



**EMC® NetWorker®
Module for Documentum®**

**Release 1.2
Multiplatform Version**

Best Practices Guide

**P/N 300-004-661
REV A01**

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright © 2004 - 2007 EMC Corporation. All rights reserved.

Published September, 2007

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

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

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

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

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

Preface 7

Chapter 1 NMD Best Practices

- 1. Objectives 12
- 2. Overview of NMD 12
 - 2.1. Conditions for backups with the SnapImage Module 13
 - 2.2. Conditions for backups without the SnapImage Module 14
- 3. Software components 15
- 4. Prerequisites and checklist 15
 - 4.1. NetWorker hardware and software prerequisites 15
 - 4.2. NetWorker software prerequisites 16
 - 4.3. NetWorker server sizing 16
- 5. Installation overview 19
- 6. Configuration overview 19
 - 6.1 Recommended parameter settings in the configuration file 19
- 7. Overview of quick usage and verification 21
 - 7.1. Manual NMD backup 22
 - 7.2. Scheduled NMD backup 23
 - 7.3. Backup index query 23
 - 7.4. Change of directory ownership and permissions during a restore... 25
 - 7.5. Content file restore 26
 - 7.6. Database and log restore 27
 - 7.7. Other component restore 28
- 8. Troubleshooting tips 31
- 9. Optimization recommendations 31
 - 9.1. Parallelism for restores 31
 - 9.2. SnapImage optimization 31
 - 9.3. Other optimization 31
- 10. Special use case recommendations 32
 - 10.1. Backups 32
 - 10.2. Restores 33
 - 10.3. UNIX symbolic links and mount points 34
- 11. Related documentation 34

Appendix A NMD Consulting Pre-site Qualifier (CPSQ)

Appendix B NetWorker Best Practices

- B.1. Solution methodology: An industry best practice 40

B.2. Datazones 40
B.3. Single datazone 41
B.4. Network best practices..... 45
B.5. SAN best practices 45
B.6. Business best practices 46
B.7. NetWorker best practices 46
B.8. NetWorker 7.x best practices 47

	Title	Page
1	Sample nsrnm _{sv} commands for different types of backups	22
2	Backup information displayed by the nsrnm _{sv} command	22
3	Sample nsrnm _{dx} commands for index searches	23
4	Backup information displayed by the nsrnm _{dx} command	24
5	Sample nsrnm _{dcr} command for file report searches	26
6	Oracle database restore	27
7	Sample nsrnm _{drs} commands for different types of restores	28
8	Restore information displayed by the nsrnm _{drs} command	29

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

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

Audience

This document is part of the EMC NetWorker Module for Documentum (NMD) documentation set. The guide is intended for use by professional services consultants and the Documentum administrators who are responsible for maintaining the Documentum Content Server and database server backup and restore system. Operators who monitor the Documentum data backups may also find this best practices guide useful.

Readers of this document are expected to be familiar with the following topics:

- ◆ Documentum and relevant database terminology and concepts, especially those related to backups and restores
- ◆ Backup and restore procedures on a Documentum Server
- ◆ Disaster recovery procedures on a Documentum Server

Related documentation

Documentation related to the use of this product can be found on the EMC Powerlink website, <http://Powerlink.EMC.com>, including:

- ◆ The NetWorker Module for Documentum release 1.2 documentation set:
 - Administration guide
 - Installation guide
 - Release notes
 - Best practices guide
 - Command reference guide
- ◆ The NetWorker documentation set:
 - Administration guide
 - Installation guide
 - Release notes
 - Command reference guide
 - Disaster recovery guide
- ◆ Appropriate versions of the following documentation sets:
 - NetWorker Module for DB2
 - NetWorker Module for Microsoft SQL Server
 - NetWorker Module for Oracle

- NetWorker Module for Sybase
- NetWorker SnapImage Module
- ◆ Other EMC documentation:
 - *Software Compatibility Guide*
 - UNIX man pages

The following additional documentation may be useful:

- ◆ Documentum Content Server documentation
- ◆ Appropriate database (IBM DB2, Microsoft SQL Server, Oracle, or Sybase) backup and recovery documentation

Conventions used in this document

EMC uses the following conventions for special notices.

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



IMPORTANT

An important notice contains information essential to operation of the software.

Typographical conventions

EMC uses the following type style conventions in this document:

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

	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces indicate content that you must specify (that is, x or y or z)
...	Ellipses indicate nonessential information omitted from the example

Where to get help EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:

<http://Powerlink.EMC.com>

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Your comments Comments and suggestions about our product documentation are always welcome.

To provide feedback:

1. Go to:
<http://Powerlink.EMC.com>
2. Click the **Feedback** link.

This guide describes the best practices for installing, configuring, and using the EMC NetWorker Module for EMC Documentum (NMD) release 1.2 on a Documentum Server host with a supported UNIX or Microsoft Windows operating system.

Note: The *Software Compatibility Guide* on the EMC Powerlink website on <http://Powerlink.EMC.com> provides detailed information on the specific operating system versions that NMD supports.

The NMD software is distributed in a downloadable file, available from the EMC website.

This guide includes the following sections:

◆ 1. Objectives	12
◆ 2. Overview of NMD	12
◆ 3. Software components	15
◆ 4. Prerequisites and checklist.....	15
◆ 5. Installation overview	19
◆ 6. Configuration overview	19
◆ 7. Overview of quick usage and verification.....	21
◆ 8. Troubleshooting tips	31
◆ 9. Optimization recommendations	31
◆ 10. Special use case recommendations	32
◆ 11. Related documentation.....	34

1. Objectives

This best practices guide provides a quick summary of key installation and administration steps as well as basic concepts for EMC® NetWorker® Module for EMC Documentum® (NMD). It also provides information on special configuration settings, optimization tuning, use case handling, and answers to general questions about the software.

This guide supplements the following documents:

- ◆ *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Installation Guide*
- ◆ *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Administration Guide*
- ◆ *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Release Notes*

2. Overview of NMD

NMD enables the Documentum repository administrator to perform streamlined backups and restores of one or more physical components of an online Documentum Content Server Document Base (docbase or repository). A *consistent* repository backup image is produced during the backups.

Note: The Documentum 5.3.x and 6.x term *repository* is synonymous with the Documentum 5.2.x term *docbase*.

