EMC NetWorker

Version 9.0.x

Server Disaster Recovery and Availability Best Practices Guide

302-001-776

REV 04

EMC²

Copyright © 1990-2016 EMC Corporation All rights reserved.

Published November 2016

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, 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.

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

CONTENTS

Figures 7

Preface 9

Chapter 1 Introduction 13
NetWorker server disaster recovery roadmap....14

Chapter 2 Availability and Recovery Options for a NetWorker Server 15
Bootstrap and indexes....16
Bootstrap save set....16
Client file index save set....16
Bootstrap recommendations and practices....17
How to obtain the bootstrap....17
Gathering the key information....18
Hardware information....18
Software information....19
Disaster recovery scenario review....19
Basic disaster recovery (same host)....19
Advanced disaster recovery (different host)....20
Ground level preparation for NetWorker server disaster recovery....21

Chapter 3 Data Storage and Devices 23
Capabilities and considerations....24
NetWorker metadata storage....24
Multi-path access and failover....24
Storage devices and media....24
Method of connectivity....25
Reliability and dependencies....26

Chapter 4 Disaster Recovery Use Cases 29
Basic disaster recovery scenario....30
Basic disaster recovery considerations....32
More advanced disaster recovery considerations....34
Index or configuration corruption....36
Corruption or loss of SAN storage....36
Loss of one server, Data Domain system, or site....36
Replication solutions....36

Chapter 5 NetWorker Server Disaster Recovery Procedures 39
Recovering a NetWorker server on Linux....40
Planning and preparing for a disaster recovery....40
Gathering key information....40
Backing up the NetWorker server....41

Downloading the NetWorker software and documentation..... 41
Information required before recovering a NetWorker Server..... 42
Gathering NetWorker bootstrap information..... 43
Replacing the hardware, then reinstalling and upgrading the operating system..... 45
Reinstalling the NetWorker server software..... 46
Re-creating links to NetWorker /nsr directories..... 46
Preparing an autochanger for disaster recovery..... 47
Opening NMC and connecting to the NetWorker server..... 47
Configuring NetWorker device and client resource..... 49
Recovering critical NetWorker server databases..... 51
Recovering the NetWorker server application and user data..... 63
Avoiding slow startups due to hostname resolution issues..... 64
Recovering a NetWorker server on Windows..... 66
Planning and preparing for a disaster recovery..... 66
Gathering key information..... 66
Backing up the NetWorker server..... 67
Downloading the NetWorker software and documentation..... 67
Information required before recovering a NetWorker Server..... 68
Replacing the hardware, then reinstalling and upgrading the operating system..... 69
Reinstalling the NetWorker server software..... 70
Preparing an autochanger for disaster recovery..... 70
Opening NMC and connecting to the NetWorker server..... 71
Configuring NetWorker device and client resource..... 73
Recovering critical NetWorker server databases..... 74
Recovering the NetWorker server application and user data..... 90
Avoiding slow startups due to hostname resolution issues..... 91

Chapter 6 NetWorker Client Disaster Recovery Procedures 93
Performing a disaster recovery of a NetWorker client on Linux and UNIX.... 94
Planning notes and preparing for a disaster recovery..... 94
Prerequisites for recovering a NetWorker client or storage node.... 95
Downloading the NetWorker software and documentation..... 95
Replacing the hardware, reinstalling, and upgrading the operating system..... 95
Reinstalling NetWorker client..... 96
Recovering NetWorker client application and user data..... 96
Performing a test backup and recovery..... 97
Performing an authoritative restore on Windows..... 97
Active Directory restore information..... 97
Selecting a restore method..... 97
Performing an authoritative AD restore on Windows Server 2008, 2008 R2, 2012, and 2012 R2..... 98
Running the ntdsutil.exe command line utility..... 99
Restart required after recovery operation..... 100
Checking authoritative restore results..... 100
Performing a non-authoritative restore on Windows..... 101
Active Directory restore information..... 101
Selecting a restore method..... 101
Performing a non-authoritative AD restore on Windows Server 2008, 2008 R2, 2012 and 2012 R2..... 102
Performing a bare metal recovery on Windows 102

Prerequisites for a Bare Metal Recovery (BMR)..... 102
Verifying the Windows BMR requirements..... 102
Performing a Windows BMR to physical or virtual computers..... 105
Performing a Windows BMR to a physical computer..... 107
Performing a BMR from a Physical Computer to a Virtual Machine (P2V)..... 111
Post-recovery tasks..... 112
Using NMM for post-recovery tasks..... 112
Using an application backup tool other than NMM..... 113
Recovering file system data..... 113
Performing post-recovery tasks for Active Directory services..... 114
Performing post-recovery tasks for hosts with Windows server roles that use SQL Server..... 115
Performing post-recovery tasks for a Microsoft Hyper-V virtual machine..... 116
Troubleshooting Windows BMR..... 116
Additional recovery options..... 120
Restart required after recovery operation..... 121

Chapter 7 NetWorker Storage Node Disaster Recovery Procedures 123

Performing a disaster recovery of a Storage Node on UNIX and Linux..... 124
Planning notes and preparing for a disaster recovery..... 124
Gathering key information..... 124
Prerequisites for recovering a NetWorker client or storage node.... 125
Downloading the NetWorker software and documentation..... 125
Replacing the hardware, then reinstalling and upgrading the operating system..... 125
Reinstalling the NetWorker storage node..... 126
Preparing an autochanger for disaster recovery..... 127
Recovering NetWorker client application and user data..... 127
Performing a test backup and recovery..... 128
Performing an authoritative restore on Windows..... 128
Active Directory restore information..... 128
Selecting a restore method..... 129
Performing an authoritative AD restore on Windows Server 2008, 2008 R2, 2012, and 2012 R2..... 129
Running the ntdsutil.exe command line utility..... 130
Restart required after recovery operation..... 132
Checking authoritative restore results..... 132
Performing a non-authoritative restore on Windows..... 132
Active Directory restore information..... 132
Selecting a restore method..... 132
Performing a non-authoritative AD restore on Windows Server 2008, 2008 R2, 2012 and 2012 R2..... 133
Performing a bare metal recovery on Windows 134
Prerequisites for a Bare Metal Recovery (BMR)..... 134
Verifying the Windows BMR requirements..... 134
Performing a Windows BMR to physical or virtual computers..... 136
Performing a Windows BMR to a physical computer..... 139
Performing a BMR from a Physical Computer to a Virtual Machine (P2V)..... 142
Post-recovery tasks..... 144
Using NMM for post-recovery tasks..... 144
Using an application backup tool other than NMM..... 145

Recovering file system data..... 145
Performing post-recovery tasks for Active Directory services..... 145
Performing post-recovery tasks for hosts with Windows server roles that use SQL Server.....147
Performing post-recovery tasks for a Microsoft Hyper-V virtual machine.....148
Troubleshooting Windows BMR..... 148
Additional recovery options.....152
Restart required after recovery operation.....153

Chapter 8 NetWorker Management Console (NMC) Disaster Recovery Procedures 155
Recovering the NMC server to the same server..... 156
Linux..... 156
Windows..... 158
Recovering the NMC server to a different server..... 160
Linux..... 160
Windows..... 162
Configuring an NMC server database backup..... 164

FIGURES

1 Disaster recovery roadmap....14
2 Example of insufficient NetWorker server management....31
3 Standard disaster recovery deployment.... 34
4 Single NetWorker server configured for two sites.... 35
5 Administrator Command Prompt - ntdsutil.... 99
6 Authoritative Restore Confirmation dialog box....100
7 Administrator Command Prompt - ntdsutil....130
8 Authoritative Restore Confirmation dialog box.... 131

Preface

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

Contact your EMC technical support professional if a product does not function correctly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document describes how to design and plan for a NetWorker disaster recovery. However, it does not provide detailed disaster recovery instructions.

Audience

This guide is part of the NetWorker documentation set, and is intended for use by system administrators who are responsible for setting up and maintaining backups on a network. Operators who monitor daily backups will also find this guide useful.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
04	November 8, 2016	Updated NetWorker Server Windows Disaster Recovery Procedures.
03	June 29, 2016	Third release of this document for NetWorker 9.0.1. The following chapters are added in this release: • NetWorker Server Disaster Recovery Procedures • NetWorker Client Disaster Recovery Procedures • NetWorker Storage Node Disaster Recovery Procedures • NetWorker Management Console (NMC) Disaster Recovery Procedures
02	December 16, 2015	Second release of this document for NetWorker 9.0. Updates to the Availability and Recovery Options for a NetWorker Server chapter.
01	September 24, 2015	First release of this document for NetWorker 9.0.

Related documentation

The NetWorker documentation set includes the following publications, available on EMC Online Support:

- *EMC NetWorker Online Software Compatibility Guide*
  Provides a list of client, server, and storage node operating systems supported by the EMC information protection software versions. You can access the guide at https://support.emc.com. From the Support by Product pages, search for NetWorker using "Find a Product", and then select the Install, License, and Configure link.
- *EMC NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *EMC NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *EMC NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *EMC NetWorker Installation Guide*
  Provides information on how to install, uninstall, and update the NetWorker software for clients, storage nodes, and servers on all supported operating systems.
- *EMC NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *EMC NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *EMC NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *EMC NetWorker Data Domain Boost Integration Guide*
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.
- *EMC NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design and plan for a NetWorker disaster recovery. However, it does not provide detailed disaster recovery instructions. The Disaster Recovery section of the NetWorker Procedure Generator (NPG) provides step-by-step disaster recovery instructions.
- *EMC NetWorker Snapshot Management Integration Guide*
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on EMC storage arrays.
- *EMC NetWorker Snapshot Management for NAS Devices Integration Guide*
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.
- *EMC NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.

- *EMC NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *EMC NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *EMC NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *EMC NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- EMC NetWorker Management Console Online Help
  Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click **Help** in the main menu.
- EMC NetWorker User Online Help
  Describes how to use the NetWorker User program, which is the Windows client interface, to connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

Special notice conventions that are used in this document
EMC uses the following conventions 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
EMC uses the following type style conventions in this document:

Table 2 Style conventions

Bold	Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”

Table 2 Style conventions (continued)

{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate non-essential information that is omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments

Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Introduction

This chapter includes the following section:

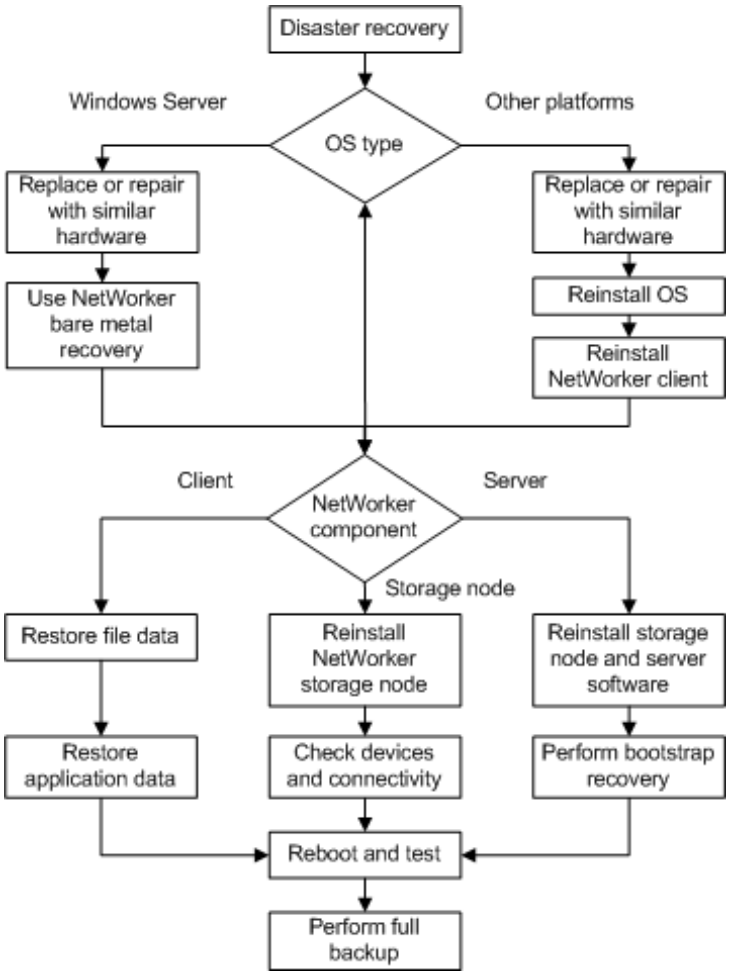
- NetWorker server disaster recovery roadmap 14

NetWorker server disaster recovery roadmap

This guide provides an aid to disaster recovery planning. It does not provide detailed step-by-step disaster recovery instructions.

The following figure lists the high-level steps to follow when performing a disaster recovery of the NetWorker server.

Figure 1 Disaster recovery roadmap



CHAPTER 2

Availability and Recovery Options for a NetWorker Server

This chapter provides an overview of the various options that can be used to protect and recover a NetWorker server, and includes the following sections:

- Bootstrap and indexes 16
- Gathering the key information 18
- Disaster recovery scenario review 19

Bootstrap and indexes

Backing up key configuration information is central to the recovery of a NetWorker server. This configuration information is stored in various locations on the NetWorker server and can change as different clients, devices, and volumes are used, updated, or changed.

The two main backup components that protect this stored data are the Bootstrap save set and the Client file index save set.

Bootstrap save set

The bootstrap is a special save set that is generated by the backup server. The bootstrap backup contains key information about the current state and configuration of NetWorker clients, devices, volumes, and other important information for backup and recovery operations.

The bootstrap consists of four components that reside on the NetWorker server:

- The media database of the NetWorker server.
- The resource files.
- The NetWorker Authentication Service database.
- Lockboxes.

The bootstrap backup is set up in the Server Backup action, which is part of the Server Protection policy. You can also specify to back up the client file index when you configure the Server Backup action. Backing up the bootstrap save set is the only guaranteed method to capture configuration information in a safe and consistent way. This save set is required to ensure a successful disaster recovery of the NetWorker server, regardless of any other protection methods that are used.

Client file index save set

After all of the save sets in a scheduled backup for a client completes, the NetWorker software saves the client-specific backup information to the client file index. Each client has a client file index directory which is stored in the nsr/index directory on the NetWorker server. The client file index acts as a record of backup data and enables simple recovery and the ability to browse and restore the data. A client file index consists of many separate files and directories, and its size depends on the amount of client data backed up.

Each client file index contains the following information:

- Backups that have been performed for a client
- Backup level and type of backup
- File attributes

The client file index is not always required to recover data. You should back up the client file index and ensure that it is available for recovery by using the appropriate bootstrap information. The availability of the client file index greatly impacts the full restoration of backup and recovery services following a disaster recovery. You can also use the client file index to determine the time required to restore a NetWorker server to a fully functional state.

You can use the `nsrck` command to rebuild the client file index for a client from the index backup.

Bootstrap recommendations and practices

The bootstrap backup is set up in the Server Backup action, which is part of the Server Protection policy. You can also specify to back up the client file index when you configure the Server Backup action. Backing up the bootstrap save set is the only guaranteed method to capture configuration information in a safe and consistent way. This save set is required to ensure a successful disaster recovery of the NetWorker server, regardless of any other protection methods that are used.

To ensure that the latest NetWorker server configuration information is captured:

- Maintain a record of the bootstrap save sets for reference. The record should be separate and independent from the backup server or any of its components. You can retain email or printed copies of the bootstrap record.
- Provide the following information in the bootstrap record:
  - The date and time of the bootstrap backup.
  - The volume and location that the bootstrap save set is stored on.
  - The save set ID (SSID) of the bootstrap.
  - The starting file and record number of the bootstrap save set on the volume.
- Perform a bootstrap backup regularly, at least once every 24 hours.
- Clone bootstrap volumes regularly to ensure that a single media failure or loss does not impact the recovery of the NetWorker server.
- Write the bootstrap save set to a device that is local to the NetWorker server.
- Write the bootstrap save set to separate, dedicated media.
- Do not mix the bootstrap save set with client backup data. This procedure speeds up the recovery process and ensures that the recovery of the NetWorker server is not dependant on client data volumes that might have inappropriate policies or protection.
- Ensure that the location of the media does not impact the access to the bootstrap data if a local disaster occurs such as a flood, fire, or loss of power. Although local copies of the bootstrap data are beneficial, they should maintain multiple copies of this information.

How to obtain the bootstrap

Use one of the following methods to obtain information about the bootstrap:

- Review the `policy_notifications.log` file, or the target destination that you configured for the policy resource notification. The **Server backup Action report** section contains information about the bootstrap and client file index backups. For example:

```
---Server backup Action report---
Policy name:Server Protection
Workflow name:Server backup
Action name:Server db backup
Action status:succeeded
Action start time:10/27/15 07:52:34
Action duration:0 hours 0 minutes 34 seconds
--- Successful Server backup Save Sets ---
4079980473/1445957561 bu-iddnwserver: index:edward-sol10x64
```

```
level=1, 1 KB, 0 files
3979317182/1445957566 bu-iddnwserver: index:edward-w2k12r2
level=1, 1 KB, 2 files
3945762750/1445957566 bu-iddnwserver: index:bu-iddnwserver
level=1, 35 MB, 43 files
3777990608/1445957584 bu-iddnwserver: bootstrap level=full,
752 KB, 224 files
--- Bootstrap backup report ---
date time level ssid file record volume
10/22/15 08:43:06 full 3609789450 0 0 DDclone.001
10/22/15 08:43:06 full 3609789450 0 0 bu-iddnwserver.001
10/22/15 10:00:30 full 3156809262 0 0 DDclone.001
10/22/15 10:00:30 full 3156809262 0 0 bu-iddnwserver.001
10/23/15 10:00:31 full 2351589295 0 0 DDclone.001
10/23/15 10:00:31 full 2351589295 0 0 bu-iddnwserver.002
10/24/15 10:00:30 full 1630255406 0 0 DDclone.001
10/24/15 10:00:30 full 1630255406 0 0 bu-iddnwserver.001
10/25/15 10:00:28 full 908921516 0 0 DDclone.001
10/25/15 10:00:28 full 908921516 0 0 bu-iddnwserver.002
10/26/15 10:00:30 full 204364846 0 0 DDclone.001
10/26/15 10:00:30 full 204364846 0 0 bu-iddnwserver.001
10/27/15 07:53:04 full 3777990608 0 0 bu-iddnwserver.002
```

In this example, the SSID/CloneID for the latest bootstrap backup is `3777990608/1445957584` on volume `bu-iddnwserver.002`.

- If the media database is not lost and the volume list is available, use the `mminfo` command to obtain bootstrap information. For example, `mminfo -av -B -s` ***`server_name`***. Where *`server_name`* is the hostname of the NetWorker server.
- Let the `nsrdr` command scan the device for the bootstrap information. For existing devices, `nsrdr` detects the latest bootstrap on a volume that contains the bootstrap information.

Gathering the key information

To aid in quick disaster recovery, maintain accurate records for each hardware, software, network, device, and media component.

Hardware information

Maintain the following hardware information and ensure that is kept up to date:

- Volume or file-system configuration
- Fully qualified domain names, IP addresses, and host names
- References for Domain Name Servers (DNS) gateways, Active Directory, or domain servers
- Hard drive configuration
- Media device names and paths
- Hardware vendor contact information and contract numbers
- Configuration information for each piece of hardware, both active and inactive, for each system

Software information

Maintain the following software information and ensure that is kept up to date:

- Copies of the original operating system media and patches and where they are located
- Software enabler and authorization codes
- Software vendor contact information and contract numbers
- The operating system version and patches that were installed
- Operating system configuration
- Emergency media that can be used to recover a computer if a disaster occurs
- NetWorker bootstrap information for each NetWorker server
- Kernel configuration and location
- Device drivers
- A list of any Windows volume mount points and UNC paths

Disaster recovery scenario review

You might encounter the following disaster recovery scenarios. Each scenario requires a different number of recovery steps and might be easier or more challenging to plan for or recover from.

In the simplest scenario, the same physical server remains in place with little or no changes to the original configuration or the surrounding environment. This is typical of a simple component failure such as a disk or power supply where the base operating system might have been removed or corrupted. In this scenario, a fresh install of the software is required.

In the more complex scenario, a major event has taken place such as a loss of an entire room or building due to flood or fire. Here, the same hardware might not be available and the surrounding environment might be disrupted or changed. The recovery process is more complex and you might need to adapt or prioritize some elements.

The following sections highlight the considerations to note when recovering the NetWorker server.

Basic disaster recovery (same host)

Recovering the NetWorker server to the same host is the simplest way to perform a disaster recovery. This base level of recovery should be planned for and in place for all NetWorker deployments.

In this disaster recovery scenario, the objective is to:

- Restore the NetWorker server as quickly as possible to the latest, last known good point before the server failed.
- Ensure that the original recovery media is available.
- Ensure that the original recovery devices are available.
- Ensure that the original environment such as SAN, IP, and storage units remain unchanged.

This is a simple recovery, if:

- An adequate bootstrap and index backups exists.
- The configuration details have not changed much and are well known or documented.
- You are able to access to the media and devices that are required for the recovery.
- The backup administrator has the appropriate skills and knowledge to perform the recovery task. NetWorker includes a command line wizard program named `nsrdr` that automates the recovery of the NetWorker server's media database, resource files, and client file indexes. The *EMC NetWorker Administration Guide* provides more details.

In some cases, the physical host might be subject to external issues that might prevent a disaster recovery to be performed or fully completed. This scenario might require manual adaptations to ensure that adequate or alternative connectivity is made available. This situation might not require restoring the bootstrap or client file index. To restore the server to the original state following a temporary change, you need to know the original configuration.

Advanced disaster recovery (different host)

The recovery of a NetWorker server to a different host is more complex than performing a basic disaster recovery to the same host. The effort and skills required to recover to a different host is significantly greater than a basic disaster recover to the same host. Recovering to a different host will typically require additional information or resources coupled with the appropriate skills set to perform and complete the task.

While the loss of a building or site is less likely to occur, the effort and speed that is required to recover the NetWorker server has a direct impact on the time to restore or maintain critical business services following an incident. Business-critical services might also be affected and might require a disaster recovery or failover process that relies on the backup and recovery services that the NetWorker server provides. It is therefore essential that an advanced disaster recovery scenario is included in any disaster recovery or business continuity plan.

Although the objective is the same as for the basic disaster recover to the same host, in this situation:

- The NetWorker server hardware is likely to be different and its connectivity and configuration might be different from the original.
- Simply restoring the bootstrap and client indexes might not be as quick or as easy to perform.
- Additional changes to the configuration might also be required before the backup and recovery service is available.
- Immediate access to the original recovery media and the devices cannot be assumed.
- The environment is likely to be different so that the SAN, IP, and storage units might not match the original server.
- Additional steps might be required to make the NetWorker server available.
- The availability of adequate bootstrap and index backups is required, but these might be copies of the original save sets.
- Additional steps might be required to access the save set backups.

Ground level preparation for NetWorker server disaster recovery

To optimize your chances for a successful disaster recovery of the NetWorker server, you must meet the following minimum requirements:

- Back up the bootstrap, and client file indexes for all clients regularly, at least every 24 hours.
- Back up the server OS configuration regularly.
- Monitor, record, and store the status and contents of each bootstrap backup in a separate physical location from the NetWorker server.
- Use a dedicated pool for bootstrap backups.
- Clone the bootstrap backups.
- Record and maintain the connectivity and details of the SAN, IP, and all storage components.

CHAPTER 3

Data Storage and Devices

This chapter includes the following sections:

- Capabilities and considerations 24
- NetWorker metadata storage 24
- Multi-path access and failover 24
- Reliability and dependencies 26

Capabilities and considerations

Successful disaster planning and recovery relies on the availability of the media on which the data is stored and the availability of the devices to read that data. In some cases, the disaster might be localized and the devices and connectivity might be available. Other more serious or catastrophic incidents will impact the environment that the NetWorker server relies on. This scenario might render the devices inoperable or prevent access to devices or media.

A number of strategies can be used to cope with these scenarios and range from:

- Having multiple devices and copies of data.
- Ensuring that alternative devices, media, or paths are available within short time periods.

These recovery strategies will enable you to restore with minimal disruption, effort, and guess work.

NetWorker metadata storage

Protecting the storage or data during its normal life can help to prevent disaster situations from occurring. These steps might also might help to improve the speed or reliability of the disaster recovery.

To help to improve the speed, reliability, scalability, and performance of the backup server:

- Keep key configuration information and index data on separate LUNs to eliminate OS corruption issues and improve overall system performance.
- Host LUNs on RAID-protected or external storage systems to improve the performance, reliability, and resilience of this data.
- Ensure that you have the appropriate amount of storage.
- Ensure that the storage is protected and is performing at optimal levels.
- Consider using advanced protection technology such as replication or snapshots of this data since they offer additional protection.

Multi-path access and failover

With any storage device that is used to store bootstrap information, consider the information outlined in the following sections.

Storage devices and media

As the resilience and ease of deploying storage devices varies, so the disaster recovery strategies that are used should be changed to suit the circumstances. For example, the ability to obtain and move a single tape device is simpler than it would be for a virtual tape library (VTL), where the installation and configuration might take considerable effort and time to achieve.

For traditional tape, you can use a single tape deck that is manually loaded. It can be located next to or inside the same hardware as the physical server. In some cases, this might be an autoloader with multiple devices and an automated robotic arm that loads and unloads the media.

For other storage devices, such as VTL or disk systems, the device might be an appliance that includes CPU, memory, networking, and multiple disk units.

Method of connectivity

The method of connectivity can vary from a simple cable for a standalone tape device, to multiple IP or SAN connections. Having the device or media available is of little use if the required connectivity is unavailable.

The availability of the following components are important aspects of disaster recovery planning:

- Spare cables
- Alternative ports and routes
- Resilient networks

Configure devices with dual ports for multipath access

In some cases, devices can be configured with dual ports or multipath access which is transparent to the backup application and device. However, for other devices this configuration might be more difficult to configure. It is simpler to configure and make available spare ports or alternative host names and routes as a disaster recovery planning step than it is to create or configure them at the time of a disaster recovery.

Most manufacturers do not support dual path tape devices or library control ports, or they impose limitations that make these options impractical. However, you can reserve alternative ports and make available alternative or backup path connections.

Make devices available in multiple locations

In some cases, you might be required to make devices available in multiple locations and then move the backup or direct the data to the appropriate devices. This scenario can provide a faster and more robust backup service. However, these configurations are often complex and might be difficult to configure, maintain, or troubleshoot. In these situations, it is often a choice between actively using and configuring the devices for normal use or having the devices in a standby state for only disaster recovery use.

Normal use is defined as actively using the devices in all locations during normal, non-disaster recovery operations. This can make the configuration more complex and presents operational and troubleshooting challenges. However, it does provide the benefit of being able to use the device and ensures that the device is operational at the time that it is required.

Standby use is defined as leaving the device in a a standby state where it is not used in normal operations. This can simplify the configuration, but the device might be inoperative when it is required. This configuration is also a less efficient use of resources since the devices are not used during normal operations.

Device failover

In both normal use and standby scenarios, device failover is an area that is often prone to error and can require some manual intervention. Although some of these issues are easy to resolve, they should be documented, understood, and practiced.

When planning for disaster recovery, consider the following:

- Device access paths might be different, might change, or might disappear. They can all impact the configuration and might require additional steps to correct.

- Device names should identify the location or use. This can facilitate easier troubleshooting and more reliable execution of disaster recovery procedures.
- Check the device status and availability. Devices that are not used regularly are more likely to exhibit issues at a time when they are most required.
  Designing resilience into the backup service is a good practice and does not have to include idle devices. However, while this solution provides a better return of investment and increases the available capacity and performance for running backup operations, designing resilience also makes the solution more complex to configure and manage. Clustering and replication technologies are used to enhance resilience in the backup environment but also to reduce complexity.

  Implementing clustering and replication technologies in your disaster recovery plan will:

  - Help to manage and automate the different elements such as disk storage and network connections.
  - Ensure that resources such as disk storage and network connections are available on the correct hardware.
  - Ensure that the resources and configurations are appropriate for the software service that is running.

Reliability and dependencies

The reliability of a backup and recovery service depends upon the reliability of the individual components, regardless of the chosen software, devices, and disaster recovery approach.

When designing a resilient backup and recovery service:

- Select devices that match the performance and operating expectations of the service:
  - You can use multiple devices and multiple paths to improve reliability and availability. Although this helps to eliminate single points of failure, it does not remove all of the single points of failure since no service can be completely reliable.
  - Careful design with consideration to the various disaster recovery scenarios will help to identify and eliminate the most common single points of failure.
- Consider the reliability of the expected duty cycle of the service and the components that are used:
  - Some devices cannot operate continuously, or may have limits on performance or functionality.
  - Using some devices, such as physical tape devices, for excessive periods might impact their reliability.
  - Appliances such as disk arrays, deduplication systems, or VTLs might also require maintenance periods in which backups cannot be performed or perform at a reduced speed or rate.
- Consider regular maintenance:
  - Issues might arise that will require some disruptive maintenance to the service.
  - The ability of a service and subcomponents of that service to be taken offline, failed over, or to recover automatically will also ensure that the maintenance is both performed and performed with minimal disruption to the service.

- Software patches and updates will be required to ensure optimum performance, reliability, and support.

CHAPTER 4

Disaster Recovery Use Cases

This chapter includes the following sections:

- Basic disaster recovery scenario 30
- Basic disaster recovery considerations 32
- More advanced disaster recovery considerations 34
- Index or configuration corruption 36
- Corruption or loss of SAN storage 36
- Loss of one server, Data Domain system, or site 36
- Replication solutions 36

Basic disaster recovery scenario

This section describes a basic NetWorker implementation to highlight important disaster recovery focus areas.

The following figure provides an example of a basic NetWorker solution that works well for a small office. If the server is powerful enough and the storage and connections are sized appropriately, it can protect 100 clients and a number of business systems.

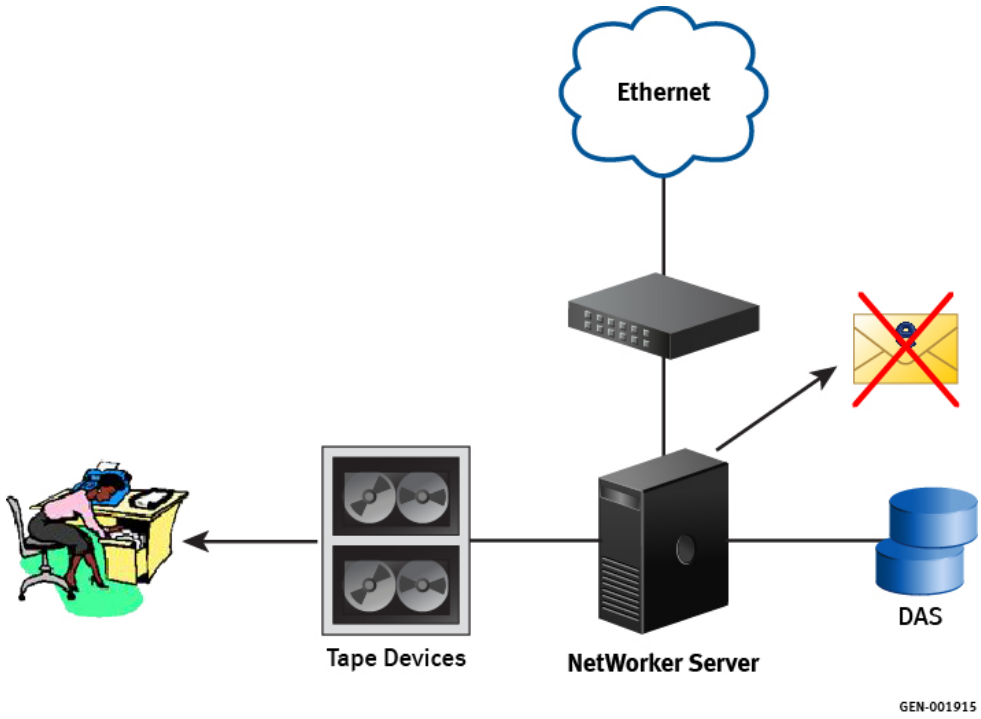
In this example, the NetWorker server configuration offers very little resilience and highlights a number of disaster recovery issues that might make recovery difficult or even impossible:

- The NetWorker server:
  - Has a single ethernet connection and therefore is a single point of failure.
  - Is using internal disks and therefore is a single point of failure.
  - Has no mirroring or storage replication.
  - Is contained to a single space within a room or a data center and therefore is a single point of failure.
- The bootstrap email has not been configured and is not monitored, so the bootstrap backup email messages are lost.
- The bootstrap and index backups are written to a single tape, which has three years of backups on it. The volume has not been changed or cloned and therefore is a single point of failure.
- The single copy of the bootstrap is created for disaster recovery purposes every three months and is stored in the office Administrators desk in a different building. However, the secretary does not know the purpose of this tape and keeps it in a locked desk, in an office a few miles away from the main building and therefore is a single point of failure.

