable save sets are removed from the media database.
recyclable volume	Storage volume whose data has exceeded both its browse and retention policies and is now available to be relabeled and reused.
Registry	Microsoft Windows database that centralizes all Windows settings and provides security and control of system, security, and user account settings.
requester	A VSS-aware application that creates and destroys a shadow copy. NetWorker software is a requester. See shadow copy .
resource	Software component whose configurable attributes define the operational properties of the NetWorker server or its clients. Clients, devices, schedules, groups, and policies are all NetWorker resources.
restore	To retrieve individual data files from backup media and copy the files to a client without applying transaction logs.
retention policy	NetWorker setting that determines the minimum period of time that backup data is retained on a storage volume and available for recovery. After this time is exceeded, the data is eligible to be overwritten.
retrieve	To locate and recover archived files and directories.
role	Grant of user privileges to the Console. There are three roles: Console Application Administrator, Console Security administrator, and the Console User. See user groups .
roll forward	To apply transactional logs to a recovered database to restore it to a state that is consistent with a given point-in-time.
rollover	Backup of a snapshot to conventional storage media, such as disk or tape. Previously known as a live backup.
rollover-only backup	Rollover whereupon the snapshot copy is deleted. Previously known as a serverless backup, live backup, or nonpersistent backup.
root	<ol style="list-style-type: none"> 1. (UNIX only) UNIX superuser account. 2. (Microsoft Windows and UNIX) Highest level of the system directory structure.
S	
save	NetWorker command that backs up client files to backup media volumes and makes data entries in the online index.
save set	<ol style="list-style-type: none"> 1. Group of files or a file system copied to storage media by a backup or snapshot rollover operation. 2. NetWorker media database record for a specific backup or rollover.
save set ID (ssid)	Internal identification number assigned to a save set.
save set recover	To recover data by specifying save sets rather than by browsing and selecting files or directories.

save set status	NetWorker attribute that indicates whether a save set is browsable, recoverable, or recyclable. The save set status also indicates whether the save set was successfully backed up.
save stream	Data and save set information that is written to a storage volume during a backup. A save stream originates from a single save set.
scanner	NetWorker command used to read a backup volume when the online indexes are not available.
scheduled backup	Type of backup that is configured to start automatically at a specified time for a group of one or more NetWorker clients. A scheduled backup generates a bootstrap save set.
secondary storage	Storage media managed by a NetWorker server or storage node that stores conventional or snapshot data. Configure a storage device on a NetWorker server or storage node for each secondary storage.
service port	Port used to listen for backup and recover requests from clients through a firewall.
shadow copy	Temporary, point-in-time copy of a volume created using VSS technology. See VSS (Volume Shadow Copy Service) .
shadow copy set	Complete roadmap of what was backed up at a single instant in time. The shadow copy set contains information about the Writers, their components, metadata, and the volumes. A backup components metadata document containing that information is created and returned to the requester after the snapshot is complete. NetWorker uses this document with the corresponding save set at recover time.
shadow copy technology	Defined and standard coordination between business application, file system, and backup application that allows a consistent copy of application and volume data to exist for replication purposes.
shared disk	Storage disk that is connected to multiple nodes in a cluster.
shell prompt	Cursor in a shell window where commands are typed.
skip	Backup level in which designated files are not backed up. See level .
snapset	See snapshot save set .
snapshot	Point-in-time, read-only copy of specific data files, volumes, or file systems on an application host. Operations on the application host are momentarily suspended while the snapshot is created on a proxy host. Also called a PiT copy, image, or shadow copy.
snapshot policy	Sets of rules that control the life cycle of snapshots. These rule specify the frequency of snapshot creation, how long snapshots are retained, and which snapshots will be backed up to conventional storage media.
snapshot save set	Group of files or other data included in a single snapshot. Previously called a snapset.
stage	To move data from one storage medium to a less costly medium, and later removing the data from its original location.

stand-alone In a cluster environment, a NetWorker server that starts in noncluster (stand-alone) mode.

stand-alone device Storage device that contains a single drive for backing up data. Stand-alone devices cannot automatically load backup volumes.

storage node Computer that manages physically attached storage devices or libraries, whose backup operations are administered from the controlling NetWorker server. Typically a “remote” storage node that resides on a host other than the NetWorker server.

stripes One or more streams of data that may be extracted in parallel from a database, and written in parallel to multiple media devices, such as tape drives.

synthetic full backup Backup that combines a full backup and its subsequent incremental backups to form a new full backup. Synthetic full backups are treated the same as ordinary full backups.

system state All files that belong to VSS Writers with a usage type of BootableSystemState or SystemService. This is required to perform an offline restore.

T

transaction log Record of named database transactions or list of changed files in a database, stored in a log file to execute quick restore and rollback transactions.

U

unscheduled backup See [manual backup](#).

- user**
1. A NetWorker user who can back up and recover files from a computer.
 2. A Console user who has standard access privileges to the Console server.

user groups Feature that assigns user privileges. See [role](#).

V

versions Date-stamped collection of available backups for any single file.

virtual cluster client NetWorker client that is not permanently bound to one physical host but is managed by a cluster manager. It is also referred to as a logical cluster client or a virtual client.

Virtual Device Interface Third party backup applications use Virtual Device Interface (VDI) to communicate with the SQL Server.

- virtual server**
1. Server, usually a web server, that shares resources with other virtual servers on the same computer to provide low-cost hosting services.
 2. In a cluster configuration, a set of two nodes, which are physical computers, and virtual servers. Each node and virtual server has its own IP address and network name. Each virtual server also owns a subset of shared cluster disks and is responsible for starting cluster applications that can fail over from one cluster node to another.

volume	<ol style="list-style-type: none"> 1. Unit of physical storage medium, such as a disk or magnetic tape, to which backup data is written. 2. Identifiable unit of data storage that may reside on one or more computer disks.
volume ID (valid)	Internal identification that NetWorker software assigns to a backup volume.
volume mount point	Disk volume that is added into the namespace of a host disk volume. This allows multiple disk volumes to be linked into a single directory tree, and a single disk or partition to be linked to more than one directory tree.
volume name	Name that you assign to a backup volume when it is labeled.
VSS (Volume Shadow Copy Service)	Microsoft technology that creates a point-in-time snapshot of a disk volume. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.
VSS component	A subordinate unit of a writer. See writer .

W

writer	Database, system service, or application code that works with VSS to provide metadata about what to back up and how to handle VSS components and applications during backup and restore. See VSS (Volume Shadow Copy Service) .
---------------	--