NMD software works with the following software components to create a comprehensive Documentum data protection system:

- ◆ Documentum Content Server
- ◆ Documentum database server
- ◆ (Optional) Documentum full-text index server
- ◆ NetWorker server
- ◆ NetWorker client
- ◆ NetWorker storage node
- ◆ (Optional) NetWorker Module for the database
- ◆ (Optional) NetWorker SnapImage™ Module
- ◆ (Optional) NDMP TapeServer on Windows *only*

The *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Administration Guide* provides more information on the software components and features, consistency in repository backups, and how to perform backups of storage areas with and without the NetWorker SnapImage Module.

NMD can use the SnapImage Module for snapshot backups of the storage area components. The following two limitations apply to the SnapImage Module:

- ◆ SnapImage software can back up an entire file system *only*. SnapImage cannot back up just the parts or directories under a file system.
- ◆ SnapImage fast restore mode is fully destructive and *cannot* be used by NMD.

Note: If storage areas share a file system with other applications, consider the possible case where the restore of a SnapImage backup of the storage areas might require a destructive restore. The *EMC NetWorker Module for Documentum Administration Guide* provides more information.

The following sections provide conditions for performing backups with and without the SnapImage Module:

- ◆ [“2.1. Conditions for backups with the SnapImage Module” on page 13](#)
- ◆ [“2.2. Conditions for backups without the SnapImage Module” on page 14](#)

The *EMC NetWorker Module for Documentum Administration Guide* also provides caveats for the use of the SnapImage Module.

2.1. Conditions for backups with the SnapImage Module

Consider performing backups *with* the SnapImage Module if the following approximate conditions apply:

- ◆ SnapImage supports the current Documentum Server platform (operating system version, file system or volume manager software, disk hardware).
- ◆ The total number of content files for all storage areas on each file system or drive is greater than approximately 2 million, and the average content file size is less than approximately 150 KB.

Note: The fewer the number of files and/or the greater the average file size, the less is the density (number of files per GB) of the file system. SnapImage is recommended for high-density file systems only.

- ◆ The storage areas on each file system make up more than 75 percent of the file system’s total used space. There is little nonstorage area data on the storage area file systems.
- ◆ The storage areas on each file system make up more than 75 percent of the overall number of files on the file system. There is little nonstorage area data on the storage area file systems.
- ◆ Extra memory and disk space is available for SnapImage file history work areas, caches, and general processing.
- ◆ For consistent repository backups, there are as many SnapImage caches as storage area file systems.

Note: Storage area file system backups must all be performed in parallel to minimize the number of disconnected or orphaned content files written to the storage area backup image.

- ◆ The storage area file systems have little disk write activity (for example, system or application logging) that cannot be redirected to a nonstorage area file system.
- ◆ The Oracle control files and online redo logs are *not* located on a disk that is backed up by SnapImage.

Note: SnapImage operations can cause the termination of an Oracle instance on the same file system.

- ◆ On Windows, the Documentum Server’s default port 10000 can be changed.

- ◆ It is acceptable that SnapImage modifies the operating system file system stack to insert its disk write interceptor driver.
- ◆ You have expertise to maintain the SnapImage environment, and you accept the caveats listed in the SnapImage documentation.

The following EMC documentation provides more information on the supported releases of the SnapImage Module:

- ◆ *EMC NetWorker Module for Documentum Release Notes*
- ◆ *Software Compatibility Guide*

2.2. Conditions for backups without the SnapImage Module

Consider performing backups *without* the SnapImage Module if one or more of the following approximate conditions apply:

- ◆ The total number of content files for all storage areas on each file system or drive is fewer than approximately 2 million, and the average content file size is equal to or greater than approximately 150 KB.
- ◆ The storage areas on each operating system file system occupy less than 75 percent of the file system's total used space. That is, there is a significant amount of nonstorage area data on the storage area file systems.
- ◆ The storage areas on each operating system file system occupy less than 75 percent of the overall number of files on the file system. That is, there is a significant amount of nonstorage area data on the storage area file systems.
- ◆ The storage area file systems have significant disk write activity (for example, system or application logging) that cannot be redirected to a nonstorage area file system.
- ◆ The Oracle control files and online redo logs are located on a disk that is backed up by SnapImage and cannot be relocated for business reasons.

Note: SnapImage operations can cause the termination of an Oracle instance on the same file system.

- ◆ On Windows, the Documentum Server's default port 10000 cannot be changed for business reasons.
- ◆ There is not extra memory and disk space for SnapImage file history work areas, caches, and general processing. Furthermore, for consistent repository backups, you do not have as many SnapImage caches as there are storage area file systems. (Storage area file system backups must all be in parallel to minimize the number of orphaned content files written to the storage area backup image.)
- ◆ The system cannot risk SnapImage modifying the operating system file system stack to insert its disk write interceptor driver.
- ◆ You do not have expertise to maintain your SnapImage environment and/or you are uncomfortable with any one or more of the several caveats listed in the SnapImage guides.
- ◆ The current Documentum platform (for example, operating system version, file system or volume manager software, disk hardware) is not supported by SnapImage and you cannot change the platform.
- ◆ You intend to regularly back up a storage area by itself, and there is more data on that storage area's file system.

3. Software components

The *EMC NetWorker Module for Documentum Administration Guide* provides information on the NMD software components and how the components interact with the NetWorker software during backup and restore operations.

4. Prerequisites and checklist

Best practices require that the customer environment has the recommended hardware and the software is properly configured prior to initiating implementation processes. The following documents provide the basic prerequisites for the NMD and NetWorker software:

- ◆ *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Installation Guide*
- ◆ *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Administration Guide*
- ◆ *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Release Notes*

The following sections provide additional NetWorker prerequisites:

- ◆ [“4.1. NetWorker hardware and software prerequisites” on page 15](#)
- ◆ [“4.2. NetWorker software prerequisites” on page 16](#)
- ◆ [“4.3. NetWorker server sizing” on page 16](#)

4.1. NetWorker hardware and software prerequisites

Ensure that the following NetWorker hardware prerequisites are met:

- ◆ Legacy disk or tape devices can be used with the NetWorker software. The devices must be non-NDMP devices, with the NDMP flag set to NO.
- ◆ For sufficient parallelism, multiple devices are used. In the NetWorker Device resource for each device, the Target Sessions attribute is set to four or greater. In the NetWorker Client and Server resources, the Parallelism attribute value is increased accordingly.

Note: [“6.1 Recommended parameter settings in the configuration file” on page 19](#) provides information on parallelism parameter settings in the NMD configuration file.