Basic NetWorker solution

Unfortunately, in this example the management of the NetWorker server has been poor and little regard has been paid to the protection of the server.

Figure 2 Example of insufficient NetWorker server management



In this example, the following issues might impede disaster recovery:

- Lack of resilience or redundancy in the backup environment. The NetWorker server is a single system and it uses RAID protected storage, but it is located locally through a direct attachment. This situation is the same for the tape devices that are located in a small autoloader near the system.
- A loss of the site might result in a loss of the tape devices, the server, and the storage. The customer in this situation only has one data room, so the use of a second site is not viable.
- The customer does not remove tapes from the site. The tapes are cycled on a monthly basis, but this process is limited to a small number of monthly backups of key systems, with most tapes remaining on site.
- Bootstrap backups have been configured to run daily and are written to an index and bootstrap tape. This tape is changed, but with staff changes and an increasing workload, it is often left for several weeks. When it is changed, a new tape is labeled and the old tape is given to the office Administrator for storage. However, the office Administrator does not know the purpose of this tape and keeps it in a locked desk, in an office a few miles away from the main building.
- The bootstrap notifications have been configured to be sent by email. Unfortunately, no one monitors the email alias.
- The bootstrap notifications email messages have failed for months and no one is aware of this situation.

If a significant disaster occurs, the company in this example might find it extremely difficult to recover its data and systems. Although some data is held offsite, the ability to recover it relies on the NetWorker server and the infrastructure to be available.

While the hardware components may be quickly found, the ability to recover the NetWorker server to its previous state remains a challenge. The bootstrap tape from the office administrator's desk can be used and may only recently have been changed. The ability to use this tape depends on someone knowing where the tape is and who to

ask and the office administrator being available to unlock the desk and deliver the tape. Unfortunately, without any records of the bootstraps, the entire tape must be scanned to rebuild the records on the new NetWorker server which is a time-consuming process. Since the tape was stored in an area that fluctuated in temperature, read errors might occur and the recovery might not be possible.

Although this situation may seem extreme, it highlights the ways in which, without careful consideration, a disaster recovery situation can have a major impact on the business.

If the following procedures were put in place, the recovery would have been much easier and faster to achieve:

- Regularly change the bootstrap tape
- Clone copies of the bootstrap and client file indexes
- Save the bootstrap notifications

Although some data is likely to have been lost forever, key data could have allowed the business to resume. Although it might not have been practical to have a second site with resilient links or remote storage, some simple measures with good management would have made the recovery situation far easier and faster.

The following examples provide information on improved levels of disaster recovery protection.

Basic disaster recovery considerations

The following steps to improve the availability of a NetWorker server can be simple and cost effective:

- Multiple paths for both network and storage connections are common and can help to reduce the likelihood of a failure that is due to a bad connection or failed NIC or HBA.
- Most storage systems use RAID to prevent one or more disk failures from impacting the system. These storage systems come in a range of sizes that suit any budget.
  Implementing these procedures should be considered as a no-cost option, although the ongoing maintenance and management is likely to incur some expense. However, these options are very simple and cost effective and will have a big impact on the speed and ease that a disaster recovery demands.

  The following figure highlights some of basic steps that can be used to improve the availability and disaster recovery capability of a NetWorker server. It shows a single site that is used for backup and recovery.

  This example shows how a backup environment can be optimized to reduce single points of failure and improve the speed and ability of a recovery, should a disaster recovery be required:

  - The bootstrap and index backups are cloned daily.
  - Copies of the bootstrap and index backup clones are removed from the site and stored in a secure remote location.
  - Dual Path Ethernet with automatic failover is configured and managed by a switch. This provides a single resilient IP connection.
  - Email notifications are captured and stored in several locations and are available from an archive.
  - The backup service and backup operations are monitored daily for nonfatal errors and warnings.

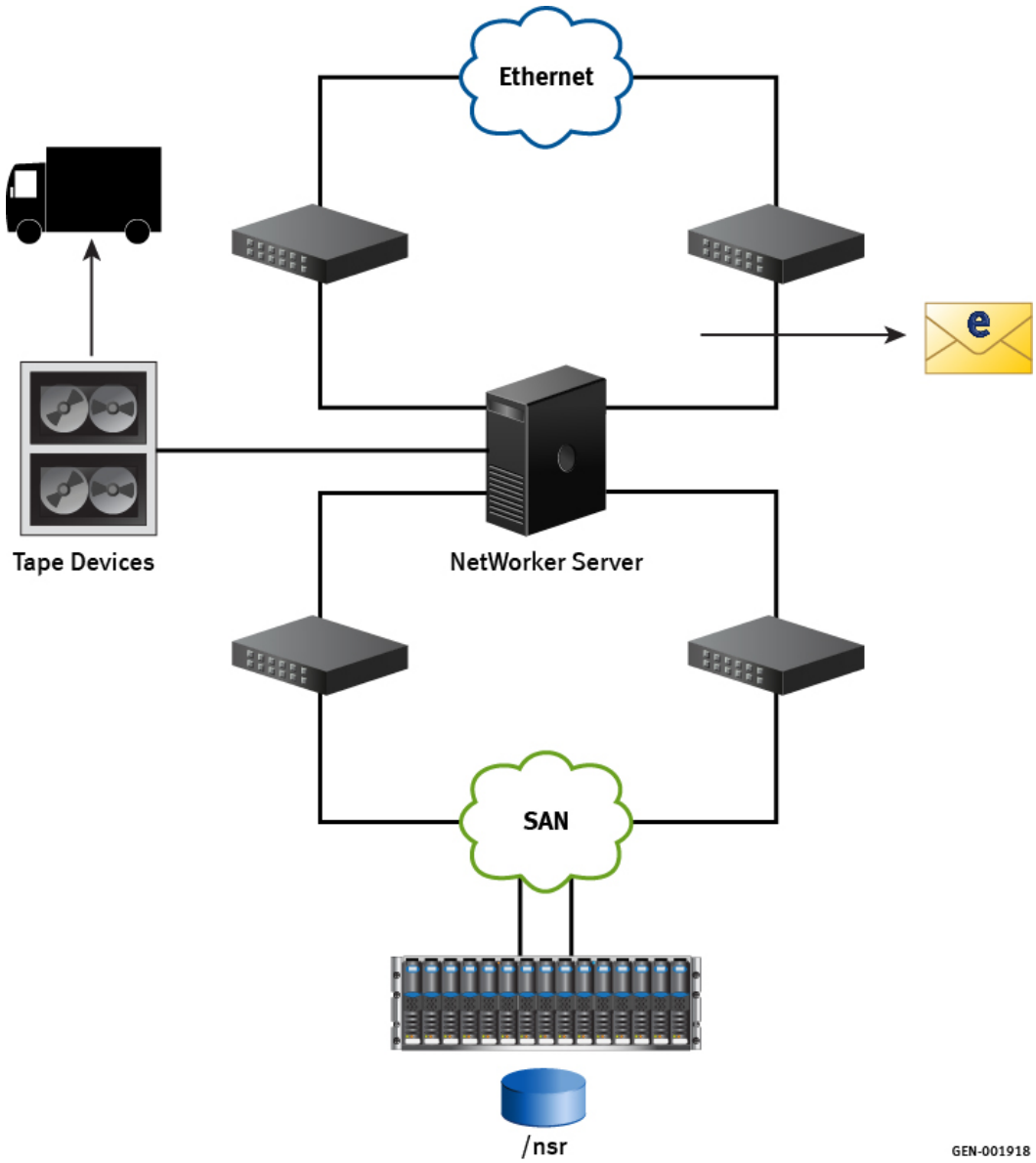
  - A dual path SAN with a storage array that offers RAID protection, replication, and snapshot capabilities is used.

Standard disaster recovery deployment

In this example, the backup environment has been optimized to improve disaster recovery performance in the following ways:

- The same single NetWorker server is made to be more resilient and robust by adding some additional network and SAN links.
- The storage is RAID protected and has additional protection through snapshots, replication, and mirroring.
- Email notifications are sent to an alias that allows them to be accessed remotely. Email notifications are saved and monitored.
- Logs are monitored for errors so that issues can be detected early.
- Tapes are removed from site on a daily basis because there is only one site available.
- Tapes are stored in a secure and controlled location.
- Some data is cloned to ensure that multiple copies exist. This steps aids in recovery and limits any exposure to media failure or loss.
- Bootstraps are cloned daily so that two copies always exist.

Figure 3 Standard disaster recovery deployment



More advanced disaster recovery considerations

This section lists other options that build on resilience and offer higher levels of protection or recovery speed. In many cases, the recommendations from the previous section will provide adequate protection and allow the backup service to be recovered in a reliable manner and in a reasonable period of time. For others, this might not provide enough protection or might not deliver a solution that is as quick or as resilient as the business demands.

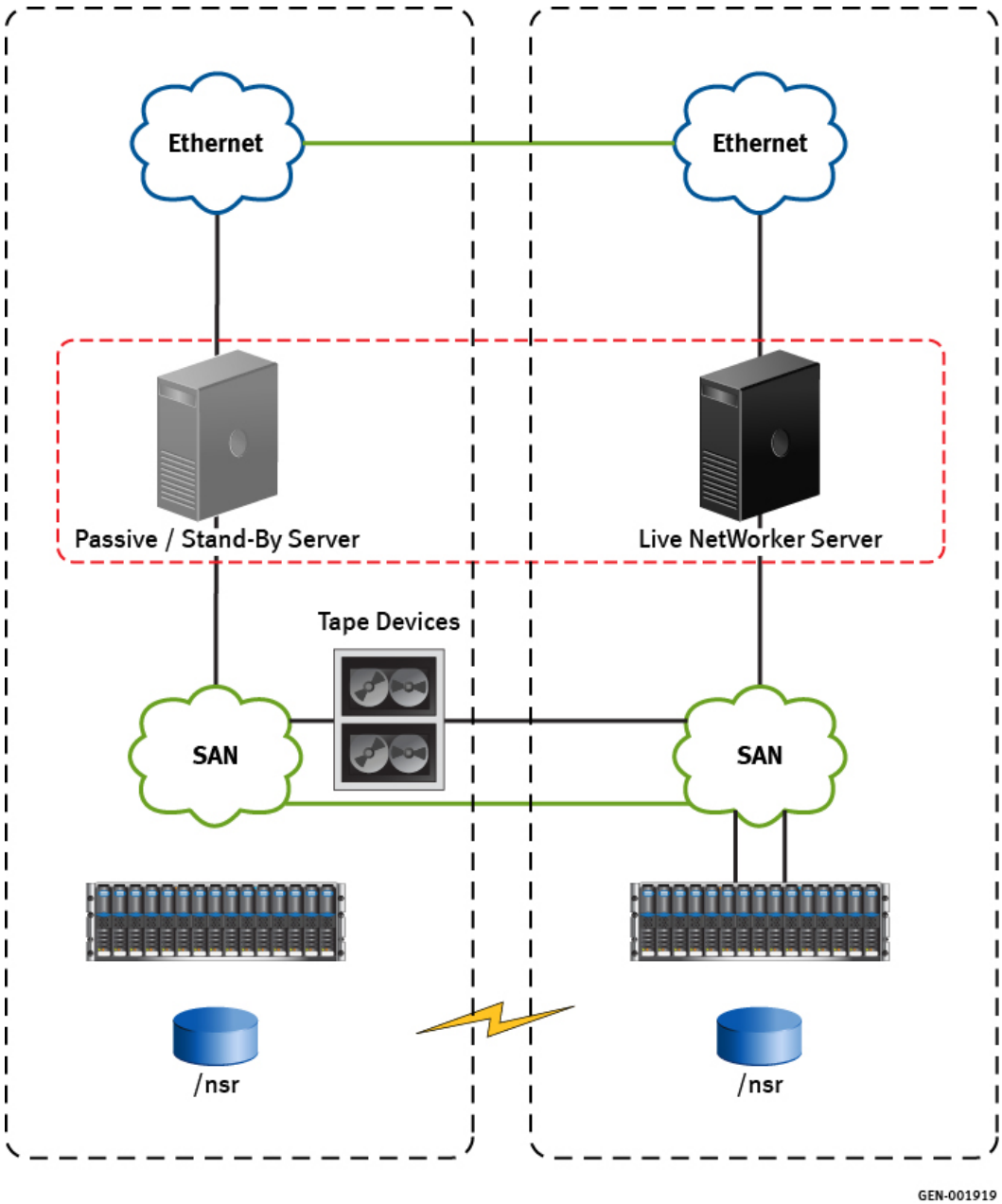
One of the best ways to improve recoverability and resilience is to introduce a second site. This practice allows the infrastructure and data to be present in two locations, which helps to mitigate the impact of an issue in a single site or with a single component within a site.

Single NetWorker server configured for two sites

This figure provides an example of a basic layout of a single NetWorker server that is configured to use two sites, where:

- The same key infrastructure, such as SAN and network, is used.
- The infrastructure is configured with dual paths.
- The storage can be duplicated to provide the ability to replicate the NetWorker configuration on the second site.
- Tape devices are used to store the bootstrap and index backups. These devices are located in a different building.
- To reduce recovery time significantly, the index storage can be replicated or made available to the second site.

Figure 4 Single NetWorker server configured for two sites



In this example:

- One of the sites has a passive or stand-by server, which sits idle until it is required.
- The tape autoloader is the single point of failure in this example because it is located in one site. Although a second autoloader helps, it adds to the complexity of the configuration. Backup to disk solutions coupled with deduplication are better options in this environment.
  One of the challenges with using this configuration, or any configuration in which a production backup server must be protected, is the ability to capture the system in a consistent manner. With backup and recovery operations taking place, the state of the server and the backup configuration files are in a constant state of change. The only way to reliably capture this information is to use the built-in bootstrap backup process.

  While replicating the configuration files is possible, the operation might result in a crash-consistent state. The bootstrap backup is the only method to ensure that the data is able to be recovered.

  In this configuration, the SAN storage can be used to provide space for an AFTD device. These can be used for bootstrap backups and be cloned to the second site to ensure that a consistent copy is available.

Index or configuration corruption

Backing up the bootstrap and index backups on the AFTD will allow for rapid and immediate recovery, if the media database, or configuration areas could be corrupted because of a fault or due to human error. Backing up the bootstrap and index backups on the AFTD will allow for rapid and immediate recovery.

Consider that configuration corruption might make access to the DD Boost devices difficult, where an AFTD device is relatively easy to reconfigure.

Corruption or loss of SAN storage

If SAN storage is lost or corrupt, you can:

- Reconfigure the DD Boost devices.
- Configure the tape device, since you will have bootstrap backups on both Data Domains systems as well as the autochanger.

Loss of one server, Data Domain system, or site

If the server, Data Domain system, or site is lost, it will not result in the loss of backup and recovery service.

If the site or single server loss is the result of a network, power, or cooling event, then the other site should allow the backup service to remain functional after a short delay to allow for the failover to occur. The loss may be temporary, in which case additional recovery actions might not be necessary. You can restore the replication and fail over so that the main site is used once the problem resolved.

If the two sites are within a few miles of each other, you can use the tape out and offsite storage.

Replication solutions

Replication is a term that is used differently by different vendors and replication solutions are rarely the same. The features that are offered can be subtly different and

require different parameters to operate. This section provides some basic background on the support and qualification of the various replication, mirroring, and snapshot features you need to consider for disaster recovery of the NetWorker server.

When planning a replication solution, consider the potential impacts on the NetWorker server, which is constantly at work reading, changing, and updating information:

- Log files are updated with events and errors.
- Client file indexes are updated to reflect new backups or to remove backups that have reached their expiration polices.
- The media database is updated to reflect the location and state of each volume used.
- Save set information is created, deleted, or changed.
- The general configuration is updated to reflect the current state of the NetWorker server with all its storage nodes, devices, and clients.

These activities require many IO operations on the server's disk. Any impacts on the speed and reliability of the IO operations will impact the performance and reliability of the NetWorker server and the disaster recovery.

Replication, mirroring, and snapshot operations all require interception and capture of any requested read, write, and change IOs that occur during the operation. Write IOs require extra processing not only for the disk updates but to confirm that the updates are successful.

If the replication disks are local, the IO activity might take very little time, especially with advanced array technologies. However, if the replication requires operations on systems that are separated by distance, the time required to perform and confirm the operations can have a significant impact.

The *NetWorker Performance and Optimization Planning Guide* provides details on specific performance requirements.

You can validate the performance impacts and support of replication solutions by a Request for Product Qualification (RPQ), which you can submit through EMC Professional Services.

CHAPTER 5

NetWorker Server Disaster Recovery Procedures

This chapter contains the following sections:

- Recovering a NetWorker server on Linux 40
- Recovering a NetWorker server on Windows 66

Recovering a NetWorker server on Linux

The following procedures describe how to recover a NetWorker server on Linux.

Planning and preparing for a disaster recovery

Use the following procedure to create planning notes for a disaster recovery.

Procedure

1. Backup important data on a normal schedule. The more time and effort that is invested in incorporating, maintaining, and testing a backup solution, the better prepared you are if a disaster occurs.
2. Back up servers regularly by using a local device as part of a backup group to ensure that a bootstrap is saved.

   Note

   Backups that are performed by using the command line or the NetWorker User GUI do not save the NetWorker server bootstrap. Use a local backup device on the server to backup the server bootstrap.

3. Perform a scheduled backup of the NetWorker server after upgrading to a new release of NetWorker software. This ensures that an upgraded version of the bootstrap is saved. Always perform a bootstrap backup before updating the software
4. Print the bootstrap information from the `savegrp.log`, which is located in the `nsr` directory. The *EMC NetWorker Administration Guide* provides instructions on how to configure the NetWorker software to send bootstrap information directly to a printer or to a specified email address. If the bootstrap is backed up to a pool, other than the preconfigured pools, save the name of the pool with the bootstrap.

   Note

   Index backups are not in bootstrap backups.

5. Maintain a copy of this information in a safe location for easy access by those assigned to perform disaster recovery. Consider maintaining a copy of this information both onsite and offsite. Having the correct information accessible is a key element in recovering from a disaster as quickly as possible

Gathering key information

Maintain accurate records for each hardware, software, network, device, and media component.

Hardware information

Maintain up-to-date information on computer hardware as follows:

- File system configuration
- Fully qualified domain names, IP addresses, and hostnames

- For Domain Name System (DNS) clients, maintain the DNS host's internet address and hostname
- Hard drive configuration
- Media device names
- Hardware vendor
- Configuration information for each piece of hardware, both active and inactive, within the organization or organizational site

Software information

Maintain up-to-date information on computer software as follows:

- Copies of the original operating system media and patches (and where they are located)
- Software enabler and authorization codes
- Software vendor contact information and contract number
- The operating system version and patches installed
- Operating system configuration
- Emergency media that can be used to recover a computer if a disaster occurs
- NetWorker bootstrap information for each NetWorker server
- Kernel configuration and location
- Device drivers
- A list of any volume mount points

Backing up the NetWorker server

Perform the following steps to back up the NetWorker server including the bootstrap and client indexes.

Procedure

1. Perform a full backup of the backup server from the command prompt:

   ```
   nsrpolicy -start -p <server_protection> -w <server_backup>
   ```

2. To view the status of the policy, type the following command:

   ```
   nsrpolicy monitor -p <server_protection> -w <server_backup>
   ```

3. To obtain the latest bootstrap information, type the following command:

   ```
   mminfo -B
   ```

   Keep the latest bootstrap information in a safe place for future reference in a disaster recovery.

Downloading the NetWorker software and documentation

To obtain the latest NetWorker software and documentation, perform the following steps.

Procedure

1. Review the online NetWorker documentation, such as the *EMC NetWorker Administration Guide*, *EMC NetWorker Installation Guide*, and *EMC NetWorker Release Notes*, for the latest information.

2. Obtain the required NetWorker cumulative hotfix media kits that provide customers with the opportunity to install the latest version of NetWorker including important hotfixes. Cumulative builds are released approximately once a month and each build contain a rollup of the fixes in each previous build.

   If additional hotfixes are required in an environment where a cumulative build is installed, hotfixes can be generated for use with the latest cumulative version. The cumulative releases for specific NetWorker versions are available at http://support.emc.com.

3. Open the NetWorker Cumulative Hotfix document for details regarding fixes that are in each build, knowledge base articles that are related to the fixes in each build, and download instructions.

Information required before recovering a NetWorker Server

The following information is required before recovering a Linux NetWorker server:

- NetWorker version and patch level
- NetWorker installation path
- NetWorker bootstrap information
- Software enabler and authorization codes
- Operating system version and patches installed
- TCP/IP properties:
  - Adapter type
  - IP address
  - Default getaway
  - Subnet mask
  - DNS server hostnames and IP addresses
- Computer properties:
  - Hostname
  - DNS domain name
  - Superuser password
- Backup or clone volume that contains the NetWorker server's most recent:
  - Bootstrap
  - Client file indexes
  - Device and SCSI drivers
  - Media device names
  - Kernel configuration and location.
- For Linux, the following boot files required for starting the kernel:
  - `/unix`
  - `/boot`
  - `/etc/default/boot`
  - `/stand/vmunix`
- If you routinely move NetWorker backup media offsite for safekeeping, ensure that all necessary volumes are available so that you can avoid delays during a recovery.

- To help ensure that you are prepared to replace and reconfigure a hard drive, maintain a current record of the system information. If one or more hard drives fail, refer to the operating system documentation and hard drive vendor documentation for detailed instructions on how to replace the hard drive.
- Obtain the following information by using the appropriate operating system commands:
  - Size of the drive
  - File system volume information
  - Volume label assigned to each disk partition
  - How the disk is partitioned
  - How the disk is loaded
  - The size of the disk
  - Each logical volume (size and label)
  - Each file system

Note

Though it does not affect NetWorker operation, EMC recommends that you note any use of mirroring, Redundant Array of Independent Disk (RAID), striping, compression, or volume sets.
To ensure that you can recover all the drive's data, install a new drive that is the same size or larger than the original drive.

Gathering NetWorker bootstrap information

This section outlines the NetWorker bootstrap information requirements.

Is the bootstrap report available?

Bootstrap report information includes the following:

- Bootstrap SSID (Save Set Identification Number).
- Volume name containing the bootstrap.
- File-number and record-number of the tape media (if used) where the bootstrap information starts.

Use one of the following methods to obtain information about the bootstrap:

- Review the `policy_notifications.log` file, or the target destination that you configured for the policy resource notification. The **Server backup Action report** section contains information about the bootstrap and client file index backups. For example:

```
---Server backup Action report---
Policy name:Server Protection
Workflow name:Server backup
Action name:Server db backup
Action status:succeeded
Action start time:10/27/15 07:52:34
Action duration:0 hours 0 minutes 34 seconds
--- Successful Server backup Save Sets ---
```

```
4079980473/1445957561 bu-iddnwserver: index:edward-sol10x64
level=1, 1 KB, 0 files
3979317182/1445957566 bu-iddnwserver: index:edward-w2k12r2
level=1, 1 KB, 2 files
3945762750/1445957566 bu-iddnwserver: index:bu-iddnwserver
level=1, 35 MB, 43 files
3777990608/1445957584 bu-iddnwserver: bootstrap level=full,
752 KB, 224 files
--- Bootstrap backup report ---
date time level ssid file record volume
10/22/15 08:43:06 full 3609789450 0 0 DDclone.001
10/22/15 08:43:06 full 3609789450 0 0 bu-iddnwserver.001
10/22/15 10:00:30 full 3156809262 0 0 DDclone.001
10/22/15 10:00:30 full 3156809262 0 0 bu-iddnwserver.001
10/23/15 10:00:31 full 2351589295 0 0 DDclone.001
10/23/15 10:00:31 full 2351589295 0 0 bu-iddnwserver.002
10/24/15 10:00:30 full 1630255406 0 0 DDclone.001
10/24/15 10:00:30 full 1630255406 0 0 bu-iddnwserver.001
10/25/15 10:00:28 full 908921516 0 0 DDclone.001
10/25/15 10:00:28 full 908921516 0 0 bu-iddnwserver.002
10/26/15 10:00:30 full 204364846 0 0 DDclone.001
10/26/15 10:00:30 full 204364846 0 0 bu-iddnwserver.001
10/27/15 07:53:04 full 3777990608 0 0 bu-iddnwserver.002
```

In this example, the SSID/CloneID for the latest bootstrap backup is `3777990608/1445957584` on volume `bu-iddnwserver.002`. Policy notifications provides more information about the notification configurations that are available in the Policy, Workflow, and Action resources.

- If the media database is not lost and the volume list is available, use the `mminfo` command to obtain bootstrap information. For example, `mminfo -av -B -s` ***server_name***. Where *server_name* is the hostname of the NetWorker server.
- If the media database is lost, use the `scanner` command to scan the source device for the bootstrap backup. For example, **`scanner -B`** ***device_name***. Where *device_name* is the name of the device that contains the bootstrap backup.

Is a local device available?

The NetWorker server requires a local device resource to recover data from a bootstrap backup. In a disaster recovery situation, the resource database is lost, and you must recreate the local device to recover from the bootstrap save set.

When you recreate the device, keep the following considerations in mind:

- Do not relabel the volume when you create the device. Relabeling a volume with bootstrap backups, or any other backups, renders the data unrecoverable.
- Additional requirements for disk based devices such as AFTD.
  - Do not allow the device wizard to label the disk volume. The **Label and Mount** option on the wizard's **Device Label and Mount** window has this option selected by default. Uncheck the **Label and Mount** option.
  - Specify the local path to the AFTD volume in the device wizard **Select Storage Node** window. Ensure that this is the same path on which the bootstrap data is stored.

Is the bootstrap on a remote device?

NetWorker supports cloning the bootstrap backup to a local or remote device. NetWorker does not support bootstrap recoveries from a remote device. To recover

the bootstrap from a cloned save set on a remote device, you must clone the save set from the remote device to a device that is local to the NetWorker server.

To recover from a clone copy of a bootstrap backup that resides on a remote device, including a CloudBoost device, perform the following steps:

1. Re-create the device that contains the cloned bootstrap save set on the NetWorker server.
2. Create a new local device on the NetWorker server.

   Note

   To prevent data loss, EMC recommends that you create a new AFTD device on the NetWorker server, to which you can recover the bootstrap data.

3. Optionally, if the SSID of the cloned bootstrap save set is unknown, perform the following steps:
   a. Use the `scanner -B` ***`device_name`*** command to determine the SSID of the save set. For example, **`scanner -B rd=bu-idd-cloudboost.iddlab.local:base/bkup`**
   b. Use the `scanner -m -S` ***`SSID`*** command to re-populate the media database with information about the cloned save set.
4. Use the `nsrclone` command or create a save set group, to clone the cloned bootstrap save set to the local device.

Replacing the hardware, then reinstalling and upgrading the operating system

To replace the hardware, then reinstall and upgrade the operating system, perform the following steps.

Procedure

1. Identify the defective or suspect hardware, and then replace the hardware as required.
2. Reinstall a minimum operating system from installation media.
3. Install any patches or upgrade the operating system to the same level as before the disaster.

   Note

   When using the LVM and the file systems of the root VolumeGroups are mounted, check which additional file systems outside of the root VolumeGroups are part of the backup. If VolumeGroups are imported, use the same logical volumes that were used in the backup.
   On Linux, ensure that all LVM device files in `/dev` are unique after the operating system installation.

4. Verify the library and tape drives on the operating system.
5. To ensure that the library and tape drive devices are correct, run the following commands:

   ```
   inquire
   sjirdtag devname
   ```

   where *devname* is the control port of the jukebox.

For example:

```
inquire
sjirdtag scsidev0.2.4
```

Reinstalling the NetWorker server software

Use the following procedure to reinstall the NetWorker server software:

Procedure

1. Reinstall the same version of the NetWorker server software in its original location. Ensure that you install the NetWorker client, storage node, and Authentication service packages.
2. Run the `/opt/nsr/authc-server/scripts/authc_configure.sh` configuration script.
3. To upgrade the NetWorker server, first recover the server to its original state, and then perform the upgrade.

   In a Linux environment, you are not required to reload the license enablers if the NetWorker configuration files exist. By default, the configuration files are located in the `/nsr/res/nsrdb` directory.
4. Reinstall any NetWorker patches that were installed before the disaster.
5. Name the NetWorker server the same as it was before the changes. For example, ensure that the new installation or the new server is configured with the same fully qualified name.
6. Name the devices shortname the same as it was before the changes.

   Installation instructions are provided in the *EMC NetWorker Installation Guide*.

Re-creating links to NetWorker /nsr directories

Perform the following steps to re-create links to NetWorker `/nsr` directories.

Procedure

1. If the `/nsr` directory or any of its subdirectories, except for `/nsr/res`, were linked, re-create those links.

   To re-create links to NetWorker directories:

   a. If NetWorker is running, stop the daemons by typing the `nsr_shutdown` command at the command line.

   b. Move the files to their original location.

   c. Create the links from the `/nsr` directory to the original location.

   d. Restart the NetWorker server.
2. Determine `/nsr/res` directory linking issues. If `/nsr/res` was linked to another directory, do not create the link at this step. Instead, create a `/nsr/res` directory. This directory is used temporarily in recovering the NetWorker server bootstrap.

Note

The resource database will not be recovered to the `/nsr/res` directory created in this step. Instead, the resource directory is recovered to the link's target directory. For example, if `/nsr/res` was linked to a directory named `/bigres`, then the resource database is recovered to `/bigres`. Ensure that there is enough space in the target directory for the recovered resource database.

Preparing an autochanger for disaster recovery

To prepare an autochanger for disaster recovery, perform the following steps. Skip these steps if an autochanger is not used for disaster recovery.

Procedure

1. Ensure that an autochanger resource exists, the directory differs for Linux and Windows:
   - For Linux: `/nsr/res`
   - For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

   If the autochanger resource does not exist, create it using the NetWorker Administration GUI. The *EMC NetWorker Administration Guide* provides details about this interface.
2. Reset the autochanger by using the `nsrjb -vHE` command.

   This command resets the autochanger, ejects backup volumes, reinitializes the element status, and checks each slot for a volume.
   - If the autochanger does not support the `-E` option, initialize the element status by using the `ielem` command.
   - Inventory the autochanger by using the `nsrjb -I` command. The output helps to determine whether the volumes required to recover the bootstrap are located inside the autochanger.

Note

None of these volumes are in the media database, so you cannot view the contents of the tape through NMC and the volume name comes up as `-*`.

Opening NMC and connecting to the NetWorker server

Perform the following steps to open the NetWorker Management Console (NMC) and connect to the NetWorker server.

Note

If the NMC server and the NetWorker server are installed on different hosts, the process owner of the NMC daemon (`gstd`) and the Administrator account for NMC must be added to the Administrators List of the NetWorker Server. In this scenario, perform all steps, otherwise skip to step 3.

Procedure

1. On the NetWorker server, open a command prompt, and then add the NMC server administrator account:

   `nsraddadmin -u "user=administrator, host=`*`shortname_console_host`*`"`

   `nsraddadmin -u "user=administrator, host=`*`longname_console_host`*`"`
   where:

   - *shortname_console_host* is the short name of the NMC server hostname.
   - *longname_console_host* is the long name of the NMC server hostname.

2. Add the process owner of the `gstd` daemon:

   a. If the NMC server is a Windows host, run the following command:

   `nsraddadmin -u "user=SYSTEM, host=`*`shortname_console_host`*`"`

   `nsraddadmin -u "user=SYSTEM, host=`*`longname_console_host`*`"`
   where:

   - *shortname_console_host* is the short name of the NMC server hostname.
   - *longname_console_host* is the long name of the NMC server hostname.

   b. If the NMC server is a Linux host, run the following command:

   `nsraddadmins -u "user=root, host=`*`shortname_console_host`*`"`

   `nsraddadmin -u "user=root, host=`*`longname_console_host`*`"`
   where:

   - *shortname_console_host* is the short name of the NMC server hostname.
   - *longname_console_host* is the long name of the NMC server hostname.

3. Open a browser, and then type the following in the address bar:

   `http://<`*`gst_server_name`*`>:/9000`
   where *gst_server_name* is replaced with the hostname of the server where the NMC server was installed.

   Note

   The NMC server is also known as the GST server.

   The **NetWorker** page displays.

4. Right-click, and then select **Launch Application**.

   The `Launching NetWorker Java` message appears and then the **NMC-Create shortcut** and **NMC Login** window appears.

5. On the **NMC Login** window:

   a. For the username, type `administrator`.

   b. For the password, type the password that was used for the Administrator user of the Authentication service.

   c. Click **OK**.

6. On the **License Agreement** window, review the license text, and then click **Accept**.
7. In the **Set NetWorker License Manager Server Name** window:
   a. Type the hostname of the License Manager server. If you did not install the License Manager software, leave this field blank.
   b. Click **Next**.
8. In the **Set Database Backup Server** window:
   a. In the **NetWorker Server** field, type the hostname of the NetWorker server.
   b. In the **Client name** field, type the hostname of the NMC server.
   c. Check the checkbox for **Create client resource on this server**.

      This step ensures that a client resource is created to backup the Management Console database.
   d. Click **Next**.
9. In the **Add NetWorker Servers** window:
   a. In the **NetWorker Servers** field, type the hostname of each NetWorker server in the environment that is required to be managed. Add one hostname per line.

      The host appears in the **Enterprise** section of the Console.
   b. Click **Finish**.

   The NMC GUI opens.
10. Close the **Getting Started** window.
11. To start using the NetWorker software, click **Enterprise** from the top level toolbar.

    In the left navigation pane, the top level object **Enterprise** displays. Underneath the navigation tree, each NetWorker server hostname which was typed earlier in the window appears.
12. Click the hostname of the NetWorker server.

    On the right side pane, **Host: Server_Name** and **Managed Applications** appear. The NetWorker Administration GUI launches.

Configuring NetWorker device and client resource

Perform the following steps to configure NetWorker device and Client resources.

Procedure

1. Create, and then configure the NetWoker server's device resources.

   To recover data by using a stand-alone device, ensure that a resource for the stand-alone device exists. The directory path differs for Linux and Windows:

   - For Linux: `/nsr/res`
   - For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

   If a resource for the standalone device does not exist, create it using the NetWorker Administration program.

2. In the NetWorker Administration program, open the NetWorker server's Client resource, and then verify that the **Aliases** attribute in the **Preferences** tab

contains the correct information. For example, aliases for a computer that is named Kingdome might be:

```
Kingdome
kingdome.seattle.washington.com
```

3. Set the NetWorker retention policy to a decade.

   The retention policy is one month by default. This enables the recovery of all the server's records.

   Note

   If the NetWorker server's browse and retention policies is not reset, any of the server's records that are more than one month old will be discarded.

4. If you are using the NetWorker Administration program:

   a. Configure the Client resource for the NetWorker server. Set the browse and retention policies to a time value that covers the oldest save sets being used for the recovery.

      This allows you to recover all of NetWorker server's records with the `nsrdr` command.

      Note

      If the retention policy set for the client instance of the NetWorker server is long enough to cover all of the save sets, all of the NetWorker server's records are recovered. However, if the retention policy set for the client is not changed and save sets exist for the NetWorker server that have a retention policy greater than one month, they are discarded because the default browse policy is one month.

5. If you are recovering data using an autochanger, perform the following steps.

   a. Ensure that an autochanger resource exists.

      The directory differs for Linux and Windows.

      - For Linux: `/nsr/res`
      - For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

      If the autochanger resource does not exist, create it using the **NetWorker Console Administration** interface. The *EMC NetWorker Administration Guide* provides details about this interface.

   b. Reset the autochanger by using the `nsrjb -vHE` command.

      This command resets the autochanger, ejects backup volumes, reinitializes the element status, and checks each slot for a volume.

      - If the autochanger does not support the `-E` option, initialize the element status by using the `ielem` command.
      - Inventory the autochanger by using the `nsrjb -I` command. This helps to determine whether the volumes required to recover the bootstrap are located inside the autochanger.

Note

None of these volumes are in the media database. The contents of the tape cannot be viewed through NMC and the volume name comes up as **-***.

Recovering critical NetWorker server databases

Protecting a NetWorker server including its critical databases requires careful planning and preparation. The recovery methods that are described in this section may not work if the NetWorker server is not adequately protected.

Note

Use the `nsrdr` command to recover NetWorker 9.0.1 databases only. To perform a roll back of the NetWorker server to an earlier version of the NetWorker software, contact EMC Customer Support.

The databases that are critical to the recovery of a NetWorker server include the bootstrap and the client file indexes.

A bootstrap includes the:

- Media database—Which contains the volume location of each save set.
- Resource files—Which contains all the resources, such as NetWorker clients and backup groups, that are defined on the NetWorker server.
- The NetWorker Authentication Service database.
- Lockboxes.

  Note

  The lockbox folder in the resource directory stores confidential information, for example, Oracle client passwords and the DD Boost password, in an encrypted format. NetWorker uses this information to perform backup and recovery operations.

The client file indexes include tracking information for each file that belongs to a client's save sets. There is one client file index for each NetWorker client.

The `nsrdr` command line program simplifies the recovery of the media bootstrap, and optionally the client file indexes for a NetWorker server. Previous releases of NetWorker required the `mmrecov` command to recover the media database and resource files, and the `nsrck` command to recover client file indexes. UNIX man page and the *EMC NetWorker Command Reference Guide* provides detailed information about the `nsrdr` command.

Note

The `mmrecov` command is deprecated in NetWorker 9.0 and later and replaced by the `nsrdr` command. EMC recommends that you perform disaster recovery by using the `nsrdr` command.

Use the procedures in this section to recover lost or corrupted bootstrap or client file indexes (CFIs). If the server databases are not corrupted and you only want to restore expired save set entries into the client file index or the media database, use the procedures in the Recovering expired save sets topic of the *EMC NetWorker Administration Guide*. Save sets are removed from the client file index when their

browse policy time has expired. Save set entries are removed from the media database when their retention policy time expires.

The `nsrdr` command is flexible. You can run the `nsrdr` program in fully interactive mode and respond to questions or you can run the program silently with command line options. You can recover the media database, resource files, and all CFIs in one operation, or recover just one item by itself. You can recover individual CFIs or all CFIs in one operation.

To help troubleshoot issues with the wizard, the `nsrdr` command logs messages to the following locations:

- On UNIX, `/nsr/logs/nsrdr.log`
- On Windows, *`NetWorker_install_path`*`\nsr\logs\nsrdr.log`

Consider the recovery options

The `nsrdr` command is flexible and can be run in a variety of ways. However, the major options to consider before running the `nsrd` command are outlined in this section. For a complete list of advanced options, refer to Options for running the nsrdr command on page 61.

Do you need to recover all client file indexes?

Recovering all client file indexes can take a long time. If you only need to recover the client file indexes for a limited set of clients, use the `nsrdr -I` option, for example:

```
nsrdr -c -I clientA clientB clientD
```

Options for running the nsrdr command on page 61 provides more options for recovering specific client file indexes with the `nsrdr` command.

Were save sets backed up after the last bootstrap backup?

If save sets were backed up after the last bootstrap backup, then these backup records might be overwritten after the bootstrap is recovered. This situation can only occur when a manual backup is taken. A manual backup does not trigger a bootstrap backup immediately, therefore the manual backup are not recorded in the bootstrap until the next scheduled backup. To protect against losing save sets that were backed up after the last bootstrap backup, use the `nsrdr -N` or `nsrdr -N -F` options.

For example:

- Use the `nsrdr -N -F` command in a NetWorker datazone that contains tape devices, file type devices, and AFTDs when you only want to protect file type devices and AFTDs against loss of save sets.
- Use the `nsrdr -N` command in a NetWorker datazone that contains tape devices, file type devices, and AFTDs when you want to protect tape devices, file type devices, and AFTDs against loss of save sets.

If you know that manual backups were not taken after the last bootstrap backup or you are not concerned about losing these backups, do not use the `-N` or `-N -F` options. These options can increase the time and complexity of the recovery considerably.

Recovering critical NetWorker server databases

Use the `nsrdr` command to recover the NetWorker server databases from a command prompt.

The `nsrdr` command line options that you use to recover the database depend on the type of devices that are used in the datazone, and how you want to perform the recovery.

Setting nsrdr tuning parameters

You can specify the following tuning parameters for `nsrdr`, the NetWorker server disaster recovery command.

- You can specify the path to the NetWorker services, such as `nsrdr`, if the default path was not used during the installation.
  - The default path on Linux is `/etc/init.d/networker`.
  - The default path on Windows is `C:\Program Files\EMC NetWorker\nsr\bin`.
- The number of parallel threads that can be spawned when recovering client file indexes (CFIs) for multiple NetWorker clients. The default value is 5, which means that up to five parallel threads are spawned to recover CFIs. If you are recovering many client CFIs, increasing this value can shorten the disaster recovery time.

If you do specify any of these parameters, they must be set up before running the command. You can set up these parameters by creating an ASCII plain text file, naming it `nsrdr.conf`, typing the parameter values in the file, and placing the file under the debug folder of the NetWorker installation path. Use the following procedure to set the tuning parameters:

Procedure

1. Create a text file, and then give it the name `nsrdr.conf`.

   Note

   Some text editors append `.txt` to the end of the file name. If this occurs, remove the `.txt` extension so that the file name is `nsrdr.conf`.

2. To specify a non-default path to the NetWorker services, add the following entry:
   - On Linux:

     `NSRDR_SERVICES_PATH = /non_default_path/nsr`
   - On Windows:

     `NSRDR_SERVICES_PATH = drive:\non_default_path\EMC NetWorker\nsr\bin`

     where *non_default_path* is the path to the NetWorker services.

3. To specify the number of parallel threads that can be spawned when recovering CFIs for multiple clients, add the following entry:

   `NSRDR_NUM_THREADS = number`

   where *number* is a value that is greater than 1.

Note

If a value of zero (0) or a negative value is typed, a default value of 5 is automatically assigned instead.

Ensure that a space is added before and after the equals (=) sign. If you specify both tuning parameters, ensure that each value is typed on a separate line.

4. Save the `nsrdr.conf` file as a plain text file, and then place it in the following directory:
   - On Linux: `/nsr/debug/`
   - On Windows: *`NW_install_path`*`\nsr\debug`

   The tuning parameters take effect the next time the `nsrdr` command is run.

Using nsrdr to perform a disaster recovery

Before you begin

Before you perform a disaster recovery of the NetWorker server databases, ensure that the authentication database directory does not contain a recovered database file that is more recent than the bootstrap that you want to recover. The name of the recovered database file is in the following format: `authcdb.h2.db.`*`timestamp`*.

The steps in this section assume that you are running the NetWorker server disaster recovery command, `nsrdr`, in fully interactive mode. EMC recommends that you use the `nsrdr` command to perform a disaster recovery of the NetWorker server. To avoid data loss, EMC recommends using the `-N` option. Options for running the nsrdr command provides information on additional command line options that are available for use with the `nsrdr` command.

Procedure

1. To connect to the NetWorker server and unmount all the volumes including tape, file type, advanced file type devices, and cloud volumes, use NMC.
   a. In the **NetWorker Administration** window, click **Devices**.
   b. Select **Devices** in the navigation tree.

      The **Devices** detail table appears.
   c. Right-click a device, and then select **Unmount**.
2. Enable the common device interface (CDI) attribute.

   Note

   NDMP and optical devices do not support CDI.

   a. From the **View** menu, select **Diagnostic Mode**.
   b. Select **Devices** in the left navigation pane.

      The **Devices** detail table appears.
   c. In the **Devices** table, double-click a device.
   d. Select the **Advanced** tab.

e. In the **Device Configuration** area, locate the CDI settings and select **SCSI commands**.

f. Stop, and then restart the NetWorker server services/daemons.

3. Log in to the NetWorker server as root for a Linux host, or Administrator on a Windows host.
4. To prevent the possibility of overwriting manual backups that were taken after the last bootstrap backup, type:

   ```
   nsrdr -N
   ```

   When you use `-N` option, consider the following:

   - For AFTD devices, you can still write to the disk, however, recover space operations are suspended until the **Scan Needed** flag is removed. A recover space operation clears the disk device of any save sets that do not have a corresponding entry in the media database.
   - For tape devices, when you try to write data to a tape-based device that has newer save sets than what is recorded in the media database, a message displays that explains how to update the media database to avoid the possibility of overwriting the newer data.

   If you are sure that backups were not done after the last bootstrap backup or you do not need to recover that data, omit the options.
5. At the `Do you want to continue?` prompt, type `Y` for yes.
6. (Optional) If you have more than one configured device, the `Configured device` output appears with a list of configured devices. At the `What is the name of the device that you plan to use?` prompt, specify the number that is assigned to the device that contains the NetWorker server bootstrap save set.
7. At the `Enter the latest bootstrap save set id` prompt, type the save set ID of the latest bootstrap.

   If you do not know the save set ID of the latest bootstrap, leave this entry blank, and then press **Enter**, and perform the following steps:

   a. At the `Do you want to scan for bootstrap save set ID on the device?` prompt, type `Y` for Yes.

   Note

   The option to scan for a bootstrap save set ID is not supported for non-English locales. In this case, use the `scanner` command to find the bootstrap ID.

   b. At the `Do you want to recover the bootstrap save set with the selected ID?` prompt, type `Y` for yes, to recover the bootstrap save set.

Note

If you are recovering from a cloud device, you are prompted to type the name of the cloud volume that contains the bootstrap save set. If you are recovering from a cloud device, you are prompted to type the datazone ID of the NetWorker server. Ensure that the datazone ID is for the NetWorker server datazone used to back up the bootstrap.

The `scanner` program is run and the bootstrap save set is recovered. Data from the bootstrap save set replaces the media database.

8. At the `Do you want to replace the existing NetWorker resource configuration database folder, res, with the folder being recovered?`, type **Y** for yes.

   The recover process performs the following tasks:

   - The recovered resource database is saved to a temporary folder named `res.R`.
   - The NetWorker server services are shut down because `nsrdr` cannot overwrite the resource database while these services are running.
   - The recovery process replaces the existing resource database folder with the recovered resource database. The replaced folder is renamed to `res.`*`timestamp`*.

9. At the `Do you want to replace the existing NetWorker Authentication Service database file, authcdb.h2.db, with the recovered database file?`, type **Y** for yes.

10. When prompted to continue, type **Y** for yes.

    The NetWorker server services are restarted after the authentication database is replaced with the recovered authentication database. The replaced file is renamed to `authcdb.h2.db.`*`timestamp`*.

11. At the `Do you want to recover the client file indexes?`, perform one of the following tasks:

    - To recover all the client file indexes, type **Y** for yes. Type **Y** for yes again when asked to confirm the choice. The disaster recovery operation recovers a client file index for each NetWorker client that was backed up including the client file index for the NetWorker server. The disaster recovery operation completes after all the client file indexes are recovered.
    - To recover the client file index for selected clients only:

      a. Type **N** for no.
      The disaster recovery operation completes.

      b. Re-type the `nsrdr` command with the **-c -I** options, and then provide a list of client names with each name separated by a space, for example:

      ```
      nsrdr -c -I clientA clientB clientD
      ```

      The `nsrdr` command skips the bootstrap recovery and you are prompted to complete the recovery of the specified client file indexes.

      The disaster recovery operation completes after all the client file indexes that you specified are recovered.

12. Open the **Administration** window in NMC, and then check that all the NetWorker Server resources appear as expected.
    a. Click the **Protection** icon, and then check that all resources appear as they were before recovery.
    b. Click the **Devices** icon, and then check that all resources appear as they were before recovery.
    c. Click the **Media** icon, and then check that all resources appear as they were before recovery.
    d. Select **Tape Volumes** or **Disk Volumes** from the **Media** screen.
    e. Check the mode status of the volume, **Tape Volumes**, which appears in the window on the right. All volumes should have the same mode that existed before the recovery. All devices that are written to should be in the appendable mode.

Remove the Scan Needed flag from volumes

When you use the `nsrdr` command to set the Scan Needed flag, all the recovered devices are set to the Scan Needed mode (displayed as `Mode = Scan Needed`).

Review the following sections for instructions on how to remove the Scan Needed flag from AFTD, Cloud, and Tape devices.

Removing the Scan Needed flag from AFTDs
If you used the `nsrdr` command to set the scan needed option, all the volumes that are appendable (non read-only) and are in the recovered media database are set to Scan Needed. If you suspect that the volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the recovered media database and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag from the volume.

For AFTD volumes that you suspect may have save sets that were saved after the last bootstrap backup, perform the following steps:

Procedure

1. If you do not know the AFTD device name that corresponds to the AFTD volume, use the `nsrmm` command with the `-C` option:

   ```
   nsrmm -C
   ```

   Output similar to the following is displayed:

   ```
   32916:nsrmm: file disk volume_name mounted on device_name,
   write enabled
   ```

   where *device_name* is the device that corresponds to the AFTD *volume_name*.

2. Use the `scanner` command to repopulate the CFI and media database with the save set information:

   `scanner -i` ***`device_name`***

   where *device_name* is the AFTD device name not the AFTD volume name.

3. Unmount the device, remove the Scan Needed status, and then remount the device. When you remove the Scan Needed status, NetWorker enables recover space operations for the device:

   a. To unmount the AFTD volume, perform the following steps:

      a. Use NMC to connect to the NetWorker server. On the **Administration** window, select **Devices**, and then click **Devices** in the left panel.

      b. Identify the device in the right panel that you want to unmount. Note the volume that is associated with the device.

      c. Right-click the device, and then select **Unmount**.

      d. Repeat for all devices that require the Scan Needed status to be removed.

   b. To remove the Scan Needed status, perform the following steps:

      a. On the **Administration** window, select **Media**, and then click **Disk Volumes** in the left panel.

      b. Identify the volume in the right panel that is associated with the device in the previous step.

      c. Right-click the volume, and then select **Mark Scan Needed**.

      d. Select **Scan is NOT needed**, and then click **OK**.

      e. Repeat for all volumes that require the Scan Needed status to be removed.

   c. To mount the AFTD volume, perform the following steps:

      a. On the **Administration** window, select the **Devices**, and then click **Devices** in the left panel.

      b. Identify the device in the right panel that you want to mount.

      c. Right-click the device, and then select **Mount**.

      d. Repeat for all devices that were unmounted.

      e. Ensure that all devices are mounted and that the Scan Needed status has been removed for the associated volumes.

Results

You can now use normal recovery procedures to recover application and user data on the NetWorker server.

NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or an NMM protected virtual DAG Exchange server, the `nsrdr.log` file contains false error messages that are related to the CFI recovery of the underlying physical hosts. Using an NMM protected virtual DAG Exchange server as an example, a messages similar to the following appears:

```
9348:nsrck: The index recovery for 'EXCH2010-2.vll1.local'
failed.9431:nsrck: can't find index backups for
'EXCH2010-2.vll1.local' on server 'sa-wq.vll1.local'
```

You can ignore error messages that are related to the physical hosts, because NetWorker does not backup the underlying physical host in a virtual environment.

Removing the Scan Needed flag from Cloud devices

If you used the `nsrdr` command to set the scan needed option, all the volumes that are appendable (non read-only) and are in the recovered media database are set to Scan Needed. If you suspect that the volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the recovered media database and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag from the volume.

For Cloud volumes that you suspect may have save sets that were saved after the last bootstrap backup, perform the following steps:

Procedure

1. If you do not know the Cloud device name that corresponds to the Cloud volume, use the `nsrmm` command with the `-C` option:

   ```
   nsrmm -C
   ```

   Output similar to the following is displayed:

   ```
   32916:nsrmm: file disk volume_name mounted on device_name,
   write enabled
   ```

   where *device_name* is the device that corresponds to the Cloud *volume_name*.

2. To repopulate the CFI and media database with the save set information, use the `scanner` command:

   ```
   scanner -i -V cloud_volume -Z datazone_ID cloud_device
   ```

where *datazone_ID* is the NetWorker server datazone ID if it is in a different datazone than the cloud device.

Results

You can now use normal recovery procedures to recover application and user data on the NetWorker server.

NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or an NMM protected virtual DAG Exchange server, the `nsrdr.log` file contains false error messages that are related to the CFI recovery of the underlying physical hosts. Using an NMM protected virtual DAG Exchange server as an example, a messages similar to the following appears:

```
9348:nsrck: The index recovery for 'EXCH2010-2.vll1.local'
failed.9431:nsrck: can't find index backups for
'EXCH2010-2.vll1.local' on server 'sa-wq.vll1.local'
```

You can ignore error messages that are related to the physical hosts, because NetWorker does not backup the underlying physical host in a virtual environment.

Removing the Scan Needed flag from tape devices

If you used the `nsrdr` command to set the scan needed option, all the volumes that are appendable (non read-only) and are in the recovered media database are set to Scan Needed. If you suspect that the volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the recovered media database and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag from the volume.

If you used the `-N` option with the `nsrdr` command and you try to mount a tape volume that has save sets that are newer than what is recorded in the media database, a message similar to the following appears:

```
             nw_server nsrd media info: Volume volume_name has save
sets unknown to media database. Last known file number in media
database is ### and last known record number is ###. Volume
volume_name must be scanned; consider scanning from last known file
and record numbers.
```

For tape volumes that you suspect may have save sets that were saved after the last bootstrap backup, perform the following steps:

Procedure

1. Make a note of the file number and record number that is displayed in the message.
2. To repopulate the CFI and media database with the save set information, use the scanner command:

   `scanner -f file -r record -i device`

3. To remove the Scan Needed flag from the tape volume, use the `nsrmm` command:

   `nsrmm -o notscan volume_name`

Results

You can now use normal recovery procedures to recover application and user data on the NetWorker server.

NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or an NMM protected virtual DAG Exchange server, the `nsrdr.log` file contains false error messages that are related to the CFI recovery of the underlying physical hosts. Using an NMM protected virtual DAG Exchange server as an example, a messages similar to the following appears:

```
9348:nsrck: The index recovery for 'EXCH2010-2.vll1.local'
failed.9431:nsrck: can't find index backups for
'EXCH2010-2.vll1.local' on server 'sa-wq.vll1.local'
```

You can ignore error messages that are related to the physical hosts, because NetWorker does not backup the underlying physical host in a virtual environment.

Options for running the nsrdr command

You can run the NetWorker server disaster recovery wizard command (`nsrdr`) with various command line options instead of running the wizard in fully interactive mode. The following table includes a brief description of the `nsrdr` command line options. For a complete description of the `nsrdr` command and its options, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

Table 3 Command line options for the nsrdr command

Option	Description
`-a`	Runs the command line wizard in non-interactive mode. At a minimum, the `-B` and `-d` options must be specified with this command. Be sure to specify a valid bootstrap ID with the `-B` option when running this command in non-interactive mode. Otherwise,

Table 3 Command line options for the nsrdr command (continued)

Option	Description
	the wizard exits as though it was canceled without providing a descriptive error message.
`-B` *bootstrap_ID*	The save set ID of the bootstrap to be recovered.
`-d` *device_name*	The device from which to recover the bootstrap.
`-K`	Use the original resource files instead of the recovered resource files.
`-v`	Verbose mode. Generates troubleshoot information.
`-q`	Quiet mode. Display only error messages.
`-c`	Recover client file indexes only. If specified with the `-a` option, you must also specify the `-I` option.
`-I` `-I` *client1 client2...*	Specify which CFIs (client file indexes) to recover. Each client name must be typed at the command prompt and separated with a space. If no client names are specified, all client file indexes are recovered. When the `-I` option is specified, ensure that it is the last option in the command string because any entries after the `-I` option are interpreted as client names.
`-f` *path/file_name*	Specify which CFIs to recover by using an ASCII text file. Place each client name on a separate line in the file. Must be used with the `-I` option. Ensure that each client name is typed correctly because there is no validation of client names.
`-t` *date/time*	Recover CFIs from the specified date or date and time. You must type a date and optionally, a time, format that is accepted by the `nsr_getdate` program. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about `nsr_getdate`.
`-N`	If tape volumes have save sets that are newer than what is recorded in the recovered bootstrap backup, they are marked as Scan Needed, to prevent the possibility of losing backed up data. For AFTD devices, this option prevents NetWorker from running recover space operations until you remove the Scan Needed flag. A recover space operation clears the disk device of any save sets that do not

Table 3 Command line options for the nsrdr command (continued)

Option	Description
	have a corresponding entry in the media database.
`-F`	This option sets the Scan Needed flag on File type devices, AFTD devices, and Cloud devices only. The `nsrdr` command will not mark tape volumes as Scan Needed. This option requires the `-N` option.

Examples

The following examples depict some common `nsrdr` commands.

- To recover the bootstrap data and selected client file indexes only, type:
  `nsrdr -I client1 client2 client3`

  where each client name is separated with a space.
- To recover the bootstrap data and selected client file indexes by using an input file, type:
  `nsrdr -f path\file_name -I`

  where *file_name* is an ASCII text file with one client name on each line.
- To skip the bootstrap recovery and recover selected client file indexes by using an input file, type:
  `nsrdr -c -f path\file_name -I`

  where *file_name* is an ASCII text file with one client name on each line.
- To skip the recovery of bootstrap data and recover all client file indexes, type:
  `nsrdr -c -I`
- To skip the recovery of bootstrap data and recover selected client file indexes, type:
  `nsrdr -c -I client1 client2`
- To skip the recovery of bootstrap data and recover selected client file indexes from a specified date, type:
  `nsrdr -c -t date/time -I client1 client2`

  where the *date/time* is the date and/or time from which the client file indexes are recovered. The date/time format is specified in *MM/DD/YYYY* format or any date and time accepted by the `nsr_getdate` command. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about the`nsr_getdate` command.
- To run `nsrdr` in non-interactive mode and to recover the bootstrap data and all client file indexes, type:
  `nsrdr -a -B bootstrap_ID -d device -I`

Recovering the NetWorker server application and user data

Perform the following steps to recover the application and user data that was on NetWorker server.

Procedure

1. Log in as root.

2. Load and inventory the devices.

   This ensures that the NetWorker server can recognize the location of each volume.

   Note

   If you load a clone volume, either delete the original volume from the media database or mark the desired save set as suspect in the media database. If you are using the clone volume, it is used for the remainder of the recovery process.

3. Run the `nwrecover` program.
4. Mark all the directories or files to be recovered.

   Note

   Overwriting operating system files may cause unpredictable results.

5. Click **Start** to begin the recovery.

   Note

   The bootstrap backup restores the `res` directory, which in turn contains the `nsrla` database directory. The `nsrla` database contains the setting for directed recoveries, so this setting should be preserved with the bootstrap restore. More information about setting the directed recover option on a NetWorker client is provided in the *EMC NetWorker Administration Guide*.

Avoiding slow startups due to hostname resolution issues

Hostname resolution issues can cause the NetWorker server to become unresponsive or start very slowly. If either of the following situations apply to the environment, consider the workaround included in this section.

- The NetWorker server uses DNS, but the DNS server is not available.
- The NetWorker server cannot resolve all of its NetWorker client hosts.

Workaround for hostname resolutions issues

Perform the following steps if the NetWorker server starts slowly or becomes unresponsive due to hostname resolution issues.

Procedure

1. Disable DNS lookup for the host being recovered, and then use the local hosts file on the NetWorker server for the hostname resolution.
   - For Windows, the hosts file is located in `C:\Windows\System32\Drivers\etc\`.
   - For Linux, the file is located in `/etc`.

   Modify the `/etc/nsswitch.conf` file to look up the hosts files, before DNS, as a hostname resolution method.

2. Ensure that the hosts file is set up so that the full qualified domain name (FQDN) is first and is followed by the corresponding shortname.

Note

If the NetWorker server's client name was originally the shortname, then the shortname must be first, followed by the longname. For example, 10.10.2.5 host.emc.com.

3. When the DNS server is available, re-enable DNS lookup.

Making changes to the etc/nsswitch.conf file

Perform the following steps to edit the `etc/nsswitch.conf` file:

Procedure

1. If the hosts line in the `/etc/nsswitch.conf` file contains the following:

   ```
   hosts: dns files
   ```

   This indicates that the DNS feature is used first. If the DNS servers are not available or cannot resolve the address, then modify the hosts line to use the `/etc/hosts` file for hostname resolution. Change the hosts line to the following:

   ```
   hosts: files
   ```

2. On the NetWorker server, populate the local hosts file with the known client's valid IP address. For those clients whose IP address is unknown, use 127.0.0.1.

   127.0.0.1 is the standard IP address used for a loopback network connection. When the NetWorker server comes up, a DNS check is performed for each client. For clients that are offline or not available, the server connects to 127.0.0.1 which immediately loops back to the same host. This approach helps the NetWorker server to become available faster instead of waiting to resolve all the clients DNS lookup.

3. When the DNS server is available, re-enable DNS lookup.

   Note

   This method for resolving the hostnames is preferred when the NetWorker server is recovered after a DNS server failure.

   When the NetWorker server is available, a valid client IP address must be updated in the local hosts file to perform a backup or recovery for the critical clients.

   When the DNS server is available and running, remove the client details from the local hosts file.

Recovering a NetWorker server on Windows

The following procedures describe how to recover a NetWorker server on Windows.

Planning and preparing for a disaster recovery

Use the following procedure to create planning notes for a disaster recovery.

Procedure

1. Backup important data on a normal schedule. The more time and effort that is invested in incorporating, maintaining, and testing a backup solution, the better prepared you are if a disaster occurs.
2. Back up servers regularly by using a local device as part of a backup group to ensure that a bootstrap is saved.

   Note

   Backups that are performed by using the command line or the NetWorker User GUI do not save the NetWorker server bootstrap. Use a local backup device on the server to backup the server bootstrap.

3. Perform a scheduled backup of the NetWorker server after upgrading to a new release of NetWorker software. This ensures that an upgraded version of the bootstrap is saved. Always perform a bootstrap backup before updating the software
4. Print the bootstrap information from the `savegrp.log`, which is located in the `nsr` directory. The *EMC NetWorker Administration Guide* provides instructions on how to configure the NetWorker software to send bootstrap information directly to a printer or to a specified email address. If the bootstrap is backed up to a pool, other than the preconfigured pools, save the name of the pool with the bootstrap.

   Note

   Index backups are not in bootstrap backups.

5. Maintain a copy of this information in a safe location for easy access by those assigned to perform disaster recovery. Consider maintaining a copy of this information both onsite and offsite. Having the correct information accessible is a key element in recovering from a disaster as quickly as possible

Gathering key information

Maintain accurate records for each hardware, software, network, device, and media component.

Hardware information

Maintain up-to-date information on computer hardware as follows:

- File system configuration
- Fully qualified domain names, IP addresses, and hostnames

- For Domain Name System (DNS) clients, maintain the DNS host's internet address and hostname
- Hard drive configuration
- Media device names
- Hardware vendor
- Configuration information for each piece of hardware, both active and inactive, within the organization or organizational site

Software information

Maintain up-to-date information on computer software as follows:

- Copies of the original operating system media and patches (and where they are located)
- Software enabler and authorization codes
- Software vendor contact information and contract number
- The operating system version and patches installed
- Operating system configuration
- Emergency media that can be used to recover a computer if a disaster occurs
- NetWorker bootstrap information for each NetWorker server
- Kernel configuration and location
- Device drivers
- A list of any volume mount points

Backing up the NetWorker server

Perform the following steps to back up the NetWorker server including the bootstrap and client indexes.

Procedure

1. Perform a full backup of the backup server from the command prompt:

   ```
   nsrpolicy -start -p <server_protection> -w <server_backup>
   ```

2. To view the status of the policy, type the following command:

   ```
   nsrpolicy monitor -p <server_protection> -w <server_backup>
   ```

3. To obtain the latest bootstrap information, type the following command:

   ```
   mminfo -B
   ```

   Keep the latest bootstrap information in a safe place for future reference in a disaster recovery.

Downloading the NetWorker software and documentation

To obtain the latest NetWorker software and documentation, perform the following steps.

Procedure

1. Review the online NetWorker documentation, such as the *EMC NetWorker Administration Guide*, *EMC NetWorker Installation Guide*, and *EMC NetWorker Release Notes*, for the latest information.

2. Obtain the required NetWorker cumulative hotfix media kits that provide customers with the opportunity to install the latest version of NetWorker including important hotfixes. Cumulative builds are released approximately once a month and each build contain a rollup of the fixes in each previous build.

   If additional hotfixes are required in an environment where a cumulative build is installed, hotfixes can be generated for use with the latest cumulative version. The cumulative releases for specific NetWorker versions are available at http://support.emc.com.

3. Open the NetWorker Cumulative Hotfix document for details regarding fixes that are in each build, knowledge base articles that are related to the fixes in each build, and download instructions.

Information required before recovering a NetWorker Server

The following information is required before recovering a Linux NetWorker server:

- NetWorker version and patch level
- NetWorker installation path
- NetWorker bootstrap information
- Software enabler and authorization codes
- Operating system version and patches installed
- TCP/IP properties:
  - Adapter type
  - IP address
  - Default getaway
  - Subnet mask
  - DNS server hostnames and IP addresses
- Computer properties:
  - Hostname
  - DNS domain name
  - Superuser password
- Backup or clone volume that contains the NetWorker server's most recent:
  - Bootstrap
  - Client file indexes
  - Device and SCSI drivers
  - Media device names
  - Kernel configuration and location.
- For Linux, the following boot files required for starting the kernel:
  - `/unix`
  - `/boot`
  - `/etc/default/boot`
  - `/stand/vmunix`
- If you routinely move NetWorker backup media offsite for safekeeping, ensure that all necessary volumes are available so that you can avoid delays during a recovery.