- ◆ All hosts are installed, configured, and operating on the network and SAN, if applicable.
- ◆ All hosts can **ping** the servers which will be the NetWorker server and storage nodes.
- ◆ If using DNS for name resolution, all hosts can perform reverse DNS lookups of hostnames by using IP addresses. For example, if there is a client named web1.legato.com with the IP address 137.69.200.8, enter the following **nslookup** command:

```
nslookup 137.69.200.8
Server: ns.legato.com
Address: 137.69.200.200
Name: web1.legato.com
Address: 137.69.200.8
```

In this example, **nslookup** returned the proper hostname for the address, web1.legato.com. If **nslookup** does not report the proper hostname or any hostname, then the DNS configuration must be corrected.

- ◆ There is enough space allocated to the NetWorker server for the client indexes. Typically, this space should be on its own file system. Additionally, the EMC best practice is that this space is *not* on a RAID 5 type disk device. A RAID 1+0 disk device is the most preferable disk configuration for the indexes, although it is not required. NetWorker documentation provides more information.
- ◆ All tape libraries and tape devices are installed, configured, and working properly.
- ◆ All tape devices are seen and accessed by native operating system utilities on systems that are connected directly to the devices or to a SAN. The utilities include Windows Backup on Windows 2000 systems, and **mt** or **tar** on UNIX systems.
- ◆ All SAN components such as host bus adapters (HBAs), bridges, switches, hubs, routers, MUXs, and so on are installed and working properly.
- ◆ The latest firmware is installed on all SAN bridges, switches, hubs, routers, MUXs, and so on. New devices do not always have the latest firmware. Contact the vendor representative or manufacturer website for verification of the latest firmware.
- ◆ Ensure that the SAN switches are zoned properly so that the NetWorker server and any storage nodes can access the appropriate tape drives and/or disk arrays.
- ◆ If restore testing will be performed, ensure that an appropriate environment is available. This may be a separate directory to restore files, a separate database instance on a production machine, or possibly a completely separate server, depending on the restores to be tested.

4.2. NetWorker software prerequisites

Ensure that the following software prerequisites are met:

- ◆ All EMC software products have been purchased and delivered. EMC Consulting does not deliver any software media or manuals. If any products have not been received, contact your EMC Sales Representative or Reseller.
- ◆ All database applications which will be backed up through NetWorker modules have been installed, configured, and are running.
- ◆ Required operating system patches are installed. Information on these can be found in the *EMC NetWorker Installation Guide* and/or *EMC NetWorker Release Notes*.

4.3. NetWorker server sizing

This section addresses the higher level server sizing for data transfer to a tape or disk target. This is not a complete server architecture sizing guide. For instance, it discusses the amount of memory and memory transfer speed. It does not address types and speeds of the memory chips themselves, nor does it discuss the details of how many HBAs a computer can support. The local engineers and vendors decide this level of detail after the data transfer requirements are determined.

There are basically two avenues that can be followed to determine the number of target drives and supporting server specifications:

1. Determine server specifications based on the appropriate number of target drives.
2. Determine the number of target drives that can be supported based on a current server's specifications.

4.3.1. Server sizing factors

No matter which avenue is followed, the following information is critical to determine the "right fit." Obtain the information from the appropriate hardware vendor:

- ◆ Target drive I/O rate in MB/s
- ◆ Expected ratio of compression
- ◆ CPU speed in MHz
- ◆ Memory bus speed in MB/s = (memory bus MHz * bus width) / 8
- ◆ Speed of peripheral buses
- ◆ HBA or SCSI card speed
- ◆ Number of cards that can be supported
- ◆ Method of delivery for data being protected (network versus direct)
- ◆ Capabilities and bandwidth of network interface card (NIC)

For example, does a GBE NIC have a TCP Offload Engine (TOE) to offset the main CPU resource use?

Kernel and resource requirements (file descriptors, memory heap) must also be properly configured in the operating system. The operating system documentation provides information on kernel tuning.

The modifiers to server sizing are the following:

- ◆ Data change rate
- ◆ Frequency of backup
- ◆ Frequency and type of target drive operations (clone, archive, stage, recover, use of B2D)

These modifiers can increase or reduce the resources needed for server sizing, but are outside the scope of this discussion.

4.3.2. Server sizing example

In the following tape-specific example, the calculations are approximations. Some of the formulas are based on lab testing of certain devices and extrapolated for others. For example, if it takes 200 MHz to support a DLT7000 tape drive writing at 18 MB/s, then by extrapolation 400 MHz of CPU is required to drive a device at 36 MB/s.

4.3.2.1. Sizing example assumptions

The following assumptions are made:

- ◆ The 9840Bs used in the "CustomerX datazone" have a native speed of 19 MB/s, so 200 Mhz of CPU should be used for each drive, but that does not allow for compression.
- ◆ There are four 600 Mhz CPUs.
- ◆ There is 4 GB of memory.
- ◆ STK has recommended a limit of two 9840Bs per HBA.

- ◆ There are two HBAs, each having a 2 GB/s transfer rate.
- ◆ During the time frame of the health check, the number of 9840B drives per HBA was reduced from five to four and finally to three, for a total of six 9840B tape drives on the NetWorker server.
- ◆ One GBE NIC is being used for network backups.
- ◆ The memory bus transfer speed is unknown.
- ◆ The fibre-ready 9840Bs are behind a new 2 GB/s IBM fibre switch.

To perform a thorough analysis, you need to determine: the memory bus transfer rate, the transfer rate of the fibre switch, and whether the GBE NIC is TOE enabled.

4.3.2.2. Sizing example logic flow

The responses to the following questions are based on the known NetWorker server specifications:

1. Is one GBE NIC sufficient to keep six 9840B tape drives spinning?

Answer: No

Assumption: The GBE NIC operates at 60 percent of the theoretical speed (60 MB/s).

With the native rate of six 9840B drives being a total of 114 MB/s, an input rate provided by a single GBE NIC is insufficient to keep six tape drives writing at capacity even with 1:1 compression, especially with higher compression rates.

2. Are there enough CPUs to support six 9840B tape drives?

Answer: Possibly

Using the model of # CPUs = (n+1) and considering that the 9840B drives require 200 MHz of CPU to write at 1:1 compression and 300 MHz for 1:1.5 compression, three 600 MHz/s CPU drives should be sufficient for six tape drives, with one left to be dedicated to processing. However, performance may decrease if the GBE NIC is not TOE enabled and requires a portion of processing power expected to be used for I/O to the 9840B drives.