- To help ensure that you are prepared to replace and reconfigure a hard drive, maintain a current record of the system information. If one or more hard drives fail, refer to the operating system documentation and hard drive vendor documentation for detailed instructions on how to replace the hard drive.
- Obtain the following information by using the appropriate operating system commands:
  - Size of the drive
  - File system volume information
  - Volume label assigned to each disk partition
  - How the disk is partitioned
  - How the disk is loaded
  - The size of the disk
  - Each logical volume (size and label)
  - Each file system

Note

Though it does not affect NetWorker operation, EMC recommends that you note any use of mirroring, Redundant Array of Independent Disk (RAID), striping, compression, or volume sets.
To ensure that you can recover all the drive's data, install a new drive that is the same size or larger than the original drive.

Replacing the hardware, then reinstalling and upgrading the operating system

To replace the hardware, then reinstall and upgrade the operating system, perform the following steps.

Procedure

1. Identify the defective or suspect hardware, and then replace the hardware as required.
2. Reinstall a minimum operating system from installation media.
3. Install any patches or upgrade the operating system to the same level as before the disaster.

   Note

   When using the LVM and the file systems of the root VolumeGroups are mounted, check which additional file systems outside of the root VolumeGroups are part of the backup. If VolumeGroups are imported, use the same logical volumes that were used in the backup.
   On Linux, ensure that all LVM device files in `/dev` are unique after the operating system installation.

4. Verify the library and tape drives on the operating system.
5. To ensure that the library and tape drive devices are correct, run the following commands:

   ```
   inquire
   sjirdtag devname
   ```

where *devname* is the control port of the jukebox.

For example:

```
inquire
sjirdtag scsidev0.2.4
```

Reinstalling the NetWorker server software

Use the following procedure to reinstall the NetWorker server software:

Installation instructions are provided in the *EMC NetWorker Installation Guide*.

Upgrading instructions are provided in the EMC NetWorker Updating from a Previous Release Guide.

Procedure

1. Reinstall the same version of the NetWorker server software in its original location. Ensure that you install the NetWorker client, storage node, and Authentication service packages.
2. To upgrade the NetWorker server, first recover the server to its original state, and then perform the upgrade.
3. Reinstall any NetWorker patches that were installed before the disaster.
4. Name the NetWorker server the same as it was before the changes. For example, ensure that the new installation or the new server is configured with the same fully qualified name.
5. Name the devices shortname the same as it was before the changes.

Preparing an autochanger for disaster recovery

To prepare an autochanger for disaster recovery, perform the following steps. Skip these steps if an autochanger is not used for disaster recovery.

Procedure

1. Ensure that an autochanger resource exists, the directory differs for Linux and Windows:
   - For Linux: `/nsr/res`
   - For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

   If the autochanger resource does not exist, create it using the NetWorker Administration GUI. The *EMC NetWorker Administration Guide* provides details about this interface.
2. Reset the autochanger by using the `nsrjb -vHE` command.

   This command resets the autochanger, ejects backup volumes, reinitializes the element status, and checks each slot for a volume.
   - If the autochanger does not support the `-E` option, initialize the element status by using the `ielem` command.
   - Inventory the autochanger by using the `nsrjb -I` command. The output helps to determine whether the volumes required to recover the bootstrap are located inside the autochanger.

Note

None of these volumes are in the media database, so you cannot view the contents of the tape through NMC and the volume name comes up as **-***.

Opening NMC and connecting to the NetWorker server

Perform the following steps to open the NetWorker Management Console (NMC) and connect to the NetWorker server.

Note

If the NMC server and the NetWorker server are installed on different hosts, the process owner of the NMC daemon (`gstd`) and the Administrator account for NMC must be added to the Administrators List of the NetWorker Server. In this scenario, perform all steps, otherwise skip to step 3.

Procedure

1. On the NetWorker server, open a command prompt, and then add the NMC server administrator account:

   `nsraddadmin -u "user=administrator, host=`*`shortname_console_host`*`"`

   `nsraddadmin -u "user=administrator, host=`*`longname_console_host`*`"`
   where:

   - *shortname_console_host* is the short name of the NMC server hostname.
   - *longname_console_host* is the long name of the NMC server hostname.

2. Add the process owner of the `gstd` daemon:

   a. If the NMC server is a Windows host, run the following command:

   `nsraddadmin -u "user=SYSTEM, host=`*`shortname_console_host`*`"`

   `nsraddadmin -u "user=SYSTEM, host=`*`longname_console_host`*`"`
   where:

   - *shortname_console_host* is the short name of the NMC server hostname.
   - *longname_console_host* is the long name of the NMC server hostname.

   b. If the NMC server is a Linux host, run the following command:

   `nsraddadmins -u "user=root, host=`*`shortname_console_host`*`"`

   `nsraddadmin -u "user=root, host=`*`longname_console_host`*`"`
   where:

   - *shortname_console_host* is the short name of the NMC server hostname.
   - *longname_console_host* is the long name of the NMC server hostname.

3. Open a browser, and then type the following in the address bar:

   `http://<`*`gst_server_name`*`>://9000`
   where *gst_server_name* is replaced with the hostname of the server where the NMC server was installed.

Note

The NMC server is also known as the GST server.

The **NetWorker** page displays.

4. Right-click, and then select **Launch Application**.

   The `Launching NetWorker Java` message appears and then the **NMC-Create shortcut** and **NMC Login** window appears.

5. On the **NMC Login** window:

   a. For the username, type `administrator`.

   b. For the password, type the password that was used for the Administrator user of the Authentication service.

   c. Click **OK**.

6. On the **License Agreement** window, review the license text, and then click **Accept**.

7. In the **Set NetWorker License Manager Server Name** window:

   a. Type the hostname of the License Manager server. If you did not install the License Manager software, leave this field blank.

   b. Click **Next**.

8. In the **Set Database Backup Server** window:

   a. In the **NetWorker Server** field, type the hostname of the NetWorker server.

   b. In the **Client name** field, type the hostname of the NMC server.

   c. Check the checkbox for **Create client resource on this server**.

      This step ensures that a client resource is created to backup the Management Console database.

   d. Click **Next**.

9. In the **Add NetWorker Servers** window:

   a. In the **NetWorker Servers** field, type the hostname of each NetWorker server in the environment that is required to be managed. Add one hostname per line.

      The host appears in the **Enterprise** section of the Console.

   b. Click **Finish**.

   The NMC GUI opens.

10. Close the **Getting Started** window.

11. To start using the NetWorker software, click **Enterprise** from the top level toolbar.

    In the left navigation pane, the top level object **Enterprise** displays. Underneath the navigation tree, each NetWorker server hostname which was typed earlier in the window appears.

12. Click the hostname of the NetWorker server.

    On the right side pane, **Host: Server_Name** and **Managed Applications** appear. The NetWorker Administration GUI launches.

Configuring NetWorker device and client resource

Perform the following steps to configure NetWorker device and Client resources.

Procedure

1. Create, and then configure the NetWoker server's device resources.

   To recover data by using a stand-alone device, ensure that a resource for the stand-alone device exists. The directory path differs for Linux and Windows:

   - For Linux: `/nsr/res`
   - For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

   If a resource for the standalone device does not exist, create it using the NetWorker Administration program.

2. In the NetWorker Administration program, open the NetWorker server's Client resource, and then verify that the **Aliases** attribute in the **Preferences** tab contains the correct information. For example, aliases for a computer that is named Kingdome might be:

   `Kingdome`

   `kingdome.seattle.washington.com`

3. Set the NetWorker retention policy to a decade.

   The retention policy is one month by default. This enables the recovery of all the server's records.

   Note

   If the NetWorker server's browse and retention policies is not reset, any of the server's records that are more than one month old will be discarded.

4. If you are using the NetWorker Administration program:

   a. Configure the Client resource for the NetWorker server. Set the browse and retention policies to a time value that covers the oldest save sets being used for the recovery.

      This allows you to recover all of NetWorker server's records with the `nsrdr` command.

      Note

      If the retention policy set for the client instance of the NetWorker server is long enough to cover all of the save sets, all of the NetWorker server's records are recovered. However, if the retention policy set for the client is not changed and save sets exist for the NetWorker server that have a retention policy greater than one month, they are discarded because the default browse policy is one month.

5. If you are recovering data using an autochanger, perform the following steps.

   a. Ensure that an autochanger resource exists.

      The directory differs for Linux and Windows.

- For Linux: `/nsr/res`
- For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

If the autochanger resource does not exist, create it using the **NetWorker Console Administration** interface. The *EMC NetWorker Administration Guide* provides details about this interface.

b. Reset the autochanger by using the `nsrjb -vHE` command.

This command resets the autochanger, ejects backup volumes, reinitializes the element status, and checks each slot for a volume.

- If the autochanger does not support the `-E` option, initialize the element status by using the `ielem` command.
- Inventory the autochanger by using the `nsrjb -I` command. This helps to determine whether the volumes required to recover the bootstrap are located inside the autochanger.

Note

None of these volumes are in the media database. The contents of the tape cannot be viewed through NMC and the volume name comes up as **-***.

Recovering critical NetWorker server databases

Protecting a NetWorker server including its critical databases requires careful planning and preparation. The recovery methods that are described in this section may not work if the NetWorker server is not adequately protected. Information about protecting a NetWorker server is provided in the *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide*.

Note

Use the `nsrdr` command to recover NetWorker 9.0.1 databases only. To perform a roll back of the NetWorker server to an earlier version of the NetWorker software, contact EMC Customer Support.

The databases that are critical to the recovery of a NetWorker server include the bootstrap and the client file indexes.

A bootstrap includes the:

- Media database—Which contains the volume location of each save set.
- Resource files—Which contains all the resources, such as NetWorker clients and backup groups, that are defined on the NetWorker server.
- The NetWorker Authentication Service database.
- Lockboxes.

Note

The lockbox folder in the resource directory stores confidential information, for example, Oracle client passwords and the DD Boost password, in an encrypted format. NetWorker uses this information to perform backup and recovery operations.

The client file indexes include tracking information for each file that belongs to a client's save sets. There is one client file index for each NetWorker client.

The `nsrdr` command line program simplifies the recovery of the media bootstrap, and optionally the client file indexes for a NetWorker server. Previous releases of NetWorker required the `mmrecov` command to recover the media database and resource files, and the `nsrck` command to recover client file indexes. UNIX man page and the *EMC NetWorker Command Reference Guide* provides detailed information about the `nsrdr` command.

Use the procedures in this section to recover lost or corrupted bootstrap or client file indexes (CFIs). If the server databases are not corrupted and you only want to restore expired save set entries into the client file index or the media database, use the procedures to recover expired save sets. Save sets are removed from the client file index when their browse policy time has expired. Save set entries are removed from the media database when their retention policy time expires.

The `nsrdr` command is flexible. You can run the `nsrdr` program in fully interactive mode and respond to questions or you can run the program silently with command line options. You can recover the media database, resource files, and all CFIs in one operation, or recover just one item by itself. You can recover individual CFIs or all CFIs for all clients in one operation.

To help troubleshoot issues with the wizard, the `nsrdr` command logs messages to the following locations:

- On UNIX, `/nsr/logs/nsrdr.log`
- On Windows, *`NetWorker_install_path`*`\nsr\logs\nsrdr.log`

Prerequisites to recover the NetWorker server databases

Depending on the state of your NetWorker server, you might require some preparation before you can recover the bootstrap and client file indexes.

There are two main scenarios to consider:

- Scenario 1: Lost bootstrap or client file indexes—In this scenario you just need to recover the NetWorker server bootstrap or client file indexes because they have been lost or deleted. The NetWorker server software, operating system, and hardware are intact but you notice that some bootstrap data such as the media database or NetWorker server resources are missing or incomplete. Additionally, you may notice that some clients are no longer browsable for recovery even though they have not exceeded their browse retention time policies; this indicates missing or incomplete client file indexes.
- Scenario 2: Disaster recovery—In this scenario, the NetWorker server host has suffered some damage, such as a disk or power supply failure, and the base operating system might have been removed or corrupted. Perform the following steps before you recover the databases:
  - Replace the damaged hardware on the system, as required. Use the same hardware that was on the system at the time of the database backup.
  - Install the OS software and patches. Use the same software versions that were on the system at the time of the database backup.
  - Install the NetWorker server software. Use the same software version that was on the system at the time of the database backup.

Note

Follow the practices described in the *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide* to reduce the likelihood of encountering a disaster recovery scenario and to maximize the likelihood of successfully recovering from a disaster.

The EMC NetWorker SolVe Desktop also includes information about NetWorker recoveries. To access the EMC NetWorker SolVe Desktop, log on to https://support.emc.com/ and search for EMC NetWorker SolVe Desktop. You must have a service agreement to use this site.

Is the NetWorker server installed?

If you need to reinstall the NetWorker server software, refer to the EMC NetWorker Installation Guide.

Is the bootstrap report available?

Bootstrap report information includes the following:

- Bootstrap SSID (Save Set Identification Number).
- Volume name containing the bootstrap.
- File-number and record-number of the tape media (if used) where the bootstrap information starts.

Use one of the following methods to obtain information about the bootstrap:

- Review the `policy_notifications.log` file, or the target destination that you configured for the policy resource notification. The **Server backup Action report** section contains information about the bootstrap and client file index backups. For example:

```
---Server backup Action report---
Policy name:Server Protection
Workflow name:Server backup
Action name:Server db backup
Action status:succeeded
Action start time:10/27/15 07:52:34
Action duration:0 hours 0 minutes 34 seconds
--- Successful Server backup Save Sets ---
4079980473/1445957561 bu-iddnwserver: index:edward-sol10x64
level=1, 1 KB, 0 files
3979317182/1445957566 bu-iddnwserver: index:edward-w2k12r2
level=1, 1 KB, 2 files
3945762750/1445957566 bu-iddnwserver: index:bu-iddnwserver
level=1, 35 MB, 43 files
3777990608/1445957584 bu-iddnwserver: bootstrap level=full,
752 KB, 224 files
--- Bootstrap backup report ---
date time level ssid file record volume
10/22/15 08:43:06 full 3609789450 0 0 DDclone.001
10/22/15 08:43:06 full 3609789450 0 0 bu-iddnwserver.001
10/22/15 10:00:30 full 3156809262 0 0 DDclone.001
10/22/15 10:00:30 full 3156809262 0 0 bu-iddnwserver.001
10/23/15 10:00:31 full 2351589295 0 0 DDclone.001
```

```
10/23/15 10:00:31 full 2351589295 0 0 bu-iddnwserver.002
10/24/15 10:00:30 full 1630255406 0 0 DDclone.001
10/24/15 10:00:30 full 1630255406 0 0 bu-iddnwserver.001
10/25/15 10:00:28 full 908921516 0 0 DDclone.001
10/25/15 10:00:28 full 908921516 0 0 bu-iddnwserver.002
10/26/15 10:00:30 full 204364846 0 0 DDclone.001
10/26/15 10:00:30 full 204364846 0 0 bu-iddnwserver.001
10/27/15 07:53:04 full 3777990608 0 0 bu-iddnwserver.002
```

In this example, the SSID/CloneID for the latest bootstrap backup is `3777990608/1445957584` on volume `bu-iddnwserver.002`. Policy notifications provides more information about the notification configurations that are available in the Policy, Workflow, and Action resources.

- If the media database is not lost and the volume list is available, use the `mminfo` command to obtain bootstrap information. For example, `mminfo -av -B -s` ***server_name***. Where *server_name* is the hostname of the NetWorker server.
- If the media database is lost, use the `scanner` command to scan the source device for the bootstrap backup. For example, **`scanner -B`** ***device_name***. Where *device_name* is the name of the device that contains the bootstrap backup.

Is a local device available?

The NetWorker server requires a local device resource to recover data from a bootstrap backup. In a disaster recovery situation, the resource database is lost, and you must recreate the local device to recover from the bootstrap save set.

When you recreate the device, keep the following considerations in mind:

- Do not relabel the volume when you create the device. Relabeling a volume with bootstrap backups, or any other backups, renders the data unrecoverable.
- Additional requirements for disk based devices such as AFTD.
  - Do not allow the device wizard to label the disk volume. The **Label and Mount** option on the wizard's **Device Label and Mount** window has this option selected by default. Uncheck the **Label and Mount** option.
  - Specify the local path to the AFTD volume in the device wizard **Select Storage Node** window. Ensure that this is the same path on which the bootstrap data is stored.

Is the bootstrap on an Atmos cloud device?

If the bootstrap is on a Atmos loud device, review the following information.

- If the bootstrap is on a cloud device and the cloud Device resource has been lost, re-create a cloud Device resource.
- Determine the name of the volume that contains the bootstrap. If the original server is not available or the bootstrap report is lost and you do not know the cloud volume name, you can obtain it by checking the Atmos server. The volume name can be found in the following location on the Atmos server:

  `/networker/datazone-id/volumes/volume_name`
- Determine the datazone ID of the NetWorker server that was used for the bootstrap backup. If the original server is not available, the datazone ID can be found on the Atmos server in the following location:

  `/networker/datazone-id/volumes/volume_name`

To locate the datazone ID of the NetWorker server if it is not available complete the following steps:

1. From the NetWorker Server **Administration** window, select **View** > **Diagnostic Mode**.
2. Right-click the NetWorker server name in the left pane and select **Properties**.
3. In the **System Summary** tab of the **NetWorker Server Properties** dialog box, record the value in the **Datazone id** field.

Is the bootstrap on a remote device?

NetWorker supports cloning the bootstrap backup to a local or remote device. NetWorker does not support bootstrap recoveries from a remote device. To recover the bootstrap from a cloned save set on a remote device, you must clone the save set from the remote device to a device that is local to the NetWorker server.

To recover from a clone copy of a bootstrap backup that resides on a remote device, including a CloudBoost device, perform the following steps:

Procedure

1. Re-create the device that contains the cloned bootstrap save set on the NetWorker server.

   Note

   Do not label the device.

2. Create a new local device on the NetWorker server.

   Note

   To prevent data loss, it is recommended that you create a new AFTD device on the NetWorker server, to which you can recover the bootstrap data.

3. Re-populate the media database with information about the cloned bootstrap save set by performing the following steps:

   a. Determine the SSID of the save set by using the `scanner` command.

      For example,
      `scanner -B` ***`device_name`***

      where *device_name* is the name of the Cloud Boost device, for example,
      `rd=bu-idd-cloudboost.iddlab.local:base/bkup`

   b. Re-populate the media database with information about the cloned save set, by using the `scanner` command.

      For example, `scanner -m` **`-S`** ***`SSID/CloneID device_name`***

4. Mount the DD Cloud Tier device.
5. Determine the SSID/CloneID of the bootstrap backup on the DD Cloud Tier device, by using the `mminfo -B` command.
6. Clone the bootstrap save set from the DD Cloud Tier device to the Data Domain device, by using the `nsrclone` command or create a save set group.

7. Determine the SSID/CloneID of the bootstrap backup on the Data Domain device, by using the `mminfo -B` command.
8. Recover the bootstrap backup from the local device, by using the `nsrdr` command.

Consider the recovery options

The `nsrdr` command is flexible and can be run in a variety of ways. However, the major options to consider before running the `nsrd` command are outlined in this section. For a complete list of advanced options, refer to Options for running the nsrdr command on page 61.

Do you need to recover all client file indexes?

Recovering all client file indexes can take a long time. If you only need to recover the client file indexes for a limited set of clients, use the `nsrdr -I` option, for example:

```
nsrdr -c -I clientA clientB clientD
```

Options for running the nsrdr command on page 61 provides more options for recovering specific client file indexes with the `nsrdr` command.

Were save sets backed up after the last bootstrap backup?

If save sets were backed up after the last bootstrap backup, then these backup records might be overwritten after the bootstrap is recovered. This situation can only occur when a manual backup is taken. A manual backup does not trigger a bootstrap backup immediately, therefore the manual backup are not recorded in the bootstrap until the next scheduled backup. To protect against losing save sets that were backed up after the last bootstrap backup, use the `nsrdr -N` or `nsrdr -N -F` options.

For example:

- Use the `nsrdr -N -F` command in a NetWorker datazone that contains tape devices, file type devices, and AFTDs when you only want to protect file type devices and AFTDs against loss of save sets.
- Use the `nsrdr -N` command in a NetWorker datazone that contains tape devices, file type devices, and AFTDs when you want to protect tape devices, file type devices, and AFTDs against loss of save sets.

If you know that manual backups were not taken after the last bootstrap backup or you are not concerned about losing these backups, do not use the `-N` or `-N -F` options. These options can increase the time and complexity of the recovery considerably.

Recovering critical NetWorker server databases

Use the `nsrdr` command to recover the NetWorker server databases from a command prompt.

The `nsrdr` command line options that you use to recover the database depend on the type of devices that are used in the datazone, and how you want to perform the recovery.

Setting nsrdr tuning parameters

You can specify the following tuning parameters for `nsrdr`, the NetWorker server disaster recovery command.

- You can specify the path to the NetWorker services, such as `nsrdr`, if the default path was not used during the installation.

  - The default path on Linux is `/etc/init.d/networker`.
  - The default path on Windows is `C:\Program Files\EMC NetWorker\nsr\bin`.
- The number of parallel threads that can be spawned when recovering client file indexes (CFIs) for multiple NetWorker clients. The default value is 5, which means that up to five parallel threads are spawned to recover CFIs. If you are recovering many client CFIs, increasing this value can shorten the disaster recovery time.

If you do specify any of these parameters, they must be set up before running the command. You can set up these parameters by creating an ASCII plain text file, naming it `nsrdr.conf`, typing the parameter values in the file, and placing the file under the debug folder of the NetWorker installation path. Use the following procedure to set the tuning parameters:

Procedure

1. Create a text file, and then give it the name `nsrdr.conf`.

   Note

   Some text editors append `.txt` to the end of the file name. If this occurs, remove the `.txt` extension so that the file name is `nsrdr.conf`.

2. To specify a non-default path to the NetWorker services, add the following entry:
   - On Linux:

     `NSRDR_SERVICES_PATH = /non_default_path/nsr`
   - On Windows:

     `NSRDR_SERVICES_PATH = drive:\non_default_path\EMC NetWorker\nsr\bin`

     where *non_default_path* is the path to the NetWorker services.

3. To specify the number of parallel threads that can be spawned when recovering CFIs for multiple clients, add the following entry:

   `NSRDR_NUM_THREADS = number`

   where *number* is a value that is greater than 1.

   Note

   If a value of zero (0) or a negative value is typed, a default value of 5 is automatically assigned instead.

   Ensure that a space is added before and after the equals (=) sign. If you specify both tuning parameters, ensure that each value is typed on a separate line.

4. Save the `nsrdr.conf` file as a plain text file, and then place it in the following directory:
   - On Linux: `/nsr/debug/`
   - On Windows: `NW_install_path\nsr\debug`

The tuning parameters take effect the next time the `nsrdr` command is run.

Using nsrdr to perform a disaster recovery

Before you begin

Before you perform a disaster recovery of the NetWorker server databases, ensure that the authentication database directory does not contain a recovered database file that is more recent than the bootstrap that you want to recover. The name of the recovered database file is in the following format: `authcdb.h2.db.`*`timestamp`*.

The steps in this section assume that you are running the NetWorker server disaster recovery command, `nsrdr`, in fully interactive mode. EMC recommends that you use the `nsrdr` command to perform a disaster recovery of the NetWorker server. To avoid data loss, EMC recommends using the `-N` option. Options for running the nsrdr command provides information on additional command line options that are available for use with the `nsrdr` command.

Procedure

1. To connect to the NetWorker server and unmount all the volumes including tape, file type, advanced file type devices, and cloud volumes, use NMC.
   a. In the **NetWorker Administration** window, click **Devices**.
   b. Select **Devices** in the navigation tree.

      The **Devices** detail table appears.
   c. Right-click a device, and then select **Unmount**.
2. Enable the common device interface (CDI) attribute.

   Note

   NDMP and optical devices do not support CDI.

   a. From the **View** menu, select **Diagnostic Mode**.
   b. Select **Devices** in the left navigation pane.

      The **Devices** detail table appears.
   c. In the **Devices** table, double-click a device.
   d. Select the **Advanced** tab.
   e. In the **Device Configuration** area, locate the CDI settings and select **SCSI commands**.
   f. Stop, and then restart the NetWorker server services/daemons.
3. Log in to the NetWorker server as root for a Linux host, or Administrator on a Windows host.
4. To prevent the possibility of overwriting manual backups that were taken after the last bootstrap backup, type:

   ```
   nsrdr -N
   ```

   When you use `-N` option, consider the following:

   - For AFTD devices, you can still write to the disk, however, recover space operations are suspended until the **Scan Needed** flag is removed. A recover space operation clears the disk device of any save sets that do not have a corresponding entry in the media database.

- For tape devices, when you try to write data to a tape-based device that has newer save sets than what is recorded in the media database, a message displays that explains how to update the media database to avoid the possibility of overwriting the newer data.

If you are sure that backups were not done after the last bootstrap backup or you do not need to recover that data, omit the options.

5. At the `Do you want to continue?` prompt, type `Y` for yes.
6. (Optional) If you have more than one configured device, the `Configured device` output appears with a list of configured devices. At the `What is the name of the device that you plan to use?` prompt, specify the number that is assigned to the device that contains the NetWorker server bootstrap save set.
7. At the `Enter the latest bootstrap save set id` prompt, type the save set ID of the latest bootstrap.

   If you do not know the save set ID of the latest bootstrap, leave this entry blank, and then press **Enter**, and perform the following steps:

   a. At the `Do you want to scan for bootstrap save set ID on the device?` prompt, type `Y` for Yes.

   Note

   The option to scan for a bootstrap save set ID is not supported for non-English locales. In this case, use the `scanner` command to find the bootstrap ID.

   b. At the `Do you want to recover the bootstrap save set with the selected ID?` prompt, type `Y` for yes, to recover the bootstrap save set.

   Note

   If you are recovering from a cloud device, you are prompted to type the name of the cloud volume that contains the bootstrap save set. If you are recovering from a cloud device, you are prompted to type the datazone ID of the NetWorker server. Ensure that the datazone ID is for the NetWorker server datazone used to back up the bootstrap.

   The `scanner` program is run and the bootstrap save set is recovered. Data from the bootstrap save set replaces the media database.
8. At the `Do you want to replace the existing NetWorker resource configuration database folder, res, with the folder being recovered?`, type `Y` for yes.

   The recover process performs the following tasks:

   - The recovered resource database is saved to a temporary folder named `res.R`.
   - The NetWorker server services are shut down because `nsrdr` cannot overwrite the resource database while these services are running.
   - The recovery process replaces the existing resource database folder with the recovered resource database. The replaced folder is renamed to `res.`*`timestamp`*.

9. At the `Do you want to replace the existing NetWorker Authentication Service database file, authcdb.h2.db, with the recovered database file?`, type **Y** for yes.
10. When prompted to continue, type **Y** for yes.

    The NetWorker server services are restarted after the authentication database is replaced with the recovered authentication database. The replaced file is renamed to `authcdb.h2.db.`*`timestamp`*.
11. At the `Do you want to recover the client file indexes?`, perform one of the following tasks:
    - To recover all the client file indexes, type **Y** for yes. Type **Y** for yes again when asked to confirm the choice. The disaster recovery operation recovers a client file index for each NetWorker client that was backed up including the client file index for the NetWorker server. The disaster recovery operation completes after all the client file indexes are recovered.
    - To recover the client file index for selected clients only:
      a. Type **N** for no.
      The disaster recovery operation completes.
      b. Re-type the `nsrdr` command with the `-c -I` options, and then provide a list of client names with each name separated by a space, for example:

      ```
      nsrdr -c -I clientA clientB clientD
      ```

      The `nsrdr` command skips the bootstrap recovery and you are prompted to complete the recovery of the specified client file indexes.

      The disaster recovery operation completes after all the client file indexes that you specified are recovered.
12. Open the **Administration** window in NMC, and then check that all the NetWorker Server resources appear as expected.
    a. Click the **Protection** icon, and then check that all resources appear as they were before recovery.
    b. Click the **Devices** icon, and then check that all resources appear as they were before recovery.
    c. Click the **Media** icon, and then check that all resources appear as they were before recovery.
    d. Select **Tape Volumes** or **Disk Volumes** from the **Media** screen.
    e. Check the mode status of the volume, **Tape Volumes**, which appears in the window on the right. All volumes should have the same mode that existed before the recovery. All devices that are written to should be in the appendable mode.

Remove the Scan Needed flag from volumes

When you use the `nsrdr` command to set the Scan Needed flag, all the recovered devices are set to the Scan Needed mode (displayed as `Mode = Scan Needed`).

Review the following sections for instructions on how to remove the Scan Needed flag from AFTD, Cloud, and Tape devices.

Removing the Scan Needed flag from AFTDs

If you used the `nsrdr` command to set the scan needed option, all the volumes that are appendable (non read-only) and are in the recovered media database are set to

Scan Needed. If you suspect that the volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the recovered media database and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag from the volume.

For AFTD volumes that you suspect may have save sets that were saved after the last bootstrap backup, perform the following steps:

Procedure

1. If you do not know the AFTD device name that corresponds to the AFTD volume, use the `nsrmm` command with the `-C` option:

   ```
   nsrmm -C
   ```

   Output similar to the following is displayed:

   ```
   32916:nsrmm: file disk volume_name mounted on device_name,
   write enabled
   ```

   where *device_name* is the device that corresponds to the AFTD *volume_name*.

2. Use the `scanner` command to repopulate the CFI and media database with the save set information:

   ```
   scanner -i device_name
   ```

   where *device_name* is the AFTD device name not the AFTD volume name.

3. Unmount the device, remove the Scan Needed status, and then remount the device. When you remove the Scan Needed status, NetWorker enables recover space operations for the device:

   a. To unmount the AFTD volume, perform the following steps:

      a. Use NMC to connect to the NetWorker server. On the **Administration** window, select **Devices**, and then click **Devices** in the left panel.

      b. Identify the device in the right panel that you want to unmount. Note the volume that is associated with the device.

      c. Right-click the device, and then select **Unmount**.

      d. Repeat for all devices that require the Scan Needed status to be removed.

   b. To remove the Scan Needed status, perform the following steps:

      a. On the **Administration** window, select **Media**, and then click **Disk Volumes** in the left panel.

b. Identify the volume in the right panel that is associated with the device in the previous step.

c. Right-click the volume, and then select **Mark Scan Needed**.

d. Select **Scan is NOT needed**, and then click **OK**.

e. Repeat for all volumes that require the Scan Needed status to be removed.

c. To mount the AFTD volume, perform the following steps:

a. On the **Administration** window, select the **Devices**, and then click **Devices** in the left panel.

b. Identify the device in the right panel that you want to mount.

c. Right-click the device, and then select **Mount**.

d. Repeat for all devices that were unmounted.

e. Ensure that all devices are mounted and that the Scan Needed status has been removed for the associated volumes.

Results

You can now use normal recovery procedures to recover application and user data on the NetWorker server.

NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or an NMM protected virtual DAG Exchange server, the `nsrdr.log` file contains false error messages that are related to the CFI recovery of the underlying physical hosts. Using an NMM protected virtual DAG Exchange server as an example, a messages similar to the following appears:

```
9348:nsrck: The index recovery for 'EXCH2010-2.vll1.local'
failed.9431:nsrck: can't find index backups for
'EXCH2010-2.vll1.local' on server 'sa-wq.vll1.local'
```

You can ignore error messages that are related to the physical hosts, because NetWorker does not backup the underlying physical host in a virtual environment.

Removing the Scan Needed flag from Cloud devices

If you used the `nsrdr` command to set the scan needed option, all the volumes that are appendable (non read-only) and are in the recovered media database are set to Scan Needed. If you suspect that the volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the recovered media database and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag from the volume.

For Cloud volumes that you suspect may have save sets that were saved after the last bootstrap backup, perform the following steps:

Procedure

1. If you do not know the Cloud device name that corresponds to the Cloud volume, use the `nsrmm` command with the `-C` option:

   ```
   nsrmm -C
   ```

   Output similar to the following is displayed:

   ```
   32916:nsrmm: file disk volume_name mounted on device_name,
   write enabled
   ```

   where *device_name* is the device that corresponds to the Cloud *volume_name*.

2. To repopulate the CFI and media database with the save set information, use the `scanner` command:

   ```
   scanner -i -V cloud_volume -Z datazone_ID cloud_device
   ```

   where *datazone_ID* is the NetWorker server datazone ID if it is in a different datazone than the cloud device.