3. Are two HBAs sufficient to support six 9840B drives?

Answer: Yes

Assumption: The HBAs in use have a true transfer rate of 2 GB/s.

At 1:5 compression and a 2 GB/s HBA transfer rate (2000 MB/s) and with three 9840B drives being written to at an I/O rate of approximately 90 MB/s, the tape drive-to-HBA ratio can support the six 9840B drives. However, remember that STK has recommended only two 9840B drives per HBA.

4. Are the internal bus transfer rates sufficient?

Answer: Unknown

As previously stated, it is very important to know the memory bus transfer rate to determine if the data can be transferred from the GBE NIC to the CPU to the HBA to the 9840B at the necessary transfer rate.

4.3.2.3. Conclusion

The current configuration of the NetWorker server is insufficient to support six 9840B tape drives because only one GBE NIC is used to bring in the data. More information is needed about the specifications of the GBE NICs in use before it can be determined whether using another NIC is of any benefit.

5. Installation overview

The *EMC NetWorker Module for Documentum Installation Guide* provides detailed information on installing the required software on the Documentum Server (also known as the NMD NSR client) and any additional hosts.

6. Configuration overview

The *EMC NetWorker Module for Documentum Administration Guide* provides detailed information on the configurations required for NMD backup and restore operations, including configurations of the following:

- ◆ Required NetWorker resources, including Client, Device, Group, Pool, and Server resources.

Note: To ensure proper backups of client indexes on all remote hosts and the successful disaster recovery of the remote hosts, the required Client and Group resources must be configured according to the instructions in Chapter 2 of the *EMC NetWorker Module for Documentum Administration Guide*.

- ◆ Optional SnapImage Module, if used for snapshot backups of storage areas.
- ◆ Mandatory and optional parameters in the NMD configuration file.

[“6.1 Recommended parameter settings in the configuration file”](#) on page 19 provides recommended settings for the NMD configuration parameters.

Note: To safeguard the configuration file on UNIX or Linux, copy the sample configuration file to a *nondefault* location before customizing the parameter settings in the file. If the NMD software is uninstalled, the sample file in the default location is also uninstalled.

- ◆ Remote database or full-text index server.
- ◆ Distributed storage areas, a *new* feature supported by NMD release 1.2.

To optimize the backup performance for remote hosts in a distributed storage area configuration, configure each remote Content Server as its own storage node.

6.1 Recommended parameter settings in the configuration file



IMPORTANT

Before you start any type of NMD backup, ensure that the *mandatory* parameters are set. Specific parameters are mandatory, depending on how NMD will be used. The *EMC NetWorker Module for Documentum Administration Guide* provides complete details on the configuration file parameters.

The following are recommended parameter settings in the NMD configuration file:

- ◆ NMD_APPEND_TASK_LOGS=yes
- ◆ NMD_DIRECTIVES_FILE=*NetWorker_directives_filepath*
- ◆ NMD_HOST_SAS_MAP=*hostname1,storage_area_name1[,storage_area_name2,...]*
NMD_HOST_SAS_MAP=*hostname2,storage_area_name1[,storage_area_name2,...]*

Used optionally for distributed storage areas *only*, NMD_HOST_SAS_MAP provides information for the mapping of storage areas to a particular host. The configuration file on the primary host can include one or more settings of the parameter, with a maximum of one setting for each different host in the distributed storage area configuration. The parameter is recommended in the following cases:

- To clarify the storage area mappings in a shared distributed storage area setup.
 - To override any misconfigured values in the far store lists of the Content Servers.
 - To distinguish between the similar locations of storage area physical paths on the different hosts.
- ◆ NMD_SA_FULL_NUM_SAVESET=16 (for nonsnapshot backups of storage areas; tune accordingly)

This is the approximate number of save sets for each full nonsnapshot backup of a storage area. For example, if you have only two large storage areas and each is 200 GB, a value of 25 to 50 might be better since the ideal upper limit for NetWorker save set sizes is approximately 4 to 8 GB (200 GB/50). The default value is 10.

- ◆ NMD_SA_INCR_NUM_SAVESET=4 (for nonsnapshot backups of storage areas; tune accordingly)

This is the approximate number of save sets for each incremental nonsnapshot backup of a storage area. The default value is 2.

- ◆ NMD_USE_DEFAULT_SAVESET_NAMES=yes
- ◆ NMD_USE_SNAPIMAGE=yes or no
 - For snapshot backups of storage areas, set to yes (mandatory).
 - For nonsnapshot backups, set to no or comment out the parameter.

- ◆ NSR_DEBUG_FILE=*debug_logfile_pathname*

The value “default” causes the default debug log file to be used:

- On UNIX or Linux:
/nsr/applogs/nsrnmdiv.pid.log or /nsr/applogs/nsrnmdivr.pid.log
 - On Windows:
install_path\nsr\applogs\nsrnmdiv.pid.log or
install_path\nsr\applogs\nsrnmdivr.pid.log
- ◆ NSR_DEBUG_LEVEL=*debug_level*

Debug levels from 0 to 9 are supported.

- A level of 9 produces the maximum trace logging.
- A level of 0 (default) produces no logging, which is suitable for normal production use.

To reduce the size of the NMD debug log file, set NMD_DRIVER_DELAY_SECS to 10 or greater.

- ◆ NSR_PARALLELISM=8 or 16 (recommended for nonsnapshot backups)

Alternatively, comment out NSR_PARALLELISM and set NMD_SAVE_PARALLELISM and NMD_RESTORE_PARALLELISM to separate values.

- ◆ `NSR_QUIET=yes`
When set to no or commented out, and `NSR_DEBUG_LEVEL` is 1 or greater, NMD backup and restore tasks generate detailed debug information.
- ◆ `NSR_SNAPIMAGE_DATA_VOLUME_POOL=NetWorker_pool_name`
This volume pool is used exclusively for save sets from SnapImage backups of the storage areas.

7. Overview of quick usage and verification

Verify the NMD configuration by performing small-sized manual backups and then isolated restores to a relocation directory. Monitor any error or warning messages sent to the screen or designated command session log file. The troubleshooting section of the *EMC NetWorker Module for Documentum Administration Guide* provides more information on quick verification tests and troubleshooting.