Results

You can now use normal recovery procedures to recover application and user data on the NetWorker server.

NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or an NMM protected virtual DAG Exchange server, the `nsrdr.log` file contains false error messages that are related to the CFI recovery of the underlying physical hosts. Using an NMM protected virtual DAG Exchange server as an example, a messages similar to the following appears:

```
9348:nsrck: The index recovery for 'EXCH2010-2.vll1.local'
failed.9431:nsrck: can't find index backups for
'EXCH2010-2.vll1.local' on server 'sa-wq.vll1.local'
```

You can ignore error messages that are related to the physical hosts, because NetWorker does not backup the underlying physical host in a virtual environment.

Removing the Scan Needed flag from tape devices

If you used the `nsrdr` command to set the scan needed option, all the volumes that are appendable (non read-only) and are in the recovered media database are set to Scan Needed. If you suspect that the volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the

recovered media database and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag from the volume.

If you used the `-N` option with the `nsrdr` command and you try to mount a tape volume that has save sets that are newer than what is recorded in the media database, a message similar to the following appears:

```
            nw_server nsrd media info: Volume volume_name has save
sets unknown to media database. Last known file number in media
database is ### and last known record number is ###. Volume
volume_name must be scanned; consider scanning from last known file
and record numbers.
```

For tape volumes that you suspect may have save sets that were saved after the last bootstrap backup, perform the following steps:

Procedure

1. Make a note of the file number and record number that is displayed in the message.
2. To repopulate the CFI and media database with the save set information, use the scanner command:

   `scanner -f` ***file*** `-r` ***record*** `-i` ***device***

3. To remove the Scan Needed flag from the tape volume, use the `nsrmm` command:

   `nsrmm -o notscan` ***volume_name***

Results

You can now use normal recovery procedures to recover application and user data on the NetWorker server.

NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or an NMM protected virtual DAG Exchange server, the `nsrdr.log` file contains false error messages that are related to the CFI recovery of the underlying physical hosts. Using an NMM protected virtual DAG Exchange server as an example, a messages similar to the following appears:

```
9348:nsrck: The index recovery for 'EXCH2010-2.vll1.local'
failed.9431:nsrck: can't find index backups for
'EXCH2010-2.vll1.local' on server 'sa-wq.vll1.local'
```

You can ignore error messages that are related to the physical hosts, because NetWorker does not backup the underlying physical host in a virtual environment.

Options for running the nsrdr command

You can run the NetWorker server disaster recovery wizard command (`nsrdr`) with various command line options instead of running the wizard in fully interactive mode. The following table includes a brief description of the `nsrdr` command line options. For a complete description of the `nsrdr` command and its options, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

Table 4 Command line options for the nsrdr command

Option	Description
`-a`	Runs the command line wizard in non-interactive mode. At a minimum, the `-B` and `-d` options must be specified with this command. Be sure to specify a valid bootstrap ID with the `-B` option when running this command in non-interactive mode. Otherwise, the wizard exits as though it was canceled without providing a descriptive error message.
`-B` *bootstrap_ID*	The save set ID of the bootstrap to be recovered.
`-d` *device_name*	The device from which to recover the bootstrap.
`-K`	Use the original resource files instead of the recovered resource files.
`-v`	Verbose mode. Generates troubleshoot information.
`-q`	Quiet mode. Display only error messages.
`-c`	Recover client file indexes only. If specified with the `-a` option, you must also specify the `-I` option.
`-I`	Specify which CFIs (client file indexes) to recover. Each client name must be typed at

Table 4 Command line options for the nsrdr command (continued)

Option	Description
`-I` *client1 client2...*	the command prompt and separated with a space. If no client names are specified, all client file indexes are recovered. When the `-I` option is specified, ensure that it is the last option in the command string because any entries after the `-I` option are interpreted as client names.
`-f` *path/file_name*	Specify which CFIs to recover by using an ASCII text file. Place each client name on a separate line in the file. Must be used with the `-I` option. Ensure that each client name is typed correctly because there is no validation of client names.
`-t` *date/time*	Recover CFIs from the specified date or date and time. You must type a date and optionally, a time, format that is accepted by the `nsr_getdate` program. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about `nsr_getdate`.
`-N`	If tape volumes have save sets that are newer than what is recorded in the recovered bootstrap backup, they are marked as Scan Needed, to prevent the possibility of losing backed up data. For AFTD devices, this option prevents NetWorker from running recover space operations until you remove the Scan Needed flag. A recover space operation clears the disk device of any save sets that do not have a corresponding entry in the media database.
`-F`	This option sets the Scan Needed flag on File type devices, AFTD devices, and Cloud devices only. The `nsrdr` command will not mark tape volumes as Scan Needed. This option requires the `-N` option.

Examples

The following examples depict some common `nsrdr` commands.

- To recover the bootstrap data and selected client file indexes only, type:
  `nsrdr -I` ***`client1 client2 client3`***

  where each client name is separated with a space.
- To recover the bootstrap data and selected client file indexes by using an input file, type:
  `nsrdr -f` ***`path\file_name`*** `-I`

where *file_name* is an ASCII text file with one client name on each line.

- To skip the bootstrap recovery and recover selected client file indexes by using an input file, type:
  `nsrdr -c -f path\file_name -I`

  where *file_name* is an ASCII text file with one client name on each line.
- To skip the recovery of bootstrap data and recover all client file indexes, type:
  `nsrdr -c -I`
- To skip the recovery of bootstrap data and recover selected client file indexes, type:
  `nsrdr -c -I client1 client2`
- To skip the recovery of bootstrap data and recover selected client file indexes from a specified date, type:
  `nsrdr -c -t date/time -I client1 client2`

  where the *date/time* is the date and/or time from which the client file indexes are recovered. The date/time format is specified in *MM/DD/YYYY* format or any date and time accepted by the `nsr_getdate` command. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about the`nsr_getdate` command.
- To run `nsrdr` in non-interactive mode and to recover the bootstrap data and all client file indexes, type:
  `nsrdr -a -B bootstrap_ID -d device -I`

Recovering the NetWorker server application and user data

Perform the following steps to recover the application and user data that was on NetWorker server.

Procedure

1. Log in as root.
2. Load and inventory the devices.

   This ensures that the NetWorker server can recognize the location of each volume.

   Note

   If you load a clone volume, either delete the original volume from the media database or mark the desired save set as suspect in the media database. If you are using the clone volume, it is used for the remainder of the recovery process.

3. Run the `nwrecover` program.
4. Mark all the directories or files to be recovered.

   Note

   Overwriting operating system files may cause unpredictable results.

5. Click **Start** to begin the recovery.

Note

The bootstrap backup restores the `res` directory, which in turn contains the `nsrla` database directory. The `nsrla` database contains the setting for directed recoveries, so this setting should be preserved with the bootstrap restore. More information about setting the directed recover option on a NetWorker client is provided in the *EMC NetWorker Administration Guide*.

Avoiding slow startups due to hostname resolution issues

Hostname resolution issues can cause the NetWorker server to become unresponsive or start very slowly. If either of the following situations apply to the environment, consider the workaround included in this section.

- The NetWorker server uses DNS, but the DNS server is not available.
- The NetWorker server cannot resolve all of its NetWorker client hosts.

Workaround for hostname resolutions issues

Perform the following steps if the NetWorker server starts slowly or becomes unresponsive due to hostname resolution issues.

Procedure

1. Disable DNS lookup for the host being recovered, and then use the local hosts file on the NetWorker server for the hostname resolution.
   - For Windows, the hosts file is located in `C:\Windows\System32\Drivers\etc\`.
   - For Linux, the file is located in `/etc`.

   Modify the `/etc/nsswitch.conf` file to look up the hosts files, before DNS, as a hostname resolution method.

2. Ensure that the hosts file is set up so that the full qualified domain name (FQDN) is first and is followed by the corresponding shortname.

   Note

   If the NetWorker server's client name was originally the shortname, then the shortname must be first, followed by the longname. For example, 10.10.2.5 host.emc.com.

3. When the DNS server is available, re-enable DNS lookup.

Making changes to the etc/nsswitch.conf file

Perform the following steps to edit the `etc/nsswitch.conf` file:

Procedure

1. If the hosts line in the `/etc/nsswitch.conf` file contains the following:

   ```
   hosts: dns files
   ```

   This indicates that the DNS feature is used first. If the DNS servers are not available or cannot resolve the address, then modify the hosts line to use the `/etc/hosts` file for hostname resolution. Change the hosts line to the following:

```
hosts: files
```

2. On the NetWorker server, populate the local hosts file with the known client's valid IP address. For those clients whose IP address is unknown, use 127.0.0.1.

   127.0.0.1 is the standard IP address used for a loopback network connection. When the NetWorker server comes up, a DNS check is performed for each client. For clients that are offline or not available, the server connects to 127.0.0.1 which immediately loops back to the same host. This approach helps the NetWorker server to become available faster instead of waiting to resolve all the clients DNS lookup.

3. When the DNS server is available, re-enable DNS lookup.

   Note

   This method for resolving the hostnames is preferred when the NetWorker server is recovered after a DNS server failure.

   When the NetWorker server is available, a valid client IP address must be updated in the local hosts file to perform a backup or recovery for the critical clients.

   When the DNS server is available and running, remove the client details from the local hosts file.

CHAPTER 6

NetWorker Client Disaster Recovery Procedures

This topic includes the following procedures.

- Performing a disaster recovery of a NetWorker client on Linux and UNIX.....94
- Performing an authoritative restore on Windows..... 97
- Performing a non-authoritative restore on Windows.....101
- Performing a bare metal recovery on Windows 102

Performing a disaster recovery of a NetWorker client on Linux and UNIX

Follow these steps to perform a disaster recovery of a NetWorker client on Linux or UNIX.

Planning notes and preparing for a disaster recovery

Back up important data on a scheduled basis. The more time and effort that is invested in incorporating, maintaining, and testing a backup solution, the better prepared you are if a disaster occurs.

Having the correct information handy in case a disaster occurs is a key element in recovering from a disaster as quickly as possible.

Gathering key information

Maintain accurate records for each hardware, software, network, device, and media component.

Hardware information

Maintain up-to-date information on computer hardware as follows:

- File system configuration
- Fully qualified domain names, IP addresses, and hostnames
- For Domain Name System (DNS) clients, maintain the DNS host's internet address and hostname
- Hard drive configuration
- Media device names
- Hardware vendor
- Configuration information for each piece of hardware, both active and inactive, within the organization or organizational site

Software information

Maintain up-to-date information on computer software as follows:

- Copies of the original operating system media and patches (and where they are located)
- Software enabler and authorization codes
- Software vendor contact information and contract number
- The operating system version and patches installed
- Operating system configuration
- Emergency media that can be used to recover a computer if a disaster occurs
- NetWorker bootstrap information for each NetWorker server
- Kernel configuration and location
- Device drivers

- A list of any volume mount points

Prerequisites for recovering a NetWorker client or storage node

Before recovering a NetWorker client or storage node, perform the following steps.

Procedure

1. Verify that the same operating system as the source host is installed on the target host.
2. Verify that the NetWorker server is functioning and available on the network.
3. Obtain the following information:
   - NetWorker server hostname.
   - NetWorker client or storage node software version and patch level on the computer before the disaster occurred.
   - Link names to the NetWorker directories you must recover. An example of a typical link from a NetWorker directory to a user directory is `/nsr` to `/var/nsr`.

Downloading the NetWorker software and documentation

To obtain the latest NetWorker software and documentation, perform the following steps.

Procedure

1. Review the online NetWorker documentation, such as the *EMC NetWorker Administration Guide*, *EMC NetWorker Installation Guide*, and *EMC NetWorker Release Notes*, for the latest information.
2. Obtain the required NetWorker cumulative hotfix media kits that provide customers with the opportunity to install the latest version of NetWorker including important hotfixes. Cumulative builds are released approximately once a month and each build contain a rollup of the fixes in each previous build.

   If additional hotfixes are required in an environment where a cumulative build is installed, hotfixes can be generated for use with the latest cumulative version. The cumulative releases for specific NetWorker versions are available at http://support.emc.com.
3. Open the NetWorker Cumulative Hotfix document for details regarding fixes that are in each build, knowledge base articles that are related to the fixes in each build, and download instructions.

Replacing the hardware, reinstalling, and upgrading the operating system

To replace the hardware, reinstall, and upgrade the operating system, perform the following steps.

Procedure

1. Identify the defective or suspect hardware, and then replace the hardware as required.
2. Reinstall a minimum operating system from the installation media.
3. Install any patches or upgrade the operating system to the same level as before the disaster.

4. When using the LVM and the file systems of the root VolumeGroups are mounted, check which additional file systems outside of the root VolumeGroups are part of the backup.
5. If VolumeGroups are imported, use the same logical volumes that were used in the backup.
6. Ensure that all LVM device files in `/dev` are unique after the operating system installation.

Reinstalling NetWorker client

To reinstall the NetWorker client software, perform the following steps.

Procedure

1. Install the latest version of the NetWorker client or the same version as the one running on the NetWorker server. Installation instructions are provided in the *EMC NetWorker Installation Guide*.

   Note

   If you must update the client software, first recover the client to its original state and then perform the update.

2. Reinstall any NetWorker backup utility patches that were installed before the disaster.
3. Re-create any links to NetWorker directories.
4. (Optional) To perform a test recovery to ensure that the recovery process is functioning correctly, use the `recover` command.

Recovering NetWorker client application and user data

To recover the application and user data, perform the following steps.

Procedure

1. To determine which volumes contain the application and user data backups for this computer, use the `mminfo -avot` command on the NetWorker server.

   For example:

   ```
   mminfo -avot -c client_name
   mminfo -avot -c storage_node_name
   ```

   where:

   - *client_name* is the hostname of the computer whose application and user data is recovered.
   - *storage_node_name* is the hostname of the computer whose application and user data is recovered.

2. To recover the data (directories and files) on the NetWorker client, use the `recover` command.

   ```
   recover> add /<file system or folder name>
   recover> del /<file name or folder name> # Exclude the file from selected list
   recover> version # Check backup version and volume location
   ```

```
recover> force # Force overwrite

recover> recover # Start recover
```

Note

Overwriting operating system files might cause unpredictable results. To determine all the operating system files that should not be overwritten during a recovery, refer to the operating system documentation. Directories or files that must be marked for recovery are based on the applications that the server was running before the disaster.

3. Restart the host.

Performing a test backup and recovery

To test the NetWorker client backup and recovery process, perform the following steps.

Procedure

1. Perform a test manual backup by using the backup commands.
2. Perform a test recovery by using the recovery commands.

   The *EMC NetWorker Administration Guide* provides additional information on testing backup and recovery configurations.

Performing an authoritative restore on Windows

Use the following procedures to perform an authoritative restore on a NetWorker server, storage node, or client.

Active Directory restore information

Active Directory (AD) is the Windows directory service and the foundation for the Windows Distributed file system (DFS). AD is a component of the Windows system state on Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 and Windows Server 2012 R2 domain controllers.

A domain controller is a computer that stores directory data and manages user interactions with a domain, including login, authentication, directory searches, and access to other shared resources.

AD, identified by its writer name, NTDS, is backed up as part of the Windows Roles and Features save set, a collection of system components that depend on each other.

These components are backed up together and usually restored together, through a BMR.

Only three of these components lend themselves to being restored separately through an online restore: Active Directory, DFSR, and Cluster Services (Cluster Database).

Selecting a restore method

Consider the following when selecting a restore method:

- The circumstances and characteristics of the failure and the two major categories of failure from an AD perspective are AD data corruption and hardware failure. AD data corruption occurs when the directory contains corrupt data that replicated to

all domain controllers. Also, when a large portion of the AD hierarchy that is accidentally changed and this change was replicated to other domain controllers.

- The roles and functions of a failed NetWorker server.
- The types of restore for AD are non-authoritative restore and authoritative restore.

Authoritative restore

An authoritative restore is an extension of the non-authoritative restore process. Perform the steps of a non-authoritative restore before performing an authoritative restore.

The main difference is that an authoritative restore can increment the version number of the attributes of all objects in an entire directory, all objects in a sub tree, or an individual object (provided that it is a leaf object) to make it authoritative in the directory.

To perform an authoritative restore, start the domain controller in **Directory Services Restore Mode**.

Restore the smallest necessary unit from the last level incremental backup of the AD. For example, do not restore the entire directory to restore a single sub tree.

The online AD restore is done through one of the following:

- The NetWorker User application—Browse to and restore the `WINDOWS ROLES AND FEATURES\NTDS` save set.
- The `recover` command. For example:

```
recover -s <NetWorker server> -U -N "WINDOWS ROLES AND FEATURES
\NTDS"
```

Performing an authoritative AD restore on Windows Server 2008, 2008 R2, 2012, and 2012 R2

Authoritative restore recovers domain controllers to a specific point in time, and marks objects in Active Directory (AD) as being authoritative with respect to their replication partners.

Complete the following steps to perform an authoritative AD restore of the `WINDOWS ROLES AND FEATURES\NTDS` save set on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

Procedure

1. Start the host in Directory Services Restore Mode (DSRM):
   a. Choose the **Windows boot** option for the domain controller.
   b. To display a list of special boot options, press **F8**.
   c. Select **Directory Services Restore Mode** (Windows Domain Controllers Only) from the list of special boot options. When you restart in this mode, AD is taken offline.
2. Log in as the Domain Administrator.
3. Recover the `WINDOWS ROLES AND FEATURES\NTDS` save set using one of the following methods:
   - To start the operation from the command prompt, type the following command:

```
recover -s <NetWorker server> -N "WINDOWS ROLES AND FEATURES
\NTDS"
```

- To start the operation from the NetWorker User Recover GUI, browse to and mark the `WINDOWS ROLES AND FEATURES\NTDS` save set, and then click **Start**.

4. When the restore completes, verify that the operation was successful.
5. Run the Windows `ntdsutil.exe` command line utility as described in Running the ntdsutil.exe command line utility on page 99.

Running the ntdsutil.exe command line utility

Use the following procedure to run the `ntdsutil.exe` command line utility.

Before you begin

To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

Procedure

1. From the **ntdsutil** prompt, run the following commands:

Command	Description
`activate instance ntds`	Sets NTDS or a specific AD LDS instance as the active instance.
`authoritative restore`	Authoritatively restores the Active Directory database or AD LDS instance.

For example:

```
NTDSUTIL: activate instance ntds

NTDSUTIL: authoritative restore
```

Figure 5 Administrator Command Prompt - ntdsutil

2. To perform an authoritative restore, use the following steps:
   a. To restore AD objects, from the authoritative prompt, type `restore object DN`. This command marks object percentages as authoritative. This command also generates a text file that contains the distinguished name of the restored object, and an LDIF file that can be used to restore back-links for objects that are being authoritatively restored. Type the following command:

```
authoritative restore: restore object DN
```

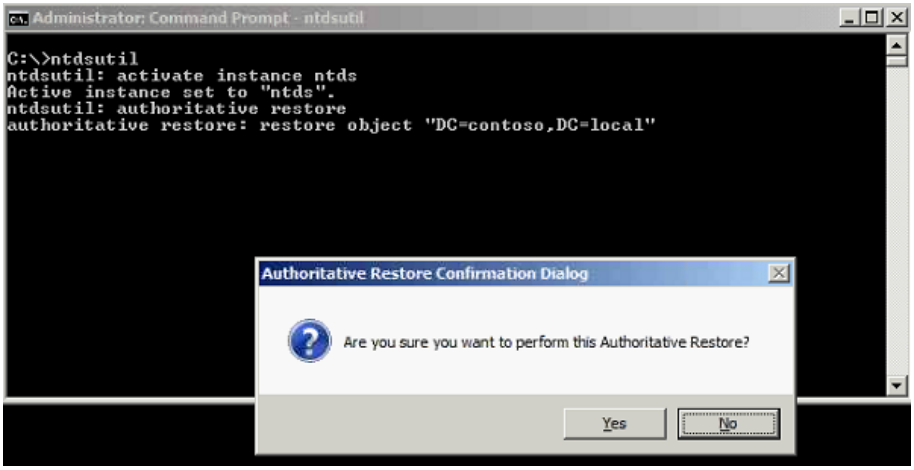
where *DN* is the distinguished name of the object to be restored.

For example:

```
restore object "DN=contoso ,DN=local"
```

This command restores everything under `contoso.local`. A confirmation dialog box appears.

Figure 6 Authoritative Restore Confirmation dialog box



b. Click **Yes** when prompted to continue the authoritative restore.

c. To restore child objects, from the authoritative prompt, type the following **`restore subtree DN`** command:

```
authoritative restore: restore subtree DN
```

where *DN* is the distinguished name of the subtree/child objects to be restored.

This command marks the subtree percentages (and all children of the subtree) as authoritative. This command also generates a file that contains the distinguished names of the restored object, and an LDIF file that can be used to restore back-links for objects that are being authoritatively restored. For example, group memberships of users.

3. Type **`quit`** to exit each prompt.
4. Restart the domain controller in Normal Mode.

Restart required after recovery operation

Newly recovered NetWorker client computers running Windows Server 2012 R2 can require an extra restart to restore access to application icons, previously viewable on the desktop.

Checking authoritative restore results

To check authoritative restore results, perform the following tasks.

Procedure

1. Open the Active Directory Users and Computers MMC snap-in.

2. If the authoritative restore was successful, the following settings appear on both `node_a` and `node_b` after restart and a complete replication cycle:
   - The modified user description has the original description.
   - The deleted user is present again.
   - The users that were added after the backup are still present.

Performing a non-authoritative restore on Windows

Use the following procedures to perform a non-authoritative restore on a NetWorker server, storage node, or client.

Active Directory restore information

Active Directory (AD) is the Windows directory service and the foundation for the Windows Distributed file system (DFS). AD is a component of the Windows system state on Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 and Windows Server 2012 R2 domain controllers.

A domain controller is a computer that stores directory data and manages user interactions with a domain, including login, authentication, directory searches, and access to other shared resources.

AD, identified by its writer name, NTDS, is backed up as part of the Windows Roles and Features save set, a collection of system components that depend on each other.

These components are backed up together and usually restored together, through a BMR.

Only three of these components lend themselves to being restored separately through an online restore: Active Directory, DFSR, and Cluster Services (Cluster Database).

Selecting a restore method

Consider the following when selecting a restore method:

- The circumstances and characteristics of the failure and the two major categories of failure from an AD perspective are AD data corruption and hardware failure. AD data corruption occurs when the directory contains corrupt data that replicated to all domain controllers. Also, when a large portion of the AD hierarchy that is accidentally changed and this change was replicated to other domain controllers.
- The roles and functions of a failed NetWorker server.
- The types of restore for AD are non-authoritative restore and authoritative restore.

Non-authoritative restore

A non-authoritative restore returns the domain controller to its state at the time of backup, then allows normal replication to overwrite that state with any changes that have occurred after the backup completed.

After restoring the system state, the domain controller queries its replication partners. The replication partners replicate any changes to the restored domain controller, ensuring that the domain controller has an accurate and updated copy of the AD database.

Non-authoritative restore is the default method for restoring AD. This method is used in most situations that result from AD data loss or corruption.

Performing a non-authoritative AD restore on Windows Server 2008, 2008 R2, 2012 and 2012 R2

To perform a non-authoritative restore of the AD on a Windows Server 2008, 2008 R2, 2012 or 2012 R2, complete the following tasks.

Procedure

1. Log in as the Domain Administrator.
2. To recover the `WINDOWS ROLES AND FEATURES\NTDS` save set, perform one of the following steps:
   - To use the command prompt for recovery, type the following command:

     `recover` **-s *<NetWorker server>* -U -N "WINDOWS ROLES AND FEATURES\NTDS"**
   - To use NetWorker User application for recovery, browse to the `WINDOWS ROLES AND FEATURES\NTDS` save set, mark it for recovery, and then click **Start**.
3. When the restore completes, verify that the operation was successful.
4. To complete the AD restore, restart the domain controller.

Performing a bare metal recovery on Windows

Follow these procedures to perform a bare metal recovery on a NetWorker client or storage node.

Prerequisites for a Bare Metal Recovery (BMR)

Before performing a Bare Metal Recovery, ensure that you meet the minimum requirements of having backed up the `DISASTER_RECOVERY:\` save set and ensure that you have completed the following tasks.

Verifying the Windows BMR requirements

In preparation for a recovery, verify that target host meets the following requirements.

Requirements for Windows BMR backup and restore

The BMR recovery process restores the operating system that was installed on the source host. If you perform a BMR recovery to a different host with different hardware, after the recovery operation and restart completes, Windows prompts you to install the required drivers.

Before you perform a BMR recovery to a different host, ensure that you meet the following requirements:

- The source and target hosts use the same processor architecture.
- The hardware on the target host is operational.
- The target host has a minimum of 512 MB of RAM.

- The target host startup hard disk capacity must be larger or the same size as on the source host, regardless of the amount of space actually in use. If the disk is smaller by a single byte, BMR fails.

  Note

  Verify whether the source critical volumes are part of a larger physical disk. If critical volumes are on a larger physical disk, all target critical volumes must be large enough to accommodate the entire underlying physical disk. Use the Windows Disk Management utility to verify disk configuration and size.

- The number of disks on the target host is greater than or equal to the number of disks there were on the source host. The disk LUN numbering on the target host must match the disk LUN numbering on the source host.
- The RAID configuration on the target host should match the disk order of the hard disks.
- The disk or RAID drivers that are used on the source system are compatible with the disk or RAID controllers in the target system. The recovery process restores the backup to the same logical disk number that was used by the source host. You cannot restore the operating system to another hard disk.
- Windows BMR supports IDE, SATA, or SCSI hard disks. You can make the backup on one type of hard disk and recover on another type of hard disk. For example, SAS to SATA is supported.
- The target system can access the Windows BMR image as a bootable CD/DVD volume or from a network start location.
- The target system has the NIC or storage device drivers installed that match the NIC.

  Note

  All NIC or storage device drivers must not require a restart to complete the driver installation process. If the drivers require a restart, then the BMR recovery process fails and prompts you to install the drivers again.

Overview of Windows Bare Metal Recovery (BMR)

NetWorker Windows BMR is an automated recovery solution that uses the Windows ASR writer and other Microsoft VSS writers to identify critical volumes and perform a full recovery on a target host.

NetWorker Windows BMR supports file system backup and recovery of critical volumes. NetWorker Module for Microsoft (NMM) supports application data backup and recovery. Additional backup and recovery procedures are required to backup and restore application data. The NMM documentation provides specific instructions on how to backup and recover applications.

You can use Windows BMR to recover a backup from a physical host. You can also use Windows BMR to recover a VMware virtual machine or VMware CD to a physical host, VMware virtual machine, or a VMware CD.

NetWorker uses a special save set called `DISASTER_RECOVERY:\`, a subset of the `ALL` save set, to backup all the data that is required to perform a Windows BMR. NetWorker performs the BMR backup while the Windows operating system is active. You can recover an offline BMR backup without first reinstalling the Windows operating system. This action prevents problems that can occur when you restore operating system files to a running version of Windows.

To support a NetWorker Windows BMR recovery, download the Windows BMR image from http://support.emc.com. This image enables you to create a bootable Windows

BMR ISO that contains NetWorker binaries and a wizard, which controls the recovery process.

Note

The *EMC NetWorker Online Software Compatibility Guide* provides more information about operating systems support for Windows BMR.

Components of the DISASTER_RECOVERY:\ save set

The `DISASTER_RECOVERY:\` save set contains a group of component save sets that are required to perform a Windows BMR recovery. A full backup of the `DISASTER_RECOVERY:\` save set contains the following components:

- All critical volumes.
- `WINDOWS ROLES AND FEATURES:\` (a subset of the `DISASTER RECOVERY:\` and `ALL` save sets).
- System Reserved partition.
- UEFI partition (if available).

NetWorker supports full and incremental backup levels of the `DISASTER_RECOVERY:\` save set. Also, when the Windows BMR recovery operation recovers data from an incremental backup, the recovery operation recovers all incremental backups.

The first time NetWorker performs a backup of the `DISASTER_RECOVERY:\` save set, NetWorker performs a level Full backup, regardless of the level that is defined for the backup.

When you configure a level Incremental backup of the `DISASTER_RECOVERY:\` save set, NetWorker backs up some components of the save set at a level Full, and other components at an Incremental level.

The following table summarizes the backup level of each save set component of the `DISASTER_RECOVERY:\` save set, when you perform an incremental backup:

Table 5 `DISASTER_RECOVERY:\` components in an incremental backup

Save set	Backup level
Critical volumes	Incremental
`WINDOWS ROLES AND FEATURES:\`	Incremental
UEFI partitions	Full
System reserved partition	Full

During an incremental backup, the backup operation checks both the modification time and the archive bit to determine if a file must be backed up. The backup operation ignores the archive bit when you assign the *nsr_avoid_archive* variable a value of **Yes** on the client host. As a result, NetWorker only uses the modification time to determine which files to back up.

Use the environment variable *nsr_avoid_archive* with caution. If you use the environment variable *nsr_avoid_archive*, test the BMR backup image to ensure that you can recover the Windows system state correctly. Performing a BMR recovery to a physical computer provides more information on validating the BMR backup image.

A Windows BMR recovery requires a successful backup of each component save set in the `DISASTER_RECOVERY:\` save set. If one component of the save set fails, then the backup operation fails. For a scheduled backup, NetWorker retries the `DISASTER_RECOVERY:\` backup. The number of retries that NetWorker performs is

based on the value that is defined in the client retries attribute of the protection group that the Client resource is assigned to.

Note

In NMC Administration GUI, the **Log** tab of the **Monitoring** window, or the **Save Set** tab of the **Media** window displays each component save set of a `DISASTER_RECOVERY:\` backup.

Performing a Windows BMR to physical or virtual computers

This section describes how to use the NetWorker Windows BMR image to perform a Bare Metal Recovery on physical hosts and VMware virtual machines.

Before you perform a BMR, verify that the new host meets the Requirements for Windows BMR backup and restore on page 102 and ensure that you complete the tasks listed in this section.

Prerequisites to performing a Windows BMR

If you do not first add the recovering host to a group that has the Recover Local Data privilege, BMR of a NetWorker server fails through the `authc` process. Before you perform a BMR, add the following entries into the users list in `NMC\Server\User Groups`.

For example, to add the recovering host in to the Application Administrators group, add the following entries to the users list in NMC:

```
group=Administrators,host=<recovering_host>
user=administrator,host=<recovering_host>
user=system,host=<recovering_host>
```

where *recovering_host* is the name of the host that you are performing the BMR to.

Gathering configuration information required by a Windows BMR

Before you start a Windows BMR, ensure that you have the following configuration information:

- The driver software for NICs or disk devices, if you perform the Windows BMR to a host with hardware that differs from the source host.
- The network name and IP address of the target host.
- The network name and IP address of the NetWorker server.
- The network name and IP address of the NetWorker storage node, if the target host uses a storage node that is not the NetWorker server.
- The default gateway and the name of the DNS server. If a DNS server is not available, use a local hosts file to resolve hostname of the NetWorker server and storage nodes to the IP address.
- The NetWorker media volumes that contain the backup save sets.

Obtaining the Windows BMR image

To perform a Windows BMR, use the Windows BMR image available from the EMC Online Support website, http://support.emc.com, to create a bootable CD/DVD or deploy for a network boot operation. The BMR image contains the Windows PE operating system. WinPE is only available in English. EMC does not provide localized versions of the Windows BMR wizard. When you use the image to boot the Windows

host, the recovery process starts the NetWorker BMR wizard, which guides you through the recovery process.

You can use the 32-bit, or 64-bit Windows BMR image to recover either an x86, or x64 operating system backup to an x86 or x64 computer.

Note

A BMR treats the AMD and Intel processors as equivalent if they follow the same architecture. For example, you can recover the operating system from the backup of AMD x64 computer to an Intel x64 computer.

Use the following procedure to download the recovery boot image.

Procedure

1. On the EMC Online Support website, search for "NetWorker Wizard ISO" at EMC Online Support, and then narrow the search results by selecting items that are associated with the NetWorker release number.
2. On the **NetWorker Software Downloads** page:
   a. Locate the section that is labeled **NetWorker *Y.Y* - Build *xxx***.
   b. Select the link to download a Windows BMR ISO recovery file.

   where:
   - *Y.Y* is the version number of the NetWorker release
   - *xxx* is the build number of the released version

Creating a Windows BMR bootable image

Create a Windows BMR bootable CD/DVD or a network boot location from the Windows BMR ISO image, which you downloaded from http://support.emc.com.

Creating a Windows BMR bootable CD/DVD

Use the ISO image to create a bootable CD/DVD, then configure the host to boot from a CD/DVD.