To verify that all backup and restore operations are functioning properly, perform the following:

1. Without using NMD, test a SnapImage backup and restore by entering the following commands:


```
nsrndmp_save -c NMD_client -M -T type
small_file_system_or_drive_fullpath
```

 where *type* is **image** (for Windows) or **celestra** (for UNIX).


```
nsrndmp_recover -s NetWorker_server -c NMD_client
-r raw_device_pathname -S save_set_ID
```
2. Back up the installation and configuration files by entering the **nsrmdsv -M ICF** command.
3. Back up the full-text index by entering either the **nsrmdsv -M FTI -a full-text_index_name** or **nsrmdsv -M FTI_ALL** command. (With Documentum 5.3.x and later, the scopes **FTI** and **FTI_ALL** both back up a single full-text index only.)
4. Back up one small, in-use storage area by entering the **nsrmdsv -M SA -a small_storage_area_name** command.
5. Back up the database by entering the **nsrmdsv -M DB** command.
6. Query the previous backups by entering the **nsrmdnx** command and inspect the command output.
7. Restore the installation and configuration files to a relocation directory on a file system with adequate disk space by entering the **nsrmdrs -d relocation_dir -C ICF** command. Quickly validate the restored data.
8. Restore the full-text index to the same relocation directory by entering the **nsrmdrs -d relocation_dir -C FTI** command.
9. Restore a single content file by entering, for example, the **nsrmdcr -B repository_name -A filestore_name -P filereport_path -T timebound -d doc_name -D relocation_dir** command.
10. Restore the small storage area to the same relocation directory by entering the **nsrmdrs -d relocation_dir -C SA -a small_storage_area_name** command.

11. Run a scheduled backup of the installation and configuration files:

Note: In a distributed storage area configuration, the installation and configuration files can be backed up on the primary host only, *not* on any remote hosts.

- a. Perform one of the following:
 - Set NMD_SCOPE=ICF (temporarily) in the NMD configuration file.
 - Specify the **nsrnm~~sv~~** **-M ICF** command in the Backup Command attribute of NetWorker Client resource.
 - b. Perform one of the following:
 - Schedule the backup through the NetWorker Administrator program.
 - Start the backup by entering the **savegrp -c NMD_client_name** command on the NetWorker server.
 - c. When the backup finishes, clear the relocation directory.
 - d. Query the backup by entering the **nsrnm~~dx~~** command and inspect the command output.
 - e. Remove the temporary settings (possibly NMD_SCOPE=ICF) from the NMD configuration file.
12. Run a scheduled backup of the entire Documentum system. This might take a long time, depending on the repository size and whether a file report dump is requested (the default).

7.1. Manual NMD backup

To perform a manual (unscheduled) NMD backup, enter the **nsrnm~~sv~~** command at the operating system command line, as either the root user on Solaris or a member of the Microsoft Windows Administrators group.

The *EMC NetWorker Module for Documentum Administration Guide* provides more information on the **nsrnm~~sv~~** command and its options.

Example 1 Sample nsrnm~~sv~~ commands for different types of backups

The following **nsrnm~~sv~~** command performs a Documentum system backup of the repository docora10:

```
nsrnmsv -B docora10 -f /space10/home/dmuser/nmd.cfg -M ALL -l full
```

The following **nsrnm~~sv~~** command performs an incremental system backup of the repository docora10:

```
nsrnmsv -B docora10 -f /space10/home/dmuser/nmd.cfg -M ALL -l incr
```

The following **nsrnm~~sv~~** command performs an incremental backup of the storage area named filestore_01 of the repository docora10:

```
nsrnmsv -B docora10 -f /space10/home/dmuser/nmd.cfg -M SA  
-a filestore_01 -l incr
```

Example 2 Backup information displayed by the nsrnm~~sv~~ command

The following **nsrnm~~sv~~** command performs an incremental backup of the storage area named nmdVitFS01 for the repository repo_vit by using the NetWorker server ivy:

```
nsrnmsv -f /nsrnm_unix.cfg -M SA -a nmdVitFS01 -s ivy -l incr
```

The **nsrnmdev** command displays the following information during the backup process:

```
09/06/07 10:36:14 nsrnmdev: Writing debug messages to
/nsr/applogs/nmd.log
09/06/07 10:36:50 nsrnmdev: NMD backup is successful.
09/06/07 10:36:50 nsrnmdev: Generating filereports...
09/06/07 10:36:59 nsrnmdev: The SA nmdVitFS01 has no records.
09/06/07 10:36:59 nsrnmdev: No file report for the SA was generated.
09/06/07 10:36:59 nsrnmdev: The filereport step completed
successfully.
completed savetime=1189055210
```

7.2. Scheduled NMD backup

To perform a scheduled NMD backup, specify the **nsrnmdev** command in the Backup Command attribute of the Client resource on the NetWorker server. [“7.1. Manual NMD backup” on page 22](#) provides more information on the **nsrnmdev** command.

Ensure that the other NetWorker resources required for a scheduled backup are configured, as described in the *EMC NetWorker Module for Documentum Administration Guide*.

In the output from every NMD scheduled backup that includes a remote host (remote database, full-text index, or storage area host), the following warning message appears:

```
WARNING!: The NetWorker indexes for the remote hosts are not
automatically backed up during scheduled backups. The NetWorker
indexes for the clients listed below may not be backed up. Please see
the NMD documentation for more information.
client1
client2
...
```

To ensure proper scheduled backups of client indexes on all remote hosts and the successful disaster recovery of the remote hosts, the required Client and Group resources must be configured according to the instructions in Chapter 2 of the *EMC NetWorker Module for Documentum Administration Guide*.

7.3. Backup index query

To browse and display the NMD backup index information, enter the **nsrnmdev** command. For example, if only the mandatory **-B** option is specified for the repository name, the **nsrnmdev** command displays the records for every backup of the repository, starting with the most recent record and ending with the oldest.

The *EMC NetWorker Module for Documentum Administration Guide* provides more information on the **nsrnmdev** command and its options.