Procedure

1. Open the CD/DVD creation software, and then select an option to burn an ISO image.
2. Browse to the location of the downloaded NetWorker Windows BMR image, and then complete the steps that are required to create a bootable CD/DVD with the image.

Enabling a protected host to boot from a CD/DVD
Procedure

1. Start the host, and then start the BIOS setup program, by pressing **F2**.

   NOTICE

   If you are restoring either from or to a virtual host such as a VMware virtual machine, you can set up options such as the host boot location within vSphere. The VMware documentation provides specific steps.

2. Select the **boot options** menu, and then ensure that the CD/DVD boot option is at the top of the list of locations from which to boot.

3. Save the changes, and then exit the BIOS program.

Creating a Windows BMR recovery network boot location

Ensure that you meet the following requirements for using the network boot option:

- Ensure the NetWorker clients that you protect with a Windows BMR backup can start from the network with a Pre-Boot Execution Environment (PXE).
- Configure and make available a Deployment Services server.
- Add the NetWorker Windows BMR boot image to the Deployment Services server so that a client host on the network can start from it.

Note

http://technet.microsoft.com/en-us/library/cc771670(WS.10).aspx describes how to configure Windows Deployment Services in Windows Server 2008 or Windows Server 2008 R2.

Enabling a host to boot from the network

The host should obtain an IP address from the WDS server, and then prompt you to perform a network boot. Typically, a network boot is activated by pressing the **F12** key.

Procedure

1. Start the host, and then start the BIOS setup program.

   Typically, this action is performed by pressing the **F2** key.

   NOTICE

   If you are restoring to a virtual host such as a VMware virtual machine, you can set up options such as the host boot location within vSphere. The VMware documentation provides specific steps.

2. Select **BIOS options necessary** so that the network boot option is enabled.

   The BIOS documentation provides more information.

3. Save the changes, and then exit the BIOS program.

Performing a Windows BMR to a physical computer

To recover a BMR backup to a physical host, perform the following steps. If the target host uses unified extensible firmware interface (UEFI) volumes, unmount the UEFI volumes before you perform the recovery operation.

Review the following information before you perform a recovery operation to a host that differs from the original:

- Ensure that the hardware configuration of the target host is similar to the original host.
- Ensure that the NetWorker server has a client resource for both the source host and the target host.
- Ensure that the Remote Access attribute of the source client resource contains the account *SYSTEM@target_client*. This attribute enables the recovery process to perform a directed recovery.
- Add `user=system,host=target_client` to the Users attribute of Application Administrators user group.

- Ensure that you have a writable volume available for the media pool being used. After the recover operation recovers all the data, the wizard generates log files in a save set named Offline Restore Logs. The recovery operation performs a backup of the log files to a volume in the media pool.
- Ensure that you enable the NetWorker server to accept manual save operations for the Recovery wizard log file backup.

Procedure

1. Start the target host from the Windows BMR image.

   The NetWorker Windows BMR wizard appears.
2. On the **Welcome** screen, click **Next**.
3. If a DNS server is not available on the network, perform the following:
   a. Exit the NetWorker Windows BMR wizard but do not restart the host.

      The WinPE command line appears.
   b. Edit the hosts file, for example, `X:\Windows\System32\Drivers\etc\hosts`.
   c. Add the IP address and hostname for the NetWorker server and the NetWorker storage node.
   d. Restart the wizard from the `X:\Program Files\EMC Networker\nsr\wizard` directory.

      For example: `X:\Program Files\EMC Networker\nsr\wizard>` **`javaw -jar WinPEWizard.jar`**
   e. When the wizard appears, click **Next**.
4. On the **Select Network Interface** screen:
   a. Select the NIC driver.
   b. Click **Next**.

   If the driver list does not contain the driver for the NIC on the target host, select **Load Driver**, and then browse to the location that contains the required driver.

   NOTICE

   The selected driver cannot require a restart operation because the recovery process loads the WinPE environment in memory only and changes are not persistent after a restart operation.
5. On the **Configure Hostname and Network** screen, complete the fields:
   a. In the **Hostname** field, type the hostname of the source host.
   b. In the **DNS domain** field, type the name of the domain in which the host resides.

      If the host resides in a workgroup instead of a domain, you can leave this field blank.
   c. In the **Configure desired IP Settings** field, choose the tab for the Network Protocol deployed on the network, either **IPv4** or **IPv6**.
   d. In the**TCP/IP Address** settings section, select either **Obtain an IP address automatically (DHCP)** or **Use the following IP Address.**

e. If you choose **Use the following IP Address**, type the IP address in the IP address field.

If applicable, type the subnet mask in the **Subnet mask** field, and then type the default gateway in **Default gateway** field.

f. In the **DNS Server** section, select either **Obtain DNS server address automatically** or **Use the following DNS server address**:

- If you choose **Use the following DNS server address**, type the IP address of the DNS server in the **Preferred DNS server** field.
- If applicable, type an alternate DNS server address in the **Alternate DNS server** field.

NOTICE

If you added the NetWorker server hostname and IP address to the `X:\Windows\System32\Drivers\etc\hosts file`, you can ignore the DNS Server fields.

g. Click **Next**.

The **Available Disks** screen displays all detected local disks.

6. If the **Windows BMR** wizard fails to detect a disk, perform the following steps:

a. Select **Load Driver**.

b. Browse to the location that contains the disk driver, and then load the required disk driver.

c. To update the list of detected disks, select **Refresh**.

d. Click **Next**.

7. On the **Select NetWorker Server** screen, complete the fields:

a. In the **Server** field, specify the NetWorker server that performed the backup:

- Select the NetWorker server from the server list. To update the list of NetWorker servers, click **Search**. The Search function locates only those NetWorker servers on the local subnet.
- Type the fully qualified domain name (FQDN).

b. In the **Client** field, ensure that the client name matches the Client resource name on the NetWorker server.

NetWorker automatically populates this field with the values that you specified in the **Hostname** and **DNS Domain** fields on the **Configure Hostname and Network** screen of the wizard. For example, if the client resource on the NetWorker server uses an FQDN, then specify the FQDN of the client in the **Client** field.

To recover the backup to a host that differs from the source host, modify the **Client** field to specify the target hostname.

If you specify a different client, the recovered host uses the same hostname and IP settings as the source computer. If the source computer is running on the same network, using the same hostname and IP settings can cause hostname and IP address conflicts.

c. Click **Next**.

8. On the **Select Bare Metal Recovery Backup** screen, select the system backup that you want to recover, and then click **Next**.

   System backups appear in descending order from most recent to oldest.

9. Review the **Save Sets to Restore** screen, and then click **Next**.

   The recovery process reformats critical volumes. The recovery process reformats non-critical volumes only if the disk signature on the target disk differs from the original disk.

   For example, to perform a quick format instead of a full format operation if the disk was replaced, select **Perform a quick format of disks**.

   Note

   A quick format is much faster than full format but does not verify each sector on the volume.

   The recovery process does not recover non-critical volume data. Recovering file system data provides more information.

10. On the **Bare Metal Recovery Summary** screen, select **Options** to display the **Non-Default Recover Options** screen.
11. On the **Non-Default Recover Options** screen:

    a. In the **Additional Options** field, type any required non-default options with their corresponding values.

       Non-default options are primarily used for troubleshooting purposes.

    b. To save and close the **Non-Default Recover Options** screen, and then return to the **Bare Metal Recovery Summary** screen, click **OK**.

    c. To begin the recovery process, click **Restore**.

12. On the **Confirmation** screen, select the **I confirm that I want to format the disks and restore the backup** option, and then click **OK**.

    NOTICE

    All data is lost on all volumes that the recovery process reformats.

    After the data recovery completes, the wizard writes the recovery log files to volumes in the backup media pool being used. If you do not have a volume available, then the recovery operation appears to be unavailable until media for the media pool becomes available.

    Note

    You can cancel the log file backup without affecting the recovery operation.

13. After the wizard and log files complete, click either **Reboot** or **Exit**:

    - To restart the system when any subsequent application data resources must be performed, click **Reboot**. If you are recovering an Active Directory domain controller, it is recovered in non-authoritative mode by default.
    - If you must recover a domain controller in authoritative mode, click **Exit**. The computer returns to the WinPE command prompt. Start into Directory

Services Restore Mode (DSRM). See Performing post recovery tasks for active directory services for more information.

Performing a BMR from a Physical Computer to a Virtual Machine (P2V)

This section describes the process of restoring a NetWorker backup of a physical computer to a virtual machine (P2V).

P2V is supported for physical computers running the following operating systems:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

P2V is supported when restoring to virtual machines created with the following hypervisors:

- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- VMware ESX 5.1
- VMware ESX 5.5
- VMware ESXi 5

Procedure

1. Perform a backup of the physical computer.
2. On the computer that runs the hypervisor, create a target virtual machine (VM).
   a. Configure the VM to use a virtual network adapter.
   b. On the **VM configuration** page:
      a. Select the LSI Logic SAS SCSI controller.
      b. Configure the disks on the VM to match the original physical computer configuration.
      c. Create the same number of physical disks.
      Extra disks can be added after the P2V recovery.
   c. Consider the following:
      - The SCSI disk numbers must match the original disk numbers.
      - The VM disk sizes must match, or exceed, the original disk sizes.

   For VMware hypervisors, use either a Windows Server 2008 (32-bit or 64-bit), 2008 R2 (64-bit), or Windows Server 2012 (64-bit) templates as the guest operating system when you create the VM.
3. On the VM, start the WinPE ISO which starts the BMR wizard.
4. On the VM, use the BMR wizard to configure the hostname and network configuration:
   a. On the **Select NetWorker Server** screen, specify the name of the physical computer as the NetWorker client.

b. On the **Save Sets to Restore** screen, review the selected items to restore, and then click **Next**.

c. On the **Select Bare Metal Recovery Backup** screen, select the backup to restore. Backups are listed in chronological order with the most recent backup first.

d. On the **Summary** screen, if the save set was created with NetWorker 8.1 or earlier, select the **Restore physical computer to virtual machine (P2V)** checkbox.

If the Restore physical computer to virtual machine (P2V) checkbox is not marked, the VM might not start successfully after the restore is complete.

e. To start the restore, select **Restore**.

5. Restart the VM when the P2V BMR is complete.

Performing Post-P2V tasks

The following section provides information about additional tasks that are required after a P2V recovery.

Procedure

1. If you are running VMware, install VMware tools.
2. To remove disabled NIC devices, use **Device Manager**:

   a. From Device Manager, select the **Show Hidden Devices** option.

   b. Select the hidden NIC device.

   c. Select **Uninstall**.

   This step is required because the original network adapter is no longer available.

3. To restore network connectivity, configure the virtual network adapter.

Post-recovery tasks

The following sections provide information about recovering data that was not recovered in the Windows BMR operation.

Using NMM for post-recovery tasks

If the recovered host has applications that are protected with NMM, all application-recovery operations must be performed by using the NMM client interface. The NMM documentation provides information on the post-recovery operations.

Before reviewing the NMM documentation, ensure that the following conditions are met:

- After the recovery has completed and the system is rebooted, check the host's disk and volume configuration. All disks and volumes should appear as they did on the original system. However, if disk signatures do not match the original disks, non-critical disks might be offline or unmounted. Use Microsoft Disk Manager to bring online or mount the disks. After the disks are online, a reboot operation should result in disk drive letter reassignments. If these correct drive letter assignments do not occur, manually assign drive letters to non-critical disks as

needed. Non-critical volumes that are accessed by mount points might have similar issues.

- To recover the host, perform additional online recovery of any required user data on non-critical volumes by using the NetWorker User program.
- If a folder is encrypted in Windows, for example, by selecting **Folder Properties** > **Advanced** > **Encrypt contents to secure data**, it is recovered as encrypted. However, the encryption attribute is not be set on the folder. You can manually reset the encryption attribute after the recovery operation. This task is a Microsoft limitation.
- Windows BMR supports backup and recovery of files and folders encrypted with Windows Encrypting File System (EFS), and volumes encrypted with BitLocker. After BMR, the EFS or BitLocker services might be running but the EFS encryption attributes on files or folders must be re-enabled and BitLocker volumes must be re-encrypted. For steps to encrypt with EFS and BitLocker, consult Microsoft documentation.

NOTICE

You cannot install the NetWorker software on volumes that are encrypted with Microsoft BitLocker.

Using an application backup tool other than NMM

If you backed up a database application with an application backup tool other than NMM, perform the following post-recovery operations:

- Recover any required file system data by completing the steps in the topic, Recovering file system data.
- Recover the application data by using the application backup tool, such as NetWorker User for SQL Server, NME, or any third-party application backup tool. Refer to the documentation that your application backup tool includes.

Recovering file system data

Perform an online recovery of any required user data on non-critical volumes. Sometimes, user data on non-critical volumes must be recovered, for instance, when disk hardware was replaced due to a disaster before the Windows BMR operation.

Procedure

1. Manually remount any non-critical volumes as needed.
2. To connect to the NetWorker server that backed up the source client data, start the NetWorker User program by using the `winworkr` command with the **-s** option.

   For example: `winworkr -s server_name`

   If the **-s** option is not used and there is only one server that is detected, that server is connected automatically. If there are no servers that are detected or if there is more than one server available, the **Change Server** dialog box appears, allowing you to choose the server.
3. To open the **Source Client** dialog box, click **Recover**.
4. Select the source client, and then click **OK**.
5. Select the destination client for the recovered data, and then click **OK**.

6. In the **Recover** screen, select the files to recover.
7. To begin the directed recovery, click **Start**.

Performing post-recovery tasks for Active Directory services

Perform the offline recovery of the `DISASTER_RECOVERY:\` component save sets if there is a non-authoritative domain controller. If a non-authoritative recovery is wanted, then no additional steps are required. However, if you must perform an authoritative recovery, follow these steps.

Procedure

1. To exit the wizard so that you can start into Directory Services Restore Mode (DSRM), on the **System Recovery Results** screen of the NetWorker Bare Metal Recovery wizard, select **Exit**.

   NOTICE

   Do not select **Reboot** in the wizard. Failure to start into DSRM mode results in a non-authoritative recovery. If you select **Reboot**, perform one of the following:

   - On restart, start the system in the WinPE operating system instead of the restored operating system.
   - Run the Windows BMR wizard again and ensure that you select **Exit**.

   The WinPE command prompt appears.
2. At the WinPE command prompt, type the following `bcdedit` commands.

   a. To force the system to start into DSRM, add a boot loader entry:

   `bcdedit` **`/copy {default} /d "Directory Service Repair Mode"`**
   A message similar to the following appears:

   ```
   The entry was successfully copied to
   {00000000-0000-0000-0000-000000000000}
   ```

   The numbers and dashes in the previous message form a Globally Unique Identifier (GUID) that identifies a new entry. In this example, the GUID is for illustration purposes only. The actual GUID that is generated when you run the command is unique.

   b. To set the safeboot option for the bootloader entry in the BCD store, type the following command using the generated GUID:

   `bcdedit` **`/set {`*`GUID_value`*`} safeboot dsrepair`**

   where *GUID_value* is the GUID displayed by the previous `bcdedit` command.

   c. To restart the system, exit the WinPE command prompt.

   Note

   Failure to start into DSRM results in a non-authoritative recovery.

3. (Optional) If you have a `WINDOWS ROLES AND FEATURES:\` Active Directory subcomponent save set that is newer than the `DISASTER_RECOVERY:\` save

set used in the preceding BMR, you can recover the save set in DSRM through the NetWorker User program.

4. From the WinPE command prompt, run the Windows `ntdsutil` utility.

   The `ntdsutil` prompt appears. The `ntdsutil` utility is a command interface similar to the NetWorker recover interface. For help with the `ntdsutil` utility, type:

   ```
   NTDSUTIL: ?
   ```

5. At the `ntdsutil` prompt, type:

   ```
   NTDSUTIL: activate instance ntds
   NTDSUTIL: authoritative restore
   ```

6. To perform an authoritative recovery of a subtree or individual object, type:

   ```
   NTDSUTIL: restore subtree "distinguished_name"
   ```

   For example:

   ```
   NTDSUTIL: restore subtree
   "OU=engineering,DC=Seattle,DC=jupiter,DC=com"
   NTDSUTIL: restore subtree
   "CN=mars,CN=users,DC=Seattle,DC=jupiter,DC=com"
   ```

   The Microsoft Windows Server Resource Kit documentation on Active Directory provides information.

7. Exit the `ntdsutil` utility by typing **`quit`** at each successive `ntdsutil` prompt until the command prompt appears.
8. Type the following command at the WinPE command prompt so that the host does not start into DSRM mode on restart.

   ```
   bcdedit /deletevalue safeboot
   ```

9. Restart the domain controller in normal mode, log in, and then verify that the authoritative changes are replicated to the Active Directory replication partners.

Performing post-recovery tasks for hosts with Windows server roles that use SQL Server

Procedure

1. On the target host, rebuild the SQL server by running the following `Setup` command:

   ```
   Setup /QUIET /ACTION=REBUILDDATABASE /
   INSTANCENAME=Instance_name /SQLSYSADMINACCOUNTS=domain_name
   \administrator
   ```

   The Setup tool is located on the SQL Server installation media and must be run from the command prompt with Windows Administrator privileges. Before you run this command, ensure that the SQL group is offline except for the shared disks.

   The following Microsoft article provides more information:

https://msdn.microsoft.com/en-us/library/ms189302

2. Bring the SQL sever services online.
3. Recover the SQL system databases (master, model, msdb) with NetWorker User for SQL Server, or a third-party application.

Performing post-recovery tasks for a Microsoft Hyper-V virtual machine

Use NMM to restore the Hyper-V virtual machines.

Troubleshooting Windows BMR

The following topics provide information to help troubleshoot Windows BMR operations.

Performing a manual uninstall and reconfigure of a NIC on Windows Server 2012 or Windows Server 2012 R2

If the guest operating system is Windows Server 2008 or Windows Server 2008 R2, the P2V BMR retains the NIC settings.

However, if the guest operating system is Windows Server 2012 or Windows Server 2012 R2, then Windows performs some Plug-N-Play configuration during the post-BMR restart. This activity disables the original NIC and creates a NIC.

Procedure

1. In the **Device Manager**, select **Display disabled devices** > **Uninstall the disabled NIC**.
2. Configure the new NIC with the wanted network settings.

Recovering and viewing Windows BMR log files

Windows BMR log files

To help troubleshoot an unsuccessful recovery, the following log files are generated and backed up during the Windows BMR operation:

- `daemon.raw`—This log file is the same as daemon.log for monitoring services.
- `Ossr_director.raw`—Contains the recovery workflow of the `DISASTER_RECOVERY:\` save set. This log also contains any errors that are related to recovering the save set files or Windows ASR writer errors.
- `recover.log`—Contains output from the NetWorker `recover.exe` program. This information is generated during the recovery of each save set. This log also contains messages about errors that are related to critical volume data recovery.
- `WinPE_Wizard.log`—Contains information about the workflow flow that is related to the NetWorker Bare Metal Recovery wizard user interface.
- `winpe_nw_support.raw`—Contains output from the `winpe_nw_support.dll` library. The output provides information about the communication between the NetWorker Bare Metal Recovery wizard and the NetWorker server.
- `winpe_os_support.log`—Contains output information that is related to Microsoft native API calls.

If the Windows BMR fails, you can recover the log files using one of the following options:

- By using FTP on the recovery host.
- By using a directed recovery.
- By copying the log files to a mapped drive.

If the Windows BMR was successful, you can recover the log files directly to the recovered host.

To view log files, you can use either a text editor or the `nsr_render_log` program, depending on the log file format.

Viewing the log files
To view the following log files, use a text editor:

- `recover.log`
- `WinPE_Wizard.log`

To view the following log files, use the `nsr_render_log` program:

- `Ossr_director.raw`
- `winpe_nw_support.raw`
  For example, to display the `Ossr_director.raw` file, type the following command at a command prompt:

  ```
  nsr_render_log "C:\logs\Client-bv1\Ossr_director.raw"
  ```

  To direct the `Ossr_director.raw` file to a text file that can be viewed in a text editor, type the following:

  ```
  nsr_render_log "C:\logs\Client-bv1\Ossr_director.raw" > mylog.txt
  ```

Accessing the log files using FTP

Procedure

1. On the recovery host, access the WinPE command line.

   You might have to exit the Windows Bare Metal Recovery wizard to access the WinPE command line. If you exit the wizard, do not restart.

2. Disable the Windows firewall.

   For example:

   ```
   wpeutil DisableFirewall
   ```

   By default, the Windows firewall is enabled on WinPE, and this action blocks the FTP port from transferring files.

3. Change to the following directory that contains the log files:

   ```
   X:\Program Files\EMC Networker\nsr\logs
   ```

4. To move the log files to another NetWorker host, use the FTP utility.

Accessing log files using a directed recovery operation

Procedure

1. To connect to the NetWorker server that backed up the source client data, start the NetWorker User program by using the `winworkr` command with the `-s` option:

   ```
   winworkr -s server_name
   ```

If the `-s` option is not included, and there is only one server that is detected, that server is connected automatically. If there are no servers that are detected or if there is more than one server available, the **Change Server** dialog box appears, enabling you to choose the server.

2. To open the **Source Client** dialog box, click **Recover**.
3. Select the source client, which is the recovered client, and then click **OK**.
4. Select the destination client for the recovered data, and then click **OK**.
5. From the **Options** menu, select **Options**, specify a folder location in which to relocate the recovered log files, and then click **OK**.
6. In the **Recover** window, select the log files to recover.

   The log files are typically located in the following directory:

   ```
   X:\Program Files\EMC Networker\nsr\logs
   ```

7. To begin the directed recovery, click **Start**.

   Recovering file system data, provides more information about the permissions that are required for directed recoveries.

BMR backup fails when System Reserved Partition is offline

BMR backups may fail with the following error:

```
device is not ready
```

Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 has 100 MB reserved as the System Reserved Partition. When backing up the system state, VSS includes the System Reserved Partition (used for BitLocker and Boot files), but the backup fails because the System Reserved Partition is offline. This can occur if the Windows automount capability is disabled. Although there are circumstances where the automount capability must be disabled, it can result in the partition being offline after a restart. Automount must be enabled for a BMR backup to succeed.

To work around this issue, use either of the following solutions:

Solution 1
From the command prompt, run `DISKPART` with the following commands:

`DISKPART`

`List volume`

`Select volume <number of 100 MB system partition>`

`Online volume` (if the volume is offline)

If automount is disabled while using third party storage software or if the user manually disabled the automount for the volume, the volumes can go offline.

This Microsoft KB article 2419286, available at http://support.microsoft.com/kb/2419286, provides details on preventing volumes from going offline by checking and setting the system automount attribute.

Solution 2
From the Disk Management console:

1. Access Disk Management from the command prompt:

   ```
   C:\>Diskmgmt.msc
   ```

2. To bring the disk online, assign the drive letter to the 100 MB partition:
   a. Right-click the 100 MB volume, and then select **Change Drive Letter and Paths**.
   b. Assign a new drive letter to the volume.
   Assigning the drive letter ensures that the volume are online after a restart.

Wizard cannot locate the NetWorker server or DNS server

If the NetWorker Bare Metal Recovery wizard cannot locate the NetWorker server or the DNS server (if one is being used), consider the following:

- If you are using a local hosts file instead of a DNS server, verify that the hostname and IP address of the NetWorker server was typed correctly.
- If you are using a DNS server, verify that the values typed in the **Configure Hostname and Network** screen were typed correctly.
- Verify that the NetWorker server was correctly specified in the **Select NetWorker Server** screen.

To verify hostname and IP address values, use the ping utility that is in the WinPE environment:

1. Exit the NetWorker Bare Metal Recovery wizard but do not restart the host.
   You are returned to the WinPE command line.
2. To locate, and then verify hostnames and IP addresses, use the **ping** utility. For example:

   ```
   ping -a hostname
   ```

3. Restart the wizard. For example:

   ```
   javaw -jar WinPEWizard.jar
   ```

   Note

   After the wizard has been restarted, you can switch between the wizard and the WinPE command line without exiting the wizard.

Multiple NICs cause errors in locating the NetWorker server

An error message similar to the following might appear when you try to recover a host with multiple NICs:

```
Error retrieving the list of Networker servers
```

This message is an indication that the NIC selected by the wizard is not the NIC that was connected to the NetWorker server when the backup was performed and the NIC might not have connectivity to the server. This applies when searching for an available server or specifying a specific server. To resolve the issue, select another NIC.

Network configuration values might not be retained after reboot

Sometimes, a host does not retain its network configuration data after a Windows BMR operation and after the host starts. If the recovered host is experiencing

network connectivity issues, confirm that network properties for the local connections are correct. If required, manually update the network configuration data on the host.

VSS backups fail because a critical disk is offline

VSS backups fail if a critical volume is offline during the backup operation. You can remedy the problem by following the steps that are outlined in the Microsoft Knowledgebase (KB) article 980794, which can be found at:

http://support.microsoft.com/kb/980794

The patch that is mentioned in this knowledgebase article is most likely on the Windows system if it is up-to-date. In this case, you can create and populate the Registry keys as described in the article.

This issue is most often encountered when backing up a passive node in an MSCS cluster and a critical volume is not on the physical host of the passive node but is instead on the physical host of the active node.

Jobquery fails to establish a connection with large scale jobs

When querying the number of save sets, jobquery fails to establish a connection with the jobsDB when the jobsDB contains more than 3,00,000 records.

The workaround is to run `nsradmin` from the command line with the following parameters:

```
nsradmin -S <jobsdatabse path>
```

8dot3name support disabled after recovery

In a WinPE 5.0 environment, `8dot3` file name support becomes disabled after recovery. This is not an issue from block-based backups.

If you require 8dot3name support, run the following command:

```
fsutil 8dot3name set C: 0
```

The Microsoft knowledgebase article 121007, available at http://support.microsoft.com/kb/121007, provides more information.

Additional recovery options

You can specify non-default recovery options on the WinPE command line or in the **Additional Options** field in the NetWorker Bare Metal Recovery wizard.

The following table describes the additional recovery options that can be used with a Windows BMR operation.

Table 6 Additional recovery options

Entry	Result
`-D x` where *x* is a number from 1 to 9, with 9 providing the most troubleshoot information and 1 providing the least.	Additional troubleshoot information is in the Windows BMR log files.

Table 6 Additional recovery options (continued)

Entry	Result
`-v`	Additional information on the progress of the recovery displays in the wizard's **System Recovery Status** window.
`-p`	By default, the Windows BMR recovery skips the formatting of non-critical disks. By using the `-p` option, any existing partitions are deleted and all disks are reformatted on the recovered computer to match the layout of the system image. However, by Microsoft specification, even if the `-p` option is selected, a non-critical volume is not reformatted if the disk signature has not changed since the backup. This option might be useful in situations where a system fails to recover because of disk mismatch errors. In this case, the `-p` option might resolve those errors. The recovery process does not recover non-critical volume data even if the volume is reformatted. Non-critical volumes can be recovered by using the NetWorker User program after the wizard has completed and the host has been restarted.
`recover -s <NetWorker server> -U -N "WINDOWS ROLES AND FEATURES \Cluster Database"`	When the restored data is meant to override the data on other nodes, it should be restored using the authoritative mode. Once this data is restored to one of the nodes, it is propagated to the other nodes and overwrites any newer data on those nodes. Perform Authoritative restore by using the command on the left. While the recovery is in progress, observe that the status of the groups changes from Online to Pending to Offline in the Failover Cluster Management application. Alternatively, check the Event Viewer, under **Application and Services Logs** > **Failover Clustering** > **Operational** on all nodes that the Cluster Service has stopped and restarted. Recover the shared drive data through *winworkr* on the cluster node with its current active node. Select **source client** as the virtual client, and **destination client** as the current active node.

Restart required after recovery operation

Newly recovered NetWorker client computers running Windows Server 2012 R2 can require an extra restart to restore access to application icons, previously viewable on the desktop.

CHAPTER 7

NetWorker Storage Node Disaster Recovery Procedures

This topic includes the following procedures.

- Performing a disaster recovery of a Storage Node on UNIX and Linux..... 124
- Performing an authoritative restore on Windows.....128
- Performing a non-authoritative restore on Windows..... 132
- Performing a bare metal recovery on Windows 134

Performing a disaster recovery of a Storage Node on UNIX and Linux

Follow these procedures to perform a disaster recovery on a NetWorker storage node on UNIX and Linux.

Planning notes and preparing for a disaster recovery

Back up important data on a scheduled basis. The more time and effort that is invested in incorporating, maintaining, and testing a backup solution, the better prepared you are if a disaster occurs.

Having the correct information handy in case a disaster occurs is a key element in recovering from a disaster as quickly as possible.

Gathering key information

Maintain accurate records for each hardware, software, network, device, and media component.

Hardware information

Maintain up-to-date information on computer hardware as follows:

- File system configuration
- Fully qualified domain names, IP addresses, and hostnames
- For Domain Name System (DNS) clients, maintain the DNS host's internet address and hostname
- Hard drive configuration
- Media device names
- Hardware vendor
- Configuration information for each piece of hardware, both active and inactive, within the organization or organizational site

Software information

Maintain up-to-date information on computer software as follows:

- Copies of the original operating system media and patches (and where they are located)
- Software enabler and authorization codes
- Software vendor contact information and contract number
- The operating system version and patches installed
- Operating system configuration
- Emergency media that can be used to recover a computer if a disaster occurs
- NetWorker bootstrap information for each NetWorker server
- Kernel configuration and location
- Device drivers

- A list of any volume mount points

Prerequisites for recovering a NetWorker client or storage node

Before recovering a NetWorker client or storage node, perform the following steps.

Procedure

1. Verify that the same operating system as the source host is installed on the target host.
2. Verify that the NetWorker server is functioning and available on the network.
3. Obtain the following information:
   - NetWorker server hostname.
   - NetWorker client or storage node software version and patch level on the computer before the disaster occurred.
   - Link names to the NetWorker directories you must recover. An example of a typical link from a NetWorker directory to a user directory is `/nsr` to `/var/nsr`.

Downloading the NetWorker software and documentation

To obtain the latest NetWorker software and documentation, perform the following steps.

Procedure

1. Review the online NetWorker documentation, such as the *EMC NetWorker Administration Guide*, *EMC NetWorker Installation Guide*, and *EMC NetWorker Release Notes*, for the latest information.
2. Obtain the required NetWorker cumulative hotfix media kits that provide customers with the opportunity to install the latest version of NetWorker including important hotfixes. Cumulative builds are released approximately once a month and each build contain a rollup of the fixes in each previous build.

   If additional hotfixes are required in an environment where a cumulative build is installed, hotfixes can be generated for use with the latest cumulative version. The cumulative releases for specific NetWorker versions are available at http://support.emc.com.
3. Open the NetWorker Cumulative Hotfix document for details regarding fixes that are in each build, knowledge base articles that are related to the fixes in each build, and download instructions.

Replacing the hardware, then reinstalling and upgrading the operating system

To replace the hardware, then reinstall and upgrade the operating system, perform the following steps.

Procedure

1. Identify the defective or suspect hardware, and then replace the hardware as required.
2. Reinstall a minimum operating system from installation media.
3. Install any patches or upgrade the operating system to the same level as before the disaster.

Note

When using the LVM and the file systems of the root VolumeGroups are mounted, check which additional file systems outside of the root VolumeGroups are part of the backup. If VolumeGroups are imported, use the same logical volumes that were used in the backup.
On Linux, ensure that all LVM device files in `/dev` are unique after the operating system installation.

4. Verify the library and tape drives on the operating system.
5. To ensure that the library and tape drive devices are correct, run the following commands:

   ```
   inquire
   sjirdtag devname
   ```

   where *devname* is the control port of the jukebox.

   For example:

   ```
   inquire
   sjirdtag scsidev0.2.4
   ```

Reinstalling the NetWorker storage node

To reinstall the NetWorker storage node and client software, perform the following steps.

Procedure

1. Reinstall the same version of the NetWorker storage node software into its original location. Installation instructions are provided in the *EMC NetWorker Installation Guide*.

   Note

   To upgrade the storage node software, first recover the storage node to its original state and then perform the upgrade.

2. Reinstall any NetWorker backup patches that were installed before the disaster.
3. Re-create any links to NetWorker directories.
4. (Optional) To perform a test recovery to ensure that the recovery process is functioning correctly, use the `recover` command.

   Note

   The NetWorker client software is also installed when you install the storage node software.

Results

The storage node can now access volumes that contain backups for other computers on the network. These volumes contain the application and user data that are required to recover computers that were protected with the NetWorker client software.

Preparing an autochanger for disaster recovery

To prepare an autochanger for disaster recovery, perform the following steps. Skip these steps if an autochanger is not used for disaster recovery.

Procedure

1. Ensure that an autochanger resource exists, the directory differs for Linux and Windows:
   - For Linux: `/nsr/res`
   - For Windows: `C:\Program Files\EMC NetWorker\nrs\res`

   If the autochanger resource does not exist, create it using the NetWorker Administration GUI. The *EMC NetWorker Administration Guide* provides details about this interface.
2. Reset the autochanger by using the `nsrjb -vHE` command.

   This command resets the autochanger, ejects backup volumes, reinitializes the element status, and checks each slot for a volume.
   - If the autochanger does not support the `-E` option, initialize the element status by using the `ielem` command.
   - Inventory the autochanger by using the `nsrjb -I` command. The output helps to determine whether the volumes required to recover the bootstrap are located inside the autochanger.

   Note

   None of these volumes are in the media database, so you cannot view the contents of the tape through NMC and the volume name comes up as **-***.

Recovering NetWorker client application and user data

To recover the application and user data, perform the following steps.

Procedure

1. To determine which volumes contain the application and user data backups for this computer, use the `mminfo -avot` command on the NetWorker server.

   For example:

   ```
   mminfo -avot -c client_name
   mminfo -avot -c storage_node_name
   ```

   where:
   - *client_name* is the hostname of the computer whose application and user data is recovered.
   - *storage_node_name* is the hostname of the computer whose application and user data is recovered.
2. To recover the data (directories and files) on the NetWorker client, use the `recover` command.

   ```
   recover> add /<file system or folder name>
   ```

```
recover> del /<file name or folder name> # Exclude the file from
selected list

recover> version # Check backup version and volume location

recover> force # Force overwrite

recover> recover # Start recover
```

Note

Overwriting operating system files might cause unpredictable results. To determine all the operating system files that should not be overwritten during a recovery, refer to the operating system documentation. Directories or files that must be marked for recovery are based on the applications that the server was running before the disaster.

3. Restart the host.

Performing a test backup and recovery

To test the NetWorker client backup and recovery process, perform the following steps.

Procedure

1. Perform a test manual backup by using the backup commands.
2. Perform a test recovery by using the recovery commands.

   The *EMC NetWorker Administration Guide* provides additional information on testing backup and recovery configurations.

Performing an authoritative restore on Windows

Use the following procedures to perform an authoritative restore on a NetWorker server, storage node, or client.

Active Directory restore information

Active Directory (AD) is the Windows directory service and the foundation for the Windows Distributed file system (DFS). AD is a component of the Windows system state on Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 and Windows Server 2012 R2 domain controllers.

A domain controller is a computer that stores directory data and manages user interactions with a domain, including login, authentication, directory searches, and access to other shared resources.

AD, identified by its writer name, NTDS, is backed up as part of the Windows Roles and Features save set, a collection of system components that depend on each other.

These components are backed up together and usually restored together, through a BMR.

Only three of these components lend themselves to being restored separately through an online restore: Active Directory, DFSR, and Cluster Services (Cluster Database).

Selecting a restore method

Consider the following when selecting a restore method:

- The circumstances and characteristics of the failure and the two major categories of failure from an AD perspective are AD data corruption and hardware failure. AD data corruption occurs when the directory contains corrupt data that replicated to all domain controllers. Also, when a large portion of the AD hierarchy that is accidentally changed and this change was replicated to other domain controllers.
- The roles and functions of a failed NetWorker server.
- The types of restore for AD are non-authoritative restore and authoritative restore.

Authoritative restore

An authoritative restore is an extension of the non-authoritative restore process. Perform the steps of a non-authoritative restore before performing an authoritative restore.

The main difference is that an authoritative restore can increment the version number of the attributes of all objects in an entire directory, all objects in a sub tree, or an individual object (provided that it is a leaf object) to make it authoritative in the directory.

To perform an authoritative restore, start the domain controller in **Directory Services Restore Mode**.

Restore the smallest necessary unit from the last level incremental backup of the AD. For example, do not restore the entire directory to restore a single sub tree.

The online AD restore is done through one of the following:

- The NetWorker User application—Browse to and restore the `WINDOWS ROLES AND FEATURES\NTDS` save set.
- The `recover` command. For example:

  ```
  recover -s <NetWorker server> -U -N "WINDOWS ROLES AND FEATURES
  \NTDS"
  ```

Performing an authoritative AD restore on Windows Server 2008, 2008 R2, 2012, and 2012 R2

Authoritative restore recovers domain controllers to a specific point in time, and marks objects in Active Directory (AD) as being authoritative with respect to their replication partners.

Complete the following steps to perform an authoritative AD restore of the `WINDOWS ROLES AND FEATURES\NTDS` save set on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

Procedure

1. Start the host in Directory Services Restore Mode (DSRM):
   a. Choose the **Windows boot** option for the domain controller.
   b. To display a list of special boot options, press **F8**.
   c. Select **Directory Services Restore Mode** (Windows Domain Controllers Only) from the list of special boot options. When you restart in this mode, AD is taken offline.

2. Log in as the Domain Administrator.
3. Recover the `WINDOWS ROLES AND FEATURES\NTDS` save set using one of the following methods:
   - To start the operation from the command prompt, type the following command:

     ```
     recover -s <NetWorker server> -N "WINDOWS ROLES AND FEATURES
     \NTDS"
     ```

   - To start the operation from the NetWorker User Recover GUI, browse to and mark the `WINDOWS ROLES AND FEATURES\NTDS` save set, and then click **Start**.
4. When the restore completes, verify that the operation was successful.
5. Run the Windows `ntdsutil.exe` command line utility as described in Running the ntdsutil.exe command line utility on page 99.

Running the ntdsutil.exe command line utility

Use the following procedure to run the `ntdsutil.exe` command line utility.

Before you begin

To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

Procedure

1. From the **ntdsutil** prompt, run the following commands:

Command	Description
`activate instance ntds`	Sets NTDS or a specific AD LDS instance as the active instance.
`authoritative restore`	Authoritatively restores the Active Directory database or AD LDS instance.

   For example:

   ```
   NTDSUTIL: activate instance ntds

   NTDSUTIL: authoritative restore
   ```

Figure 7 Administrator Command Prompt - ntdsutil

2. To perform an authoritative restore, use the following steps:

a. To restore AD objects, from the authoritative prompt, type `restore object DN`. This command marks object percentages as authoritative. This command also generates a text file that contains the distinguished name of the restored object, and an LDIF file that can be used to restore back-links for objects that are being authoritatively restored. Type the following command:

```
authoritative restore: restore object DN
```

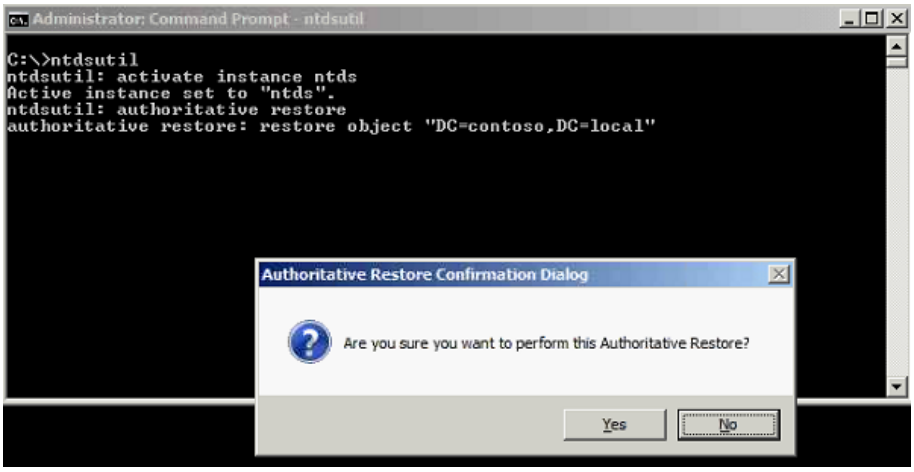
where *DN* is the distinguished name of the object to be restored.

For example:

```
restore object "DN=contoso ,DN=local"
```

This command restores everything under `contoso.local`. A confirmation dialog box appears.

Figure 8 Authoritative Restore Confirmation dialog box



b. Click **Yes** when prompted to continue the authoritative restore.

c. To restore child objects, from the authoritative prompt, type the following **`restore subtree DN`** command:

```
authoritative restore: restore subtree DN
```

where *DN* is the distinguished name of the subtree/child objects to be restored.

This command marks the subtree percentages (and all children of the subtree) as authoritative. This command also generates a file that contains the distinguished names of the restored object, and an LDIF file that can be used to restore back-links for objects that are being authoritatively restored. For example, group memberships of users.

3. Type `quit` to exit each prompt.
4. Restart the domain controller in Normal Mode.

Restart required after recovery operation

Newly recovered NetWorker client computers running Windows Server 2012 R2 can require an extra restart to restore access to application icons, previously viewable on the desktop.

Checking authoritative restore results

To check authoritative restore results, perform the following tasks.

Procedure

1. Open the Active Directory Users and Computers MMC snap-in.
2. If the authoritative restore was successful, the following settings appear on both `node_a` and `node_b` after restart and a complete replication cycle:
   - The modified user description has the original description.
   - The deleted user is present again.
   - The users that were added after the backup are still present.

Performing a non-authoritative restore on Windows

Use the following procedures to perform a non-authoritative restore on a NetWorker server, storage node, or client.

Active Directory restore information

Active Directory (AD) is the Windows directory service and the foundation for the Windows Distributed file system (DFS). AD is a component of the Windows system state on Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 and Windows Server 2012 R2 domain controllers.

A domain controller is a computer that stores directory data and manages user interactions with a domain, including login, authentication, directory searches, and access to other shared resources.

AD, identified by its writer name, NTDS, is backed up as part of the Windows Roles and Features save set, a collection of system components that depend on each other.

These components are backed up together and usually restored together, through a BMR.

Only three of these components lend themselves to being restored separately through an online restore: Active Directory, DFSR, and Cluster Services (Cluster Database).

Selecting a restore method

Consider the following when selecting a restore method:

- The circumstances and characteristics of the failure and the two major categories of failure from an AD perspective are AD data corruption and hardware failure. AD data corruption occurs when the directory contains corrupt data that replicated to all domain controllers. Also, when a large portion of the AD hierarchy that is accidentally changed and this change was replicated to other domain controllers.
- The roles and functions of a failed NetWorker server.

- The types of restore for AD are non-authoritative restore and authoritative restore.

Non-authoritative restore

A non-authoritative restore returns the domain controller to its state at the time of backup, then allows normal replication to overwrite that state with any changes that have occurred after the backup completed.

After restoring the system state, the domain controller queries its replication partners. The replication partners replicate any changes to the restored domain controller, ensuring that the domain controller has an accurate and updated copy of the AD database.

Non-authoritative restore is the default method for restoring AD. This method is used in most situations that result from AD data loss or corruption.

Performing a non-authoritative AD restore on Windows Server 2008, 2008 R2, 2012 and 2012 R2

To perform a non-authoritative restore of the AD on a Windows Server 2008, 2008 R2, 2012 or 2012 R2, complete the following tasks.

Procedure

1. Log in as the Domain Administrator.
2. To recover the `WINDOWS ROLES AND FEATURES\NTDS` save set, perform one of the following steps:
   - To use the command prompt for recovery, type the following command:

     `recover` **-s *<NetWorker server>* -U -N "WINDOWS ROLES AND FEATURES\NTDS"**
   - To use NetWorker User application for recovery, browse to the `WINDOWS ROLES AND FEATURES\NTDS` save set, mark it for recovery, and then click **Start**.
3. When the restore completes, verify that the operation was successful.
4. To complete the AD restore, restart the domain controller.

Performing a bare metal recovery on Windows

Follow these procedures to perform a bare metal recovery on a NetWorker client or storage node.

Prerequisites for a Bare Metal Recovery (BMR)

Before performing a Bare Metal Recovery, ensure that you meet the minimum requirements of having backed up the `DISASTER_RECOVERY:\` save set and ensure that you have completed the following tasks.

Verifying the Windows BMR requirements

In preparation for a recovery, verify that target host meets the following requirements.

Requirements for Windows BMR backup and restore

The BMR recovery process restores the operating system that was installed on the source host. If you perform a BMR recovery to a different host with different hardware, after the recovery operation and restart completes, Windows prompts you to install the required drivers.

Before you perform a BMR recovery to a different host, ensure that you meet the following requirements:

- The source and target hosts use the same processor architecture.
- The hardware on the target host is operational.
- The target host has a minimum of 512 MB of RAM.
- The target host startup hard disk capacity must be larger or the same size as on the source host, regardless of the amount of space actually in use. If the disk is smaller by a single byte, BMR fails.

  Note

  Verify whether the source critical volumes are part of a larger physical disk. If critical volumes are on a larger physical disk, all target critical volumes must be large enough to accommodate the entire underlying physical disk. Use the Windows Disk Management utility to verify disk configuration and size.

- The number of disks on the target host is greater than or equal to the number of disks there were on the source host. The disk LUN numbering on the target host must match the disk LUN numbering on the source host.
- The RAID configuration on the target host should match the disk order of the hard disks.
- The disk or RAID drivers that are used on the source system are compatible with the disk or RAID controllers in the target system. The recovery process restores the backup to the same logical disk number that was used by the source host. You cannot restore the operating system to another hard disk.
- Windows BMR supports IDE, SATA, or SCSI hard disks. You can make the backup on one type of hard disk and recover on another type of hard disk. For example, SAS to SATA is supported.

- The target system can access the Windows BMR image as a bootable CD/DVD volume or from a network start location.
- The target system has the NIC or storage device drivers installed that match the NIC.

Note

All NIC or storage device drivers must not require a restart to complete the driver installation process. If the drivers require a restart, then the BMR recovery process fails and prompts you to install the drivers again.

Overview of Windows Bare Metal Recovery (BMR)

NetWorker Windows BMR is an automated recovery solution that uses the Windows ASR writer and other Microsoft VSS writers to identify critical volumes and perform a full recovery on a target host.

NetWorker Windows BMR supports file system backup and recovery of critical volumes. NetWorker Module for Microsoft (NMM) supports application data backup and recovery. Additional backup and recovery procedures are required to backup and restore application data. The NMM documentation provides specific instructions on how to backup and recover applications.

You can use Windows BMR to recover a backup from a physical host. You can also use Windows BMR to recover a VMware virtual machine or VMware CD to a physical host, VMware virtual machine, or a VMware CD.

NetWorker uses a special save set called `DISASTER_RECOVERY:\`, a subset of the `ALL` save set, to backup all the data that is required to perform a Windows BMR. NetWorker performs the BMR backup while the Windows operating system is active. You can recover an offline BMR backup without first reinstalling the Windows operating system. This action prevents problems that can occur when you restore operating system files to a running version of Windows.

To support a NetWorker Windows BMR recovery, download the Windows BMR image from http://support.emc.com. This image enables you to create a bootable Windows BMR ISO that contains NetWorker binaries and a wizard, which controls the recovery process.

Note

The *EMC NetWorker Online Software Compatibility Guide* provides more information about operating systems support for Windows BMR.

Components of the DISASTER_RECOVERY:\ save set

The `DISASTER_RECOVERY:\` save set contains a group of component save sets that are required to perform a Windows BMR recovery. A full backup of the `DISASTER_RECOVERY:\` save set contains the following components:

- All critical volumes.
- `WINDOWS ROLES AND FEATURES:\` (a subset of the `DISASTER RECOVERY:\` and `ALL` save sets).
- System Reserved partition.
- UEFI partition (if available).

NetWorker supports full and incremental backup levels of the `DISASTER_RECOVERY:\` save set. Also, when the Windows BMR recovery operation recovers data from an incremental backup, the recovery operation recovers all incremental backups.

The first time NetWorker performs a backup of the `DISASTER_RECOVERY:\` save set, NetWorker performs a level Full backup, regardless of the level that is defined for the backup.

When you configure a level Incremental backup of the `DISASTER_RECOVERY:\` save set, NetWorker backs up some components of the save set at a level Full, and other components at an Incremental level.

The following table summarizes the backup level of each save set component of the `DISASTER_RECOVERY:\` save set, when you perform an incremental backup:

Table 7 `DISASTER_RECOVERY:\` components in an incremental backup

Save set	Backup level
Critical volumes	Incremental
`WINDOWS ROLES AND FEATURES:\`	Incremental
UEFI partitions	Full
System reserved partition	Full

During an incremental backup, the backup operation checks both the modification time and the archive bit to determine if a file must be backed up. The backup operation ignores the archive bit when you assign the *nsr_avoid_archive* variable a value of **Yes** on the client host. As a result, NetWorker only uses the modification time to determine which files to back up.

Use the environment variable *nsr_avoid_archive* with caution. If you use the environment variable *nsr_avoid_archive*, test the BMR backup image to ensure that you can recover the Windows system state correctly. Performing a BMR recovery to a physical computer provides more information on validating the BMR backup image.

A Windows BMR recovery requires a successful backup of each component save set in the `DISASTER_RECOVERY:\` save set. If one component of the save set fails, then the backup operation fails. For a scheduled backup, NetWorker retries the `DISASTER_RECOVERY:\` backup. The number of retries that NetWorker performs is based on the value that is defined in the client retries attribute of the protection group that the Client resource is assigned to.

Note

In NMC Administration GUI, the **Log** tab of the **Monitoring** window, or the **Save Set** tab of the **Media** window displays each component save set of a `DISASTER_RECOVERY:\` backup.

Performing a Windows BMR to physical or virtual computers

This section describes how to use the NetWorker Windows BMR image to perform a Bare Metal Recovery on physical hosts and VMware virtual machines.

Before you perform a BMR, verify that the new host meets the Requirements for Windows BMR backup and restore on page 102 and ensure that you complete the tasks listed in this section.

Prerequisites to performing a Windows BMR

If you do not first add the recovering host to a group that has the Recover Local Data privilege, BMR of a NetWorker server fails through the `authc` process. Before you

perform a BMR, add the following entries into the users list in `NMC\Server\User Groups`.

For example, to add the recovering host in to the Application Administrators group, add the following entries to the users list in NMC:

```
group=Administrators,host=<recovering_host>
user=administrator,host=<recovering_host>
user=system,host=<recovering_host>
```

where *recovering_host* is the name of the host that you are performing the BMR to.

Gathering configuration information required by a Windows BMR

Before you start a Windows BMR, ensure that you have the following configuration information:

- The driver software for NICs or disk devices, if you perform the Windows BMR to a host with hardware that differs from the source host.
- The network name and IP address of the target host.
- The network name and IP address of the NetWorker server.
- The network name and IP address of the NetWorker storage node, if the target host uses a storage node that is not the NetWorker server.
- The default gateway and the name of the DNS server. If a DNS server is not available, use a local hosts file to resolve hostname of the NetWorker server and storage nodes to the IP address.
- The NetWorker media volumes that contain the backup save sets.

Obtaining the Windows BMR image

To perform a Windows BMR, use the Windows BMR image available from the EMC Online Support website, http://support.emc.com, to create a bootable CD/DVD or deploy for a network boot operation. The BMR image contains the Windows PE operating system. WinPE is only available in English. EMC does not provide localized versions of the Windows BMR wizard. When you use the image to boot the Windows host, the recovery process starts the NetWorker BMR wizard, which guides you through the recovery process.

You can use the 32-bit, or 64-bit Windows BMR image to recover either an x86, or x64 operating system backup to an x86 or x64 computer.

Note

A BMR treats the AMD and Intel processors as equivalent if they follow the same architecture. For example, you can recover the operating system from the backup of AMD x64 computer to an Intel x64 computer.

Use the following procedure to download the recovery boot image.

Procedure

1. On the EMC Online Support website, search for “NetWorker Wizard ISO” at EMC Online Support, and then narrow the search results by selecting items that are associated with the NetWorker release number.
2. On the **NetWorker Software Downloads** page:
   a. Locate the section that is labeled **NetWorker *Y.Y* - Build *xxx***.

b. Select the link to download a Windows BMR ISO recovery file.

where:

- *Y.Y* is the version number of the NetWorker release
- *xxx* is the build number of the released version

Creating a Windows BMR bootable image

Create a Windows BMR bootable CD/DVD or a network boot location from the Windows BMR ISO image, which you downloaded from http://support.emc.com.

Creating a Windows BMR bootable CD/DVD

Use the ISO image to create a bootable CD/DVD, then configure the host to boot from a CD/DVD.

Procedure

1. Open the CD/DVD creation software, and then select an option to burn an ISO image.
2. Browse to the location of the downloaded NetWorker Windows BMR image, and then complete the steps that are required to create a bootable CD/DVD with the image.

Enabling a protected host to boot from a CD/DVD
Procedure

1. Start the host, and then start the BIOS setup program, by pressing **F2**.

   NOTICE

   If you are restoring either from or to a virtual host such as a VMware virtual machine, you can set up options such as the host boot location within vSphere. The VMware documentation provides specific steps.

2. Select the **boot options** menu, and then ensure that the CD/DVD boot option is at the top of the list of locations from which to boot.
3. Save the changes, and then exit the BIOS program.

Creating a Windows BMR recovery network boot location

Ensure that you meet the following requirements for using the network boot option:

- Ensure the NetWorker clients that you protect with a Windows BMR backup can start from the network with a Pre-Boot Execution Environment (PXE).
- Configure and make available a Deployment Services server.
- Add the NetWorker Windows BMR boot image to the Deployment Services server so that a client host on the network can start from it.

Note

http://technet.microsoft.com/en-us/library/cc771670(WS.10).aspx describes how to configure Windows Deployment Services in Windows Server 2008 or Windows Server 2008 R2.

Enabling a host to boot from the network

The host should obtain an IP address from the WDS server, and then prompt you to perform a network boot. Typically, a network boot is activated by pressing the **F12** key.

Procedure

1. Start the host, and then start the BIOS setup program.

   Typically, this action is performed by pressing the **F2** key.

   NOTICE

   If you are restoring to a virtual host such as a VMware virtual machine, you can set up options such as the host boot location within vSphere. The VMware documentation provides specific steps.

2. Select **BIOS options necessary** so that the network boot option is enabled.

   The BIOS documentation provides more information.

3. Save the changes, and then exit the BIOS program.

Performing a Windows BMR to a physical computer

To recover a BMR backup to a physical host, perform the following steps. If the target host uses unified extensible firmware interface (UEFI) volumes, unmount the UEFI volumes before you perform the recovery operation.

Review the following information before you perform a recovery operation to a host that differs from the original:

- Ensure that the hardware configuration of the target host is similar to the original host.
- Ensure that the NetWorker server has a client resource for both the source host and the target host.
- Ensure that the Remote Access attribute of the source client resource contains the account *SYSTEM@target_client*. This attribute enables the recovery process to perform a directed recovery.
- Add `user=system,host=target_client` to the Users attribute of Application Administrators user group.
- Ensure that you have a writable volume available for the media pool being used. After the recover operation recovers all the data, the wizard generates log files in a save set named Offline Restore Logs. The recovery operation performs a backup of the log files to a volume in the media pool.
- Ensure that you enable the NetWorker server to accept manual save operations for the Recovery wizard log file backup.

Procedure

1. Start the target host from the Windows BMR image.

   The NetWorker Windows BMR wizard appears.

2. On the **Welcome** screen, click **Next**.
3. If a DNS server is not available on the network, perform the following:

   a. Exit the NetWorker Windows BMR wizard but do not restart the host.

      The WinPE command line appears.

b. Edit the hosts file, for example, `X:\Windows\System32\Drivers\etc\hosts`.

c. Add the IP address and hostname for the NetWorker server and the NetWorker storage node.

d. Restart the wizard from the `X:\Program Files\EMC Networker\nsr\wizard` directory.

For example: `X:\Program Files\EMC Networker\nsr\wizard>` **`javaw -jar WinPEWizard.jar`**

e. When the wizard appears, click **Next**.

4. On the **Select Network Interface** screen:

a. Select the NIC driver.

b. Click **Next**.

If the driver list does not contain the driver for the NIC on the target host, select **Load Driver**, and then browse to the location that contains the required driver.

NOTICE

The selected driver cannot require a restart operation because the recovery process loads the WinPE environment in memory only and changes are not persistent after a restart operation.

5. On the **Configure Hostname and Network** screen, complete the fields:

a. In the **Hostname** field, type the hostname of the source host.

b. In the **DNS domain** field, type the name of the domain in which the host resides.

If the host resides in a workgroup instead of a domain, you can leave this field blank.

c. In the **Configure desired IP Settings** field, choose the tab for the Network Protocol deployed on the network, either **IPv4** or **IPv6**.

d. In the**TCP/IP Address** settings section, select either **Obtain an IP address automatically (DHCP)** or **Use the following IP Address.**

e. If you choose **Use the following IP Address**, type the IP address in the IP address field.

If applicable, type the subnet mask in the **Subnet mask** field, and then type the default gateway in **Default gateway** field.

f. In the **DNS Server** section, select either **Obtain DNS server address automatically** or **Use the following DNS server address**:

- If you choose **Use the following DNS server address**, type the IP address of the DNS server in the **Preferred DNS server** field.
- If applicable, type an alternate DNS server address in the **Alternate DNS server** field.

NOTICE

If you added the NetWorker server hostname and IP address to the `X:\Windows\System32\Drivers\etc\hosts file`, you can ignore the DNS Server fields.

g. Click **Next**.

The **Available Disks** screen displays all detected local disks.

6. If the **Windows BMR** wizard fails to detect a disk, perform the following steps:

   a. Select **Load Driver**.

   b. Browse to the location that contains the disk driver, and then load the required disk driver.

   c. To update the list of detected disks, select **Refresh**.

   d. Click **Next**.

7. On the **Select NetWorker Server** screen, complete the fields:

   a. In the **Server** field, specify the NetWorker server that performed the backup:

      - Select the NetWorker server from the server list. To update the list of NetWorker servers, click **Search**. The Search function locates only those NetWorker servers on the local subnet.
      - Type the fully qualified domain name (FQDN).

   b. In the **Client** field, ensure that the client name matches the Client resource name on the NetWorker server.

      NetWorker automatically populates this field with the values that you specified in the **Hostname** and **DNS Domain** fields on the **Configure Hostname and Network** screen of the wizard. For example, if the client resource on the NetWorker server uses an FQDN, then specify the FQDN of the client in the **Client** field.

      To recover the backup to a host that differs from the source host, modify the **Client** field to specify the target hostname.

      If you specify a different client, the recovered host uses the same hostname and IP settings as the source computer. If the source computer is running on the same network, using the same hostname and IP settings can cause hostname and IP address conflicts.

   c. Click **Next**.

8. On the **Select Bare Metal Recovery Backup** screen, select the system backup that you want to recover, and then click **Next**.

   System backups appear in descending order from most recent to oldest.

9. Review the **Save Sets to Restore** screen, and then click **Next**.

   The recovery process reformats critical volumes. The recovery process reformats non-critical volumes only if the disk signature on the target disk differs from the original disk.

   For example, to perform a quick format instead of a full format operation if the disk was replaced, select **Perform a quick format of disks**.

Note

A quick format is much faster than full format but does not verify each sector on the volume.

The recovery process does not recover non-critical volume data. Recovering file system data provides more information.

10. On the **Bare Metal Recovery Summary** screen, select **Options** to display the **Non-Default Recover Options** screen.
11. On the **Non-Default Recover Options** screen:
    a. In the **Additional Options** field, type any required non-default options with their corresponding values.

       Non-default options are primarily used for troubleshooting purposes.

    b. To save and close the **Non-Default Recover Options** screen, and then return to the **Bare Metal Recovery Summary** screen, click **OK**.

    c. To begin the recovery process, click **Restore**.
12. On the **Confirmation** screen, select the **I confirm that I want to format the disks and restore the backup** option, and then click **OK**.

    NOTICE

    All data is lost on all volumes that the recovery process reformats.

    After the data recovery completes, the wizard writes the recovery log files to volumes in the backup media pool being used. If you do not have a volume available, then the recovery operation appears to be unavailable until media for the media pool becomes available.

    Note

    You can cancel the log file backup without affecting the recovery operation.

13. After the wizard and log files complete, click either **Reboot** or **Exit**:
    - To restart the system when any subsequent application data resources must be performed, click **Reboot**. If you are recovering an Active Directory domain controller, it is recovered in non-authoritative mode by default.
    - If you must recover a domain controller in authoritative mode, click **Exit**. The computer returns to the WinPE command prompt. Start into Directory Services Restore Mode (DSRM). See Performing post recovery tasks for active directory services for more information.

Performing a BMR from a Physical Computer to a Virtual Machine (P2V)

This section describes the process of restoring a NetWorker backup of a physical computer to a virtual machine (P2V).

P2V is supported for physical computers running the following operating systems:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

- Windows Server 2012 R2

P2V is supported when restoring to virtual machines created with the following hypervisors:

- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- VMware ESX 5.1
- VMware ESX 5.5
- VMware ESXi 5

Procedure

1. Perform a backup of the physical computer.
2. On the computer that runs the hypervisor, create a target virtual machine (VM).
   a. Configure the VM to use a virtual network adapter.
   b. On the **VM configuration** page:
      a. Select the LSI Logic SAS SCSI controller.
      b. Configure the disks on the VM to match the original physical computer configuration.
      c. Create the same number of physical disks.
      Extra disks can be added after the P2V recovery.
   c. Consider the following:
      - The SCSI disk numbers must match the original disk numbers.
      - The VM disk sizes must match, or exceed, the original disk sizes.

   For VMware hypervisors, use either a Windows Server 2008 (32-bit or 64-bit), 2008 R2 (64-bit), or Windows Server 2012 (64-bit) templates as the guest operating system when you create the VM.
3. On the VM, start the WinPE ISO which starts the BMR wizard.
4. On the VM, use the BMR wizard to configure the hostname and network configuration:
   a. On the **Select NetWorker Server** screen, specify the name of the physical computer as the NetWorker client.
   b. On the **Save Sets to Restore** screen, review the selected items to restore, and then click **Next**.
   c. On the **Select Bare Metal Recovery Backup** screen, select the backup to restore. Backups are listed in chronological order with the most recent backup first.
   d. On the **Summary** screen, if the save set was created with NetWorker 8.1 or earlier, select the **Restore physical computer to virtual machine (P2V)** checkbox.

      If the Restore physical computer to virtual machine (P2V) checkbox is not marked, the VM might not start successfully after the restore is complete.

e. To start the restore, select **Restore**.

5. Restart the VM when the P2V BMR is complete.

Performing Post-P2V tasks

The following section provides information about additional tasks that are required after a P2V recovery.

Procedure

1. If you are running VMware, install VMware tools.
2. To remove disabled NIC devices, use **Device Manager**:
   a. From Device Manager, select the **Show Hidden Devices** option.
   b. Select the hidden NIC device.
   c. Select **Uninstall**.

   This step is required because the original network adapter is no longer available.
3. To restore network connectivity, configure the virtual network adapter.

Post-recovery tasks

The following sections provide information about recovering data that was not recovered in the Windows BMR operation.

Using NMM for post-recovery tasks

If the recovered host has applications that are protected with NMM, all application-recovery operations must be performed by using the NMM client interface. The NMM documentation provides information on the post-recovery operations.

Before reviewing the NMM documentation, ensure that the following conditions are met:

- After the recovery has completed and the system is rebooted, check the host's disk and volume configuration. All disks and volumes should appear as they did on the original system. However, if disk signatures do not match the original disks, non-critical disks might be offline or unmounted. Use Microsoft Disk Manager to bring online or mount the disks. After the disks are online, a reboot operation should result in disk drive letter reassignments. If these correct drive letter assignments do not occur, manually assign drive letters to non-critical disks as needed. Non-critical volumes that are accessed by mount points might have similar issues.
- To recover the host, perform additional online recovery of any required user data on non-critical volumes by using the NetWorker User program.
- If a folder is encrypted in Windows, for example, by selecting **Folder Properties** > **Advanced** > **Encrypt contents to secure data**, it is recovered as encrypted. However, the encryption attribute is not be set on the folder. You can manually reset the encryption attribute after the recovery operation. This task is a Microsoft limitation.
- Windows BMR supports backup and recovery of files and folders encrypted with Windows Encrypting File System (EFS), and volumes encrypted with BitLocker. After BMR, the EFS or BitLocker services might be running but the EFS encryption attributes on files or folders must be re-enabled and BitLocker volumes

must be re-encrypted. For steps to encrypt with EFS and BitLocker, consult Microsoft documentation.

NOTICE

You cannot install the NetWorker software on volumes that are encrypted with Microsoft BitLocker.

Using an application backup tool other than NMM

If you backed up a database application with an application backup tool other than NMM, perform the following post-recovery operations:

- Recover any required file system data by completing the steps in the topic, Recovering file system data.
- Recover the application data by using the application backup tool, such as NetWorker User for SQL Server, NME, or any third-party application backup tool. Refer to the documentation that your application backup tool includes.