Example 3 Sample nsrnmdev commands for index searches

The following **nsrnmdev** command searches on the NetWorker server jupiter for all the backup records of the repository docora10 that belong to the client mars:

```
nsrnmdev -B docora10 -c mars -s jupiter
```

The following **nsrnmdev** command searches for all the incremental backups of scope SA for the storage area named filestore_01 in the repository docora10 that occurred after the last week:

```
nsrnmdev -B docora10 -M SA -a filestore_01 -L "last week" -l incr
```

The following **nsrnmidx** command searches for all the backups of scope FTI_ALL containing the full-text indexes of the repository docora10 that occurred between last week and yesterday:

```
nsrnmidx -B docora10 -M FTI_ALL -L "last week" -U yesterday
```

Example 4 Backup information displayed by the nsrnmidx command

The following **nsrnmidx** command searches the backup index on the client named lunaire for backups of the repository testdocbase:

```
nsrnmidx -B testdocbase -c lunaire
```

The **nsrnmidx** command displays the following backup index information and shows the records for two backup of the specific storage area:

```
===== Record Head #0 =====
cs_host_count: 2
database_conn: NMD
database_host:
database_name:
database_type: Oracle
dcb_version: 5.3+
DM_HOME: /Doc5.3/product/5.3
DOCBASE_NAME: testdocbase
DOCUMENTUM: /Doc5.3
DOCUMENTUM_SHARED: /Doc5.3/product/shared
FTI_COUNT: 0
fti_host:
fti_idxserver_count: 0
JAVA_HOME: /Doc5.3/product/shared/java/1.4.2_11
JAVA_PATH: /Doc5.3/product/shared/java/1.4.2_11/bin
NMD_BACKUP_FTI_QUIESCE: nsrnmftiq.sh
NMD_BACKUP_FTI_UNQUIESCE: nsrnmftiu.sh
NMD_FILEREPORT_INCLUDED: yes
NMD_FTI_INCLUDED: yes
NMD_NUM_SAS_DROPPED: 0
NMD_RCS_CFG_FILE: x.x
NMD_USE_DEFAULT_SAVESET_NAMES: yes
NMD_USE_SNAPIMAGE: no
NMDDE_DM_DOCBASE: testdocbase
NMDDE_DM_USER: oracle
NMDDE_METADATA_OUTPUT_DEST: /newfs/filereport/fp
NSR_BACKUP_LEVEL: INCR
NSR_CLIENT: lunaire.blrsql.com
NSR_DATA_VOLUME_POOL: NMDPool
NSR_GROUP: nmd
NSR_SERVER: lunaire
OBJECT_NAME: filestore_01
ORACLE_HOME: /opt/ORACLE/OraHome_1
PARTIAL_BACKUP: no
SA_COUNT: 1
SA_END: 1185176829 (Mon Jul 23 13:17:09 2007)
SA_START: 1185176829 (Mon Jul 23 13:17:09 2007)
SCOPE: SA
TAG: 1185176835
type: DCTM_PHY
===== Record Head #1 =====
cs_host_count: 2
database_conn: NMD
database_host:
database_name:
database_type: Oracle
dcb_version: 5.3+
DM_HOME: /Doc5.3/product/5.3
```



```

DOCBASE_NAME: testdocbase
DOCUMENTUM: /Doc5.3
DOCUMENTUM_SHARED: /Doc5.3/product/shared
FTI_COUNT: 0
fti_host:
fti_idxserver_count: 0
JAVA_HOME: /Doc5.3/product/shared/java/1.4.2_11
JAVA_PATH: /Doc5.3/product/shared/java/1.4.2_11/bin
NMD_BACKUP_FTI_QUIESCE: nsrnmftiq.sh
NMD_BACKUP_FTI_UNQUIESCE: nsrnmftiu.sh
NMD_FILEREPORT_INCLUDED: yes
NMD_FTI_INCLUDED: yes
NMD_NUM_SAS_DROPPED: 0
NMD_RCS_CFG_FILE: x.x
NMD_USE_DEFAULT_SAVESET_NAMES: yes
NMD_USE_SNAPIMAGE: no
NMDDE_DM_DOCBASE: testdocbase
NMDDE_DM_USER: oracle
NMDDE_METADATA_OUTPUT_DEST: /newfs/filereport/fp
NSR_BACKUP_LEVEL: FULL
NSR_CLIENT: lunaire.blrsql.com
NSR_DATA_VOLUME_POOL: NMDPool
NSR_GROUP: nmd
NSR_SERVER: lunaire.blrsql.com
OBJECT_NAME: fs_rcs_rowan_rowan
ORACLE_HOME: /opt/ORACLE/OraHome_1
PARTIAL_BACKUP: no
SA_COUNT: 1
SA_END: 1185176131 (Mon Jul 23 13:05:31 2007)
SA_START: 1185176110 (Mon Jul 23 13:05:10 2007)
SCOPE: SA
TAG: 1185176135
type: DCTM_PHY

```

7.4. Change of directory ownership and permissions during a restore

You must run an NMD restore as the root user on UNIX or Linux, or as a member of the Administrators group on Windows. During a restore or disaster recovery of a full-text index, storage area, or installation and configuration file component, if an upper-level parent directory of the component is missing, the directory is automatically re-created and the ownership and permissions of the directory are changed to the user that performs the restore, such as the root user on UNIX.

- ◆ If /reloc/abc/file1 is being restored and the abc directory is missing on the Documentum Server, the abc directory is created and its ownership is changed to the user that performs the restore.
- ◆ Similarly, if the /reloc directory is missing, both the /reloc and /reloc/abc directories are created during the restore and the ownership of the directories is changed to the user that performs the restore.

The user that performs the restore must manually change the ownership and permissions of any created directory back to those of the original user (dminstall user) by using the appropriate operating system commands.

If required, change the directory ownership by one of the following methods:

- ◆ On UNIX or Linux, enter the following command:

```
chown dminstall_userid dir_pathname
```

where *dir_pathname* is the pathname of the parent directory.

- ◆ On Windows, perform the following:
 1. In Windows Explorer, right-click the parent directory and select **Properties**.
 2. On the **Properties** screen, click **Security**.
 3. Select the correct name under **Group or user names**, and click **Advanced**.
 4. On the **Advanced Security Settings** screen, click **Owner**.
 5. Select the correct name under **Change owner to**, and click **OK**.

7.5. Content file restore

To browse Documentum file reports (optionally generated at the end of storage area backups) and display a list of content files from the file reports that match the specified search criteria, enter the **nsrnm dcr** command. The command can optionally restore the content files found during the browse operation.



IMPORTANT

Restore the content files to a relocation area, and hand them to the user. The user then adds the corresponding document to the repository by using the restored files.

If the `NMD_FILEREPORT_INCLUDED` and `NMDDE_METADATA_OUTPUT_DEST` parameters are set properly in the configuration file before a storage area backup, Documentum file reports that contain content file metadata are generated at the end of the backup. `NMD_FILEREPORT_INCLUDED` must *not* be set to `no`. The backup must be of scope `ALL`, `SA`, or `SA_ALL`. A separate file report is generated for *each* storage area backed up.