Recovering file system data

Perform an online recovery of any required user data on non-critical volumes. Sometimes, user data on non-critical volumes must be recovered, for instance, when disk hardware was replaced due to a disaster before the Windows BMR operation.

Procedure

1. Manually remount any non-critical volumes as needed.
2. To connect to the NetWorker server that backed up the source client data, start the NetWorker User program by using the `winworkr` command with the **-s** option.

   For example: `winworkr -s server_name`

   If the **-s** option is not used and there is only one server that is detected, that server is connected automatically. If there are no servers that are detected or if there is more than one server available, the **Change Server** dialog box appears, allowing you to choose the server.
3. To open the **Source Client** dialog box, click **Recover**.
4. Select the source client, and then click **OK**.
5. Select the destination client for the recovered data, and then click **OK**.
6. In the **Recover** screen, select the files to recover.
7. To begin the directed recovery, click **Start**.

Performing post-recovery tasks for Active Directory services

Perform the offline recovery of the `DISASTER_RECOVERY:\` component save sets if there is a non-authoritative domain controller. If a non-authoritative recovery is wanted, then no additional steps are required. However, if you must perform an authoritative recovery, follow these steps.

Procedure

1. To exit the wizard so that you can start into Directory Services Restore Mode (DSRM), on the **System Recovery Results** screen of the NetWorker Bare Metal Recovery wizard, select **Exit**.

NOTICE

Do not select **Reboot** in the wizard. Failure to start into DSRM mode results in a non-authoritative recovery. If you select **Reboot**, perform one of the following:

- On restart, start the system in the WinPE operating system instead of the restored operating system.
- Run the Windows BMR wizard again and ensure that you select **Exit**.

The WinPE command prompt appears.

2. At the WinPE command prompt, type the following `bcdedit` commands.

   a. To force the system to start into DSRM, add a boot loader entry:

   ```
   bcdedit /copy {default} /d "Directory Service Repair Mode"
   ```

   A message similar to the following appears:

   ```
   The entry was successfully copied to
   {00000000-0000-0000-0000-000000000000}
   ```

   The numbers and dashes in the previous message form a Globally Unique Identifier (GUID) that identifies a new entry. In this example, the GUID is for illustration purposes only. The actual GUID that is generated when you run the command is unique.

   b. To set the safeboot option for the bootloader entry in the BCD store, type the following command using the generated GUID:

   ```
   bcdedit /set {GUID_value} safeboot dsrepair
   ```

   where *GUID_value* is the GUID displayed by the previous `bcdedit` command.

   c. To restart the system, exit the WinPE command prompt.

   Note

   Failure to start into DSRM results in a non-authoritative recovery.

3. (Optional) If you have a `WINDOWS ROLES AND FEATURES:\` Active Directory subcomponent save set that is newer than the `DISASTER_RECOVERY:\` save set used in the preceding BMR, you can recover the save set in DSRM through the NetWorker User program.

4. From the WinPE command prompt, run the Windows `ntdsutil` utility.

   The `ntdsutil` prompt appears. The `ntdsutil` utility is a command interface similar to the NetWorker recover interface. For help with the `ntdsutil` utility, type:

   ```
   NTDSUTIL: ?
   ```

5. At the `ntdsutil` prompt, type:

   ```
   NTDSUTIL: activate instance ntds
   NTDSUTIL: authoritative restore
   ```

6. To perform an authoritative recovery of a subtree or individual object, type:

   ```
   NTDSUTIL: restore subtree "distinguished_name"
   ```

   For example:

   ```
   NTDSUTIL: restore subtree
   "OU=engineering,DC=Seattle,DC=jupiter,DC=com"
   NTDSUTIL: restore subtree
   "CN=mars,CN=users,DC=Seattle,DC=jupiter,DC=com"
   ```

   The Microsoft Windows Server Resource Kit documentation on Active Directory provides information.

7. Exit the `ntdsutil` utility by typing **`quit`** at each successive `ntdsutil` prompt until the command prompt appears.
8. Type the following command at the WinPE command prompt so that the host does not start into DSRM mode on restart.

   ```
   bcdedit /deletevalue safeboot
   ```

9. Restart the domain controller in normal mode, log in, and then verify that the authoritative changes are replicated to the Active Directory replication partners.

Performing post-recovery tasks for hosts with Windows server roles that use SQL Server

Procedure

1. On the target host, rebuild the SQL server by running the following `Setup` command:

   ```
   Setup /QUIET /ACTION=REBUILDDATABASE /
   INSTANCENAME=Instance_name /SQLSYSADMINACCOUNTS=domain_name
   \administrator
   ```

   The Setup tool is located on the SQL Server installation media and must be run from the command prompt with Windows Administrator privileges. Before you run this command, ensure that the SQL group is offline except for the shared disks.

   The following Microsoft article provides more information:

   https://msdn.microsoft.com/en-us/library/ms189302

2. Bring the SQL sever services online.
3. Recover the SQL system databases (master, model, msdb) with NetWorker User for SQL Server, or a third-party application.

Performing post-recovery tasks for a Microsoft Hyper-V virtual machine

Use NMM to restore the Hyper-V virtual machines.

Troubleshooting Windows BMR

The following topics provide information to help troubleshoot Windows BMR operations.

Performing a manual uninstall and reconfigure of a NIC on Windows Server 2012 or Windows Server 2012 R2

If the guest operating system is Windows Server 2008 or Windows Server 2008 R2, the P2V BMR retains the NIC settings.

However, if the guest operating system is Windows Server 2012 or Windows Server 2012 R2, then Windows performs some Plug-N-Play configuration during the post-BMR restart. This activity disables the original NIC and creates a NIC.

Procedure

1. In the **Device Manager**, select **Display disabled devices** > **Uninstall the disabled NIC**.
2. Configure the new NIC with the wanted network settings.

Recovering and viewing Windows BMR log files

Windows BMR log files

To help troubleshoot an unsuccessful recovery, the following log files are generated and backed up during the Windows BMR operation:

- `daemon.raw`—This log file is the same as daemon.log for monitoring services.
- `Ossr_director.raw`—Contains the recovery workflow of the `DISASTER_RECOVERY:\` save set. This log also contains any errors that are related to recovering the save set files or Windows ASR writer errors.
- `recover.log`—Contains output from the NetWorker `recover.exe` program. This information is generated during the recovery of each save set. This log also contains messages about errors that are related to critical volume data recovery.
- `WinPE_Wizard.log`—Contains information about the workflow flow that is related to the NetWorker Bare Metal Recovery wizard user interface.
- `winpe_nw_support.raw`—Contains output from the `winpe_nw_support.dll` library. The output provides information about the communication between the NetWorker Bare Metal Recovery wizard and the NetWorker server.
- `winpe_os_support.log`—Contains output information that is related to Microsoft native API calls.

If the Windows BMR fails, you can recover the log files using one of the following options:

- By using FTP on the recovery host.
- By using a directed recovery.
- By copying the log files to a mapped drive.

If the Windows BMR was successful, you can recover the log files directly to the recovered host.

To view log files, you can use either a text editor or the `nsr_render_log` program, depending on the log file format.

Viewing the log files

To view the following log files, use a text editor:

- `recover.log`
- `WinPE_Wizard.log`

To view the following log files, use the `nsr_render_log` program:

- `Ossr_director.raw`
- `winpe_nw_support.raw`
  For example, to display the `Ossr_director.raw` file, type the following command at a command prompt:

  ```
  nsr_render_log "C:\logs\Client-bv1\Ossr_director.raw"
  ```

  To direct the `Ossr_director.raw` file to a text file that can be viewed in a text editor, type the following:

  ```
  nsr_render_log "C:\logs\Client-bv1\Ossr_director.raw" > mylog.txt
  ```

Accessing the log files using FTP

Procedure

1. On the recovery host, access the WinPE command line.

   You might have to exit the Windows Bare Metal Recovery wizard to access the WinPE command line. If you exit the wizard, do not restart.

2. Disable the Windows firewall.

   For example:

   ```
   wpeutil DisableFirewall
   ```

   By default, the Windows firewall is enabled on WinPE, and this action blocks the FTP port from transferring files.

3. Change to the following directory that contains the log files:

   ```
   X:\Program Files\EMC Networker\nsr\logs
   ```

4. To move the log files to another NetWorker host, use the FTP utility.

Accessing log files using a directed recovery operation

Procedure

1. To connect to the NetWorker server that backed up the source client data, start the NetWorker User program by using the `winworkr` command with the `-s` option:

   ```
   winworkr -s server_name
   ```

   If the `-s` option is not included, and there is only one server that is detected, that server is connected automatically. If there are no servers that are detected

or if there is more than one server available, the **Change Server** dialog box appears, enabling you to choose the server.

2. To open the **Source Client** dialog box, click **Recover**.
3. Select the source client, which is the recovered client, and then click **OK**.
4. Select the destination client for the recovered data, and then click **OK**.
5. From the **Options** menu, select **Options**, specify a folder location in which to relocate the recovered log files, and then click **OK**.
6. In the **Recover** window, select the log files to recover.

   The log files are typically located in the following directory:

   ```
   X:\Program Files\EMC Networker\nsr\logs
   ```

7. To begin the directed recovery, click **Start**.

   Recovering file system data, provides more information about the permissions that are required for directed recoveries.

BMR backup fails when System Reserved Partition is offline

BMR backups may fail with the following error:

```
device is not ready
```

Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 has 100 MB reserved as the System Reserved Partition. When backing up the system state, VSS includes the System Reserved Partition (used for BitLocker and Boot files), but the backup fails because the System Reserved Partition is offline. This can occur if the Windows automount capability is disabled. Although there are circumstances where the automount capability must be disabled, it can result in the partition being offline after a restart. Automount must be enabled for a BMR backup to succeed.

To work around this issue, use either of the following solutions:

Solution 1

From the command prompt, run `DISKPART` with the following commands:

`DISKPART`

`List volume`

`Select volume <number of 100 MB system partition>`

`Online volume` (if the volume is offline)

If automount is disabled while using third party storage software or if the user manually disabled the automount for the volume, the volumes can go offline.

This Microsoft KB article 2419286, available at http://support.microsoft.com/kb/2419286, provides details on preventing volumes from going offline by checking and setting the system automount attribute.

Solution 2

From the Disk Management console:

1. Access Disk Management from the command prompt:

```
C:\>Diskmgmt.msc
```

2. To bring the disk online, assign the drive letter to the 100 MB partition:
   a. Right-click the 100 MB volume, and then select **Change Drive Letter and Paths**.
   b. Assign a new drive letter to the volume.
      Assigning the drive letter ensures that the volume are online after a restart.

Wizard cannot locate the NetWorker server or DNS server

If the NetWorker Bare Metal Recovery wizard cannot locate the NetWorker server or the DNS server (if one is being used), consider the following:

- If you are using a local hosts file instead of a DNS server, verify that the hostname and IP address of the NetWorker server was typed correctly.
- If you are using a DNS server, verify that the values typed in the **Configure Hostname and Network** screen were typed correctly.
- Verify that the NetWorker server was correctly specified in the **Select NetWorker Server** screen.

To verify hostname and IP address values, use the ping utility that is in the WinPE environment:

1. Exit the NetWorker Bare Metal Recovery wizard but do not restart the host.
   You are returned to the WinPE command line.
2. To locate, and then verify hostnames and IP addresses, use the **ping** utility. For example:

   ```
   ping -a hostname
   ```

3. Restart the wizard. For example:

   ```
   javaw -jar WinPEWizard.jar
   ```

   Note

   After the wizard has been restarted, you can switch between the wizard and the WinPE command line without exiting the wizard.

Multiple NICs cause errors in locating the NetWorker server

An error message similar to the following might appear when you try to recover a host with multiple NICs:

```
Error retrieving the list of Networker servers
```

This message is an indication that the NIC selected by the wizard is not the NIC that was connected to the NetWorker server when the backup was performed and the NIC might not have connectivity to the server. This applies when searching for an available server or specifying a specific server. To resolve the issue, select another NIC.

Network configuration values might not be retained after reboot

Sometimes, a host does not retain its network configuration data after a Windows BMR operation and after the host starts. If the recovered host is experiencing network connectivity issues, confirm that network properties for the local connections are correct. If required, manually update the network configuration data on the host.

VSS backups fail because a critical disk is offline

VSS backups fail if a critical volume is offline during the backup operation. You can remedy the problem by following the steps that are outlined in the Microsoft Knowledgebase (KB) article 980794, which can be found at:

http://support.microsoft.com/kb/980794

The patch that is mentioned in this knowledgebase article is most likely on the Windows system if it is up-to-date. In this case, you can create and populate the Registry keys as described in the article.

This issue is most often encountered when backing up a passive node in an MSCS cluster and a critical volume is not on the physical host of the passive node but is instead on the physical host of the active node.

Jobquery fails to establish a connection with large scale jobs

When querying the number of save sets, jobquery fails to establish a connection with the jobsDB when the jobsDB contains more than 3,00,000 records.

The workaround is to run `nsradmin` from the command line with the following parameters:

```
nsradmin -S <jobsdatabse path>
```

8dot3name support disabled after recovery

In a WinPE 5.0 environment, `8dot3` file name support becomes disabled after recovery. This is not an issue from block-based backups.

If you require 8dot3name support, run the following command:

```
fsutil 8dot3name set C: 0
```

The Microsoft knowledgebase article 121007, available at http://support.microsoft.com/kb/121007, provides more information.

Additional recovery options

You can specify non-default recovery options on the WinPE command line or in the **Additional Options** field in the NetWorker Bare Metal Recovery wizard.

The following table describes the additional recovery options that can be used with a Windows BMR operation.

Table 8 Additional recovery options

Entry	Result
`-D x` where *x* is a number from 1 to 9, with 9 providing the most troubleshoot information and 1 providing the least.	Additional troubleshoot information is in the Windows BMR log files.
`-v`	Additional information on the progress of the recovery displays in the wizard's **System Recovery Status** window.

Table 8 Additional recovery options (continued)

Entry	Result
`-p`	By default, the Windows BMR recovery skips the formatting of non-critical disks. By using the `-p` option, any existing partitions are deleted and all disks are reformatted on the recovered computer to match the layout of the system image. However, by Microsoft specification, even if the `-p` option is selected, a non-critical volume is not reformatted if the disk signature has not changed since the backup. This option might be useful in situations where a system fails to recover because of disk mismatch errors. In this case, the `-p` option might resolve those errors. The recovery process does not recover non-critical volume data even if the volume is reformatted. Non-critical volumes can be recovered by using the NetWorker User program after the wizard has completed and the host has been restarted.
`recover -s <NetWorker server> -U -N "WINDOWS ROLES AND FEATURES \Cluster Database"`	When the restored data is meant to override the data on other nodes, it should be restored using the authoritative mode. Once this data is restored to one of the nodes, it is propagated to the other nodes and overwrites any newer data on those nodes. Perform Authoritative restore by using the command on the left. While the recovery is in progress, observe that the status of the groups changes from Online to Pending to Offline in the Failover Cluster Management application. Alternatively, check the Event Viewer, under **Application and Services Logs** > **Failover Clustering** > **Operational** on all nodes that the Cluster Service has stopped and restarted. Recover the shared drive data through *winworkr* on the cluster node with its current active node. Select **source client** as the virtual client, and **destination client** as the current active node.

Restart required after recovery operation

Newly recovered NetWorker client computers running Windows Server 2012 R2 can require an extra restart to restore access to application icons, previously viewable on the desktop.

CHAPTER 8

NetWorker Management Console (NMC) Disaster Recovery Procedures

This chapter contains the following topics:

- Recovering the NMC server to the same server 156
- Recovering the NMC server to a different server 160
- Configuring an NMC server database backup 164

Recovering the NMC server to the same server

The procedures to recover the NMC server to the same server differ for Linux and Windows.

Linux

Follow this procedure to recover the NMC server on Linux.

Prerequisites to recovering NMC server database

This section describes how to recover the NetWorker Management Console (NMC) server on a Linux environment.

Procedure

1. If required, install the operating system on the target NMC server.
2. On the target NMC server, install the NetWorker and NMC server software. When prompted to specify the NetWorker Authentication Service host, specify the same NetWorker Authentication Service host as the source NMC server.

   Refer to the *EMC NetWorker Installation Guide* for more information.
3. If you use a License Manager server, install and configure the License Manager software first. If you use the License Manager software and the License Manager server moves to a new host, specify the new License Manager hostname in the **Console** window.
4. If the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP, complete the procedure that is outlined in Special Circumstances to ensure that LDAP information is maintained.
5. During a recovery of the NMC server database, the console GUI is unavailable. Consequently, messages such as mount requests cannot be addressed from the console. Consider the following during a recovery of the NMC server database:
   - Monitor the daemon log files for messages. The use of the NetWorker `nsr_render_log` command can make the `daemon.log` file more user friendly for interpretation.
   - Use the `nsrwatch` command to view messages and use commands such as `nsrjb` to address those messages.
     The *EMC NetWorker Command Reference Guide* provides more information about `nsr_render_log`, `nsrwatch`, `nsrjb`, and other NetWorker commands.

Special Circumstances

To recover the LDAP authority files and the NMC database, follow these procedures.

Recover LDAP authority files

If the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP authentication, recover the LDAP authority files:

1. To recover all files in the `console_install_dir/cst` directory, use the `recover` command, the NetWorker User program, or the NMC Recovery wizard. Recover these files to the `console_install_dir/cst` directory on the target NMC server.

2. Configure the LDAP authorities on the recovered Console server before using the Configure Login Authentication wizard.

Recover the NMC database and keep the install directory intact

The recovery operation overwrites the existing database files. To recover the NMC database but keep the install directory intact, add the `-d <dir_name>` flag to the `recoverpsm` command. This step relocates the recovered files.

For example, type the following command:

```
recoverpsm -f -s <NetWorker_server> -c <source_NMC_server> -p
<AES_Passphrase> <staging_dir> -d <dir_name>
```

where:

- *NetWorker_server* is the name of the NetWorker server.
- *source_NMC_server* is the name of the source NMC server.
- *AES_Passphrase* is the passphrase that was specified for the NMC database backup.
- *staging_dir* is the staging directory specified during the backup of the database on the source NMC server.
- *dir_name* is the directory that is specified to relocate the recovered files.

Note

Use the `mminfo` command on the NetWorker server to determine the name of the staging directory.

The *EMC NetWorker Command Reference Guide* provides a complete description of the `recoverpsm` command line options.

Recovering the latest NMC backup into the same location

From the Windows NMC server, perform the following steps to recover the latest NMC backup that was taken on the original server into the same location.

Procedure

1. Stop the NMC server that is running on the server if it is started.

   ```
   C:\> net stop gstd
   ```

2. Change directory to the NMC bin directory.

   ```
   C:\>cd "<NMC Install directory>\GST\bin"
   ```

   By default, the NMC bin directory is located in `C:\Program Files\EMC NetWorker\Management`

3. Issue the recovery command:

   ```
   recoverpsm.exe -s <NetWorker_server_name> -c <client_name> -f
   ```

4. Start the NMC software:

   ```
   C:\> net start gstd
   ```

Windows

Follow this procedure to recover the NMC server on Windows.

Prerequisites to Recovering NMC Server

This section describes how to recover the NetWorker Management Console (NMC) server to the same server on a Windows environment.

To recover an NMC server from one host to another, both hosts must run on the same operating system.

Procedure

1. If required, install the operating system on the target server or perform a bare metal recover (BMR) of the host, if possible.
2. On the target NMC server, install the NetWorker and NMC server software. When prompted to specify the NetWorker Authentication Service host, specify the same NetWorker Authentication Service host as the source NMC server.

   Refer to the *EMC NetWorker Installation Guide* for more information.
3. If you use a License Manager server, then install and configure the License Manager software first. If you use the License Manager software and the License Manager server moves to a new host, then specify the new License Manager hostname in the **Console** window.
4. To ensure that LDAP information is maintained if the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP, complete the procedure that is outlined in Special Circumstances .
5. During a recovery of the NMC server database, the console GUI is unavailable. Consequently, messages such as mount requests cannot be addressed from the console. Consider the following during a recovery of the NMC server database:
   - Monitor the daemon log files for messages. The use of the NetWorker `nsr_render_log` command can make the `daemon.log` file more user friendly for interpretation.
   - Use the `nsrwatch` to view messages, and use commands such as `nsrjb`, to address those issues.
     The *EMC NetWorker Command Reference Guide* provides more information about `nsrwatch`, `nsrjb`, and other NetWorker commands.

Note

The recovery operation overwrites the existing database files. See Special Circumstances if you do want to overwrite the existing database files.

Special Circumstances

To recover the LDAP authority files and the NMC database, follow these procedures.

Recover LDAP authority files

If the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP authentication, recover the LDAP authority files:

1. To recover all files in the `console_install_dir/cst` directory, use the `recover` command, the NetWorker User program, or the NMC Recovery wizard. Recover these files to the `console_install_dir/cst` directory on the target NMC server.

2. Configure the LDAP authorities on the recovered Console server before using the Configure Login Authentication wizard.

Recover the NMC database and keep the install directory intact

The recovery operation overwrites the existing database files. To recover the NMC database but keep the install directory intact, add the `-d <dir_name>` flag to the `recoverpsm` command. This step relocates the recovered files.

For example, type the following command:

```
recoverpsm -f -s <NetWorker_server> -c <source_NMC_server> -p
<AES_Passphrase> <staging_dir> -d <dir_name>
```

where:

- *NetWorker_server* is the name of the NetWorker server.
- *source_NMC_server* is the name of the source NMC server.
- *AES_Passphrase* is the passphrase that was specified for the NMC database backup.
- *staging_dir* is the staging directory specified during the backup of the database on the source NMC server.
- *dir_name* is the directory that is specified to relocate the recovered files.

Note

Use the `mminfo` command on the NetWorker server to determine the name of the staging directory.

The *EMC NetWorker Command Reference Guide* provides a complete description of the `recoverpsm` command line options.

Recovering the latest NMC backup into the same location

From the Windows NMC server, perform the following steps to recover the latest NMC backup that was taken on the original server into the same location.

Procedure

1. Stop the NMC server that is running on the server if it is started.

   ```
   C:\> net stop gstd
   ```

2. Change directory to the NMC bin directory.

   ```
   C:\>cd "<NMC Install directory>\GST\bin"
   ```

   By default, the NMC bin directory is located in `C:\Program Files\EMC NetWorker\Management`

3. Issue the recovery command:

   ```
   recoverpsm.exe -s <NetWorker_server_name> -c <client_name> -f
   ```

4. Start the NMC software:

   ```
   C:\> net start gstd
   ```

Recovering the NMC server to a different server

The procedures to recover the NMC server to a different server differ for Linux and Windows.

Linux

Follow this procedure to recover the NMC server to a different server on Linux.

Prerequisites to recovering NMC server database

This section describes how to recover the NetWorker Management Console (NMC) server on a Linux environment.

Procedure

1. If required, install the operating system on the target NMC server.
2. On the target NMC server, install the NetWorker and NMC server software. When prompted to specify the NetWorker Authentication Service host, specify the same NetWorker Authentication Service host as the source NMC server.

   Refer to the *EMC NetWorker Installation Guide* for more information.
3. If you use a License Manager server, install and configure the License Manager software first. If you use the License Manager software and the License Manager server moves to a new host, specify the new License Manager hostname in the **Console** window.
4. If the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP, complete the procedure that is outlined in Special Circumstances to ensure that LDAP information is maintained.
5. During a recovery of the NMC server database, the console GUI is unavailable. Consequently, messages such as mount requests cannot be addressed from the console. Consider the following during a recovery of the NMC server database:
   - Monitor the daemon log files for messages. The use of the NetWorker `nsr_render_log` command can make the `daemon.log` file more user friendly for interpretation.
   - Use the `nsrwatch` command to view messages and use commands such as `nsrjb` to address those messages.
     The *EMC NetWorker Command Reference Guide* provides more information about `nsr_render_log`, `nsrwatch`, `nsrjb`, and other NetWorker commands.

Special Circumstances

To recover the LDAP authority files and the NMC database, follow these procedures.

Recover LDAP authority files

If the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP authentication, recover the LDAP authority files:

1. To recover all files in the `console_install_dir/cst` directory, use the `recover` command, the NetWorker User program, or the NMC Recovery wizard. Recover these files to the `console_install_dir/cst` directory on the target NMC server.

2. Configure the LDAP authorities on the recovered Console server before using the Configure Login Authentication wizard.

Recover the NMC database and keep the install directory intact

The recovery operation overwrites the existing database files. To recover the NMC database but keep the install directory intact, add the `-d <dir_name>` flag to the `recoverpsm` command. This step relocates the recovered files.

For example, type the following command:

```
recoverpsm -f -s <NetWorker_server> -c <source_NMC_server> -p
<AES_Passphrase> <staging_dir> -d <dir_name>
```

where:

- *NetWorker_server* is the name of the NetWorker server.
- *source_NMC_server* is the name of the source NMC server.
- *AES_Passphrase* is the passphrase that was specified for the NMC database backup.
- *staging_dir* is the staging directory specified during the backup of the database on the source NMC server.
- *dir_name* is the directory that is specified to relocate the recovered files.

Note

Use the `mminfo` command on the NetWorker server to determine the name of the staging directory.

The *EMC NetWorker Command Reference Guide* provides a complete description of the `recoverpsm` command line options.

Recovering the latest NMC backup to a different server

Perform the following steps to recover the latest NMC backup that was taken on the original NetWorker server to a different server.

NetWorker server

Perform the following steps on the NetWorker server.

Procedure

1. To identify the backup to be recovered, type the following command at a command prompt:

   ```
   -mminfo -ot -q client=NMCServer,level=full -r
   client,name,savetime,nsavetime
   ```

   where *NMCServer* is the NMC server name.

2. From the returned save sets, choose `NMCASA:/gst_on_<NMC_server_shortname>/lgto_gst`.
3. Note the *nsavetime* value from the `recover` command.

NMC server

Perform the following steps on the NMC server.

Procedure

1. Stop NMC software running in the server if it is started.

2. Set the appropriate library path environment variable to the following on your distribution of Linux:

   console_install_dir/postgres/lib

   The environment variable to set is **LD_LIBRARY_PATH**.

3. Change the directory to the NMC bin directory.
4. From the bin directory, run one of the following recovery commands below:
   - **recoverpsm -s <NetWorker_server_name> -c <client_name> -f -t <nsavetime_of_backup> -O**
   - **recoverpsm -s <NetWorker_server_name> -c <client_name> -f -O**
5. Recover the `gstd_db.conf` file.
6. To start the NMC software, type the `/etc/init.d/gst start` command.

Windows

Follow this procedure to recover the NMC server to a different server on Windows.

Prerequisites to Recovering NMC Server

This section describes how to recover the NetWorker Management Console (NMC) server to the same server on a Windows environment.

To recover an NMC server from one host to another, both hosts must run on the same operating system.

Procedure

1. If required, install the operating system on the target server or perform a bare metal recover (BMR) of the host, if possible.
2. On the target NMC server, install the NetWorker and NMC server software. When prompted to specify the NetWorker Authentication Service host, specify the same NetWorker Authentication Service host as the source NMC server.

   Refer to the *EMC NetWorker Installation Guide* for more information.
3. If you use a License Manager server, then install and configure the License Manager software first. If you use the License Manager software and the License Manager server moves to a new host, then specify the new License Manager hostname in the **Console** window.
4. To ensure that LDAP information is maintained if the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP, complete the procedure that is outlined in Special Circumstances .
5. During a recovery of the NMC server database, the console GUI is unavailable. Consequently, messages such as mount requests cannot be addressed from the console. Consider the following during a recovery of the NMC server database:
   - Monitor the daemon log files for messages. The use of the NetWorker `nsr_render_log` command can make the `daemon.log` file more user friendly for interpretation.
   - Use the `nsrwatch` to view messages, and use commands such as `nsrjb`, to address those issues.
     The *EMC NetWorker Command Reference Guide* provides more information about `nsrwatch`, `nsrjb`, and other NetWorker commands.

Note

The recovery operation overwrites the existing database files. See Special Circumstances if you do want to overwrite the existing database files.

Special Circumstances

To recover the LDAP authority files and the NMC database, follow these procedures.

Recover LDAP authority files

If the source NMC server managed NetWorker 8.2.x and earlier servers that use LDAP authentication, recover the LDAP authority files:

1. To recover all files in the `console_install_dir/cst` directory, use the `recover` command, the NetWorker User program, or the NMC Recovery wizard. Recover these files to the `console_install_dir/cst` directory on the target NMC server.
2. Configure the LDAP authorities on the recovered Console server before using the Configure Login Authentication wizard.

Recover the NMC database and keep the install directory intact

The recovery operation overwrites the existing database files. To recover the NMC database but keep the install directory intact, add the **-d <*dir_name*>** flag to the `recoverpsm` command. This step relocates the recovered files.

For example, type the following command:

```
recoverpsm -f -s <NetWorker_server> -c <source_NMC_server> -p
<AES_Passphrase> <staging_dir> -d <dir_name>
```

where:

- *NetWorker_server* is the name of the NetWorker server.
- *source_NMC_server* is the name of the source NMC server.
- *AES_Passphrase* is the passphrase that was specified for the NMC database backup.
- *staging_dir* is the staging directory specified during the backup of the database on the source NMC server.
- *dir_name* is the directory that is specified to relocate the recovered files.

Note

Use the `mminfo` command on the NetWorker server to determine the name of the staging directory.

The *EMC NetWorker Command Reference Guide* provides a complete description of the `recoverpsm` command line options.

Recovering the NMC backup taken on the original server to a different server

From the Windows NMC server, perform the following steps to recover the latest NMC backup that was taken on the original server to a different server.

NetWorker Server

Perform the following tasks on the NetWorker server that performed the NMC database backup.

Procedure

1. To identify the backup that you want to recover, run the following command:

   ```
   mminfo -ot -q client=<NMC server name>, level=full -r
   client,name,savetime,nsavetime
   ```

2. From the returned save sets, choose `C:\Program Files\EMC NetWorker\Management` from the date you require the recovery.
3. Note the *nsavetime* value for use in the `recoverpsm` command as outlined below.

NMC Server

Perform the following tasks on the NMC server.

Procedure

1. Stop NMC software running in the new server if it is started:

   ```
   C:\> net stop gstd
   ```

2. Change directory to the NMC bin directory.

   ```
   C:\>cd "<NMC Install directory>\GST\bin"
   ```

   By default, the NMC directory is located in `C:\Program Files\EMC NetWorker\Management\GST`

3. Recover the backup using either of the following commands:

   ```
   recoverpsm.exe -s <NetWorker_server_name> -c
   <New_NMC_server_name> -S gst_on_<old NMC server short name> -f -
   O
   ```

   Or

   ```
   recoverpsm.exe -s <NetWorker_server_name> -c
   <New_NMC_server_name> -S gst_on_<Old_NMC_server_short_name> -f -
   t <nsavetime_value_of_backup> -O
   ```

4. Recover the `gstd_db.conf` file.
5. Start the NMC software:

   ```
   C:\> net start gstd
   ```

Configuring an NMC server database backup

The first time that you connect to the NMC GUI, the Console Configuration wizard prompts you to configure an NMC server database backup. If you did not configure

the NMC database backup or you want to configure a new NetWorker server to backup the NMC server database, perform the following steps.

Before you begin

Connect to the NMC GUI with an account that has the Console Application Administrators role.

Procedure

1. On the toolbar, select **Setup**.
2. From the **Setup** window, select **Setup** > **Set Database Backup Server**.
3. In the **NetWorker server** field, specify the hostname of the NetWorker server that will backup the NMC server database.
4. Leave the **Create Client resource and add to the 'Server protection policy'** checkbox selected.
5. In the **Client name** field, specify the hostname of the NMC server.
6. Click **OK**.

Results

When you define an NMC database backup, the wizard performs the following actions on the NetWorker server:

- Creates a Client resource for the NMC server database backup. The **Save set** field for the client contains the path to the database staging directory. By default, the staging directory is in `C:\Program Files\EMC NetWorker\Management\nmcdb_stage` on Windows and `/opt/lgtonmc/nmcdb` on Linux.

  Note

  The file system that contains the staging directory must have free disk space that is a least equal to the size of the current NMC database. The section "Changing the staging directory for NMC database backups" in the *EMC NetWorker Administration Guide* describes how to change the staging directory location.

- Creates a group called NMC server.
- Adds the Client resource to the NMC server group.
- Creates a workflow that is called NMC server backup in the Server Protection policy. The workflow contains the NMC server backup action, which performs a full backup of the NMC server database every day at 2 P.M.
- Adds the NMC server group to the NMC server backup workflow.

Note

The NMC server database backup only supports the full and skip backup levels. If you edit the NMC server backup action and change the levels in the backup schedule to a different level, for example synthetic full, NetWorker performs a full backup of the database.