Note: If the information in the Documentum database about a storage area's files is inconsistent with the actual physical files in the storage area (for example, due to a Documentum bug or improper configuration of the storage area or the content file being parked at the BOCS), the **nsrnm dcr** command might *not* restore all the expected files from a backup of the storage area.

For example, the **nsrnm dcr** command might restore fewer files from a storage area backup than are listed in the backup file reports. However, the file reports might be based on incorrect information about the storage area or parked-content information within the Documentum database.

The *EMC NetWorker Module for Documentum Administration Guide* provides more information on the **nsrnm dcr** command and its options.

Example 5 Sample nsrnm dcr command for file report searches

The following **nsrnm dcr** command searches file reports for the storage area `filestore_01` of the repository `babilon`. The file reports searched are those that were created on May 22, 2006. The search looks for document names containing the (case-insensitive) string "mobile", with the folder name `mobilitydocs` and version number 1.0. The documents were checked in from the client `waterloo`.

```
nsrnm dcr -B babilon -A filestore_01
-P "F:\Documentum\stores\Filereports\current"
-T "20060522" -V -c "waterloo" -d "mobile"
-f "mobilitydocs" -v "1\0"
```

Note: In the regular expression "v1\0", the escape character `\` is included before the dot.

7.6 Database and log restore

The **nsrnmidx** command can be used to search for the required database or database log backup in the backup index before starting a restore. For example, the index might be searched for a backup of scope ALL, DB, or DB_LOG that contains the required database or logs. The *EMC NetWorker Module for Documentum Administration Guide* provides more information on the **nsrnmidx** command.

To restore database files and database logs from an NMD backup, use the appropriate method, depending on how the files were originally backed up. For example, if the database files were backed up by using a NetWorker Module or user-created scripts, the corresponding method must be used for the restore.

Example 6 Oracle database restore

When an Oracle database is backed up during an NMD backup by using the NetWorker Module for Oracle, you can restore the Oracle database to a point in time as follows:

1. Enter the **nsrnmidx** command to browse the backup index and select the correct backup that includes the Oracle database. From the **nsrnmidx** command output, record the SA_START value that specifies the start time of the backup record of type SA.

Note: If a remote database host is used and its system time is out-of-sync with the Documentum host system time, then the times reported by **nsrnmidx** must be adjusted accordingly. The reported times for database and storage area backups are based on the Documentum host system time.

The *EMC NetWorker Module for Documentum Administration Guide* provides more information on the **nsrnmidx** command.

2. Restore the database files and (if required) logs from the backup by using an RMAN restore script that includes the appropriate Oracle restore commands. The following sources provide more information on RMAN restore scripts:
 - *EMC NetWorker Module for Oracle Administration Guide*
 - Oracle backup and recovery documentation
3. Recover the database to the point in time specified by the SA_START value in the **nsrnmidx** command output from [Step 1](#). For the recovery, use the appropriate Oracle commands to apply the archived redo logs and online redo logs. There are two ways to use the Oracle recovery commands:
 - Include the Oracle commands in the RMAN restore script in [Step 2](#).
 - After the RMAN restore script of [Step 2](#) has completed successfully, enter the Oracle commands at the operating system command line.

The Oracle backup and recovery documentation provides more information on the Oracle commands.



IMPORTANT

The database must be recovered to the point in time specified by SA_START in [Step 1](#). Do not recover the database beyond the SA_START time of the backup by applying the log files.

7.7. Other component restore

All defective full-text index and storage area components being restored should be offline and quiesced before the restore. The components must be quiesced *manually* outside of NMD, for example, through the Documentum Administrator GUI.

Note: The NMD_RECOVER_QUIESCE parameter in previous NMD releases was used to specify that `nsrnmdrs` perform the quiesce operation before a restore. This parameter is *no longer* supported with NMD 1.2.

To browse the NMD backup index and restore selected components from a specified backup, enter the `nsrnmdrs` command, as either the root user on UNIX or a member of the Microsoft Windows Administrators group. The command restores Documentum Server storage areas, full-text indexes, and installation and configuration files.

During a full-text index backup, temporary files located in the index staging area (the `fixml` directory) are also backed up. When the full-text index backup is restored, the `fixml` directory is also restored. As a result, the following procedure is recommended to restore a full-text index backup:

1. Restore the full-text index backup to a temporary relocation directory by using the `nsrnmdrs` command with the `-d` option.
2. After the restore, move the required full-text index files from the temporary directory to the appropriate final location.



IMPORTANT

Do *not* restore a backup over the original, existent source data. Use a relocation directory. Alternatively, perform the following:

1. Place the corresponding repository component in offline mode.
2. Rename the root directory of the component.
3. Re-create the root directory.
4. Perform the restore.

When restoring the database component, restore the backup to the point in time at the end of the database backup. To determine this point in time, use the `nsrnmidx` command. Do *not* roll forward the database by applying logs.

When restoring a storage area, randomly open some of the files to verify that there is no corruption.

The *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Administration Guide* provides more information on the `nsrnmdrs` command and its options.

Example 7 Sample `nsrnmdrs` commands for different types of restores

The following `nsrnmdrs` command restores the latest backup that contains all the storage areas of the repository `docora10`:

```
nsrnmdrs -B docora10 -f /space10/home/dmuser/nmd.cfg -C SA
```

The following `nsrnmdrs` command restores the storage area named `filestore_01` from the latest backup that occurred between 12/12/07 and 12/13/07 and relocates the storage area to the directory `/space2/sa_dec12`:

```
nsrnmdrs -B docora10 -f /space10/home/dmuser/nmd.cfg -L "12/12/07"
-C SA -a filestore_01 -d /space2/sa_dec12
```

The following **nsrnmdrs** command restores all the full-text indexes from the latest backup that occurred before today:

```
nsrnmdrs -B docora92 -f /space10/home/dmuser/nmd.cfg -C FTI -U "today"
-d /space2/docora10_ftindex
```

Example 8 Restore information displayed by the **nsrnmdrs** command

The following **nsrnmdrs** command searches the backup index and restores the latest backup of the storage area named `filestore_01` of the repository `testdocbase`, relocating it to the `/newfs/restore` directory:

```
nsrnmdrs -f /nsrnm_hp.cfg -B testdocbase -C SA -a filestore_01
-d /newfs/restore
```

The **nsrnmdrs** command displays the following information during the restore process:

```
07/23/07 13:28:40 nsrnmdrs: Note: This session will restore the backup
with the latest timestamp
Freeing the previous query.
The server has been set to: lunaire.blrsql.com
The client has been set to: lunaire.blrsql.com
The repository has been set to: testdocbase
The scope has been set to: NULL
The type has been set to: SA
The name has been set to: filestore_01
The time query operation is: 0
The time is: 18446744073709551615
The lnm_index_t handle has been created.
The count is set to 1.
We are performing a name query on filestore_01.
The count is 1.
We are querying for object /docbase/testdocbase/SA/filestore_01/.
lnm_index_cfx_connect: Creating CFX connections:
server('lunaire.blrsql.com') client('lunaire.blrsql.com') retries (4)
lnm_index_cfx_pconn: Getting the LGTO parameters for server
'lunaire.blrsql.com' and client 'lunaire.blrsql.com'.
lnm_index_cfx_pconn: Getting the LGTO authentication from server
'lunaire.blrsql.com'.
lnm_index_cfx_pconn: Getting the NW index connection.
lnm_index_cfx_connect: Starting the connection to the NW client
indexes.
lnm_index_cfx_start: Starting the NW index connection with server
'lunaire.blrsql.com' and client 'lunaire.blrsql.com'.
lnm_index_cfx_lookup6: Performing the NW client index lookup on:
name: /docbase/testdocbase/SA/filestore_01/
lnm_index_cfx_lookup6: 1 records returned.
The CFX query succeeded.
Getting the metadata for DCTM_PHY_testdocbase (1185176835).
lnm_index_cfx_connect: The CFX connection has already been created.
lnm_index_cfx_lookup: Performing the NW client index lookup on:
name: DCTM_PHY_testdocbase
time: 1185176835
lnm_index_cfx_lookup: 1 records returned.
The index query was successful.
The name is DCTM_PHY_testdocbase.
The save time is 1185176835.
Searching for continuation record DCTM_PHY_testdocbase<1>.
lnm_index_cfx_connect: The CFX connection has already been created.
lnm_index_cfx_lookup: Performing the NW client index lookup on:
name: DCTM_PHY_testdocbase<1>
time: 1185176835
lnm_index_cfx_lookup: 0 records returned.
The continued meta data has been obtained.
The continued meta data has joined.
```

```

The meta data was successfully XDR decoded.
The meta data has been obtained.
The meta data has been obtained.
There are records available for future queries.
07/23/07 13:28:40 nsrnmdrs:      --- Component(s) selected for restore
---
nsrnmdrs:      --- Storage Area Start ---
nsrnmdrs:      =====
nsrnmdrs:      --cs_host:lunaire--
nsrnmdrs:      --end Save Time:Mon Jul 23 13:17:09 2007--
nsrnmdrs:      --INCR_START_TICKET:-2147483544--
nsrnmdrs:      --name:filestore_01--
nsrnmdrs:      --path:/Doc5.3/data/testdocbase/content_storage_01/00000086--
nsrnmdrs:      --start Save Time:Mon Jul 23 13:17:09 2007--
nsrnmdrs:      --ticket:-2147483544--
nsrnmdrs:      --type:SA--
nsrnmdrs:      --recovery location: /newfs/restore--
nsrnmdrs:      =====
07/23/07 13:28:40 nsrnmdrs: Would you like to proceed with the restore
? [y/n]:y

      cs_host_count: 2;
      database_conn: NMD;
      database_host: ;
      database_name: ;
      database_type: Oracle;
      dcb_version: 5.3+;
      DM_HOME: /Doc5.3/product/5.3;
      DOCBASE_NAME: testdocbase;
      DOCUMENTUM: /Doc5.3;
      DOCUMENTUM_SHARED: /Doc5.3/product/shared;
      FTI_COUNT: 0;
      fti_host: ;
      fti_idxserver_count: 0;
      JAVA_HOME: /Doc5.3/product/shared/java/1.4.2_11;
      JAVA_PATH: /Doc5.3/product/shared/java/1.4.2_11/bin;
      NMD_BACKUP_FTI_QUIESCE: nsrnmddfaiq.sh;
      NMD_BACKUP_FTI_UNQUIESCE: nsrnmddfaiu.sh;
      NMD_FILEREPORT_INCLUDED: yes;
      NMD_FTI_INCLUDED: yes;
      NMD_NUM_SAS_DROPPED: 0;
      NMD_RCS_CFG_FILE: x.x;
      NMD_USE_DEFAULT_SAVESET_NAMES: yes;
      NMD_USE_SNAPIMAGE: no;
      NMDDE_DM_DOCBASE: testdocbase;
      NMDDE_DM_USER: oracle;
      NMDDE_METADATA_OUTPUT_DEST: /newfs/filereport/fp;
      NSR_BACKUP_LEVEL: INCR;
      NSR_CLIENT: lunaire.blrsql.com;
      NSR_DATA_VOLUME_POOL: NMDPool;
      NSR_GROUP: nmd;
      NSR_SERVER: lunaire;
      OBJECT_NAME: filestore_01;
      ORACLE_HOME: /opt/ORACLE/OraHome_1;
      PARTIAL_BACKUP: no;
      SA_COUNT: 1;
      SA_END: 1185176829;
      SA_START: 1185176829;
      SCOPE: SA;
      TAG: 1185176835;
      type: DCTM_PHY;
07/23/07 13:28:53 nsrnmdrs: Restore successful

```

8. Troubleshooting tips

The *EMC NetWorker Module for Documentum Administration Guide* provides detailed information on troubleshooting and specific recommendations to address NMD backup and restore issues.

9. Optimization recommendations

9.1. Parallelism for restores

The following types of restores use the **recover -t** command:

- ◆ Restores of storage areas with SnapImage
- ◆ Restores of storage areas, full-text indexes, and installation and configuration files without SnapImage

Note: Restores of full-text indexes and installation and configuration files with SnapImage use the **recover -S** command.

Currently on UNIX, the use of a single **recover -t** task provides inherent parallelism during a restore, both with a single tape and across multiple concurrent tapes. As a result, it may be more beneficial to set the restore parallelism to a value of 1 or 2, instead of a higher value that can lead to tape head thrashing.

9.2. SnapImage optimization

SnapImage backups are most beneficial under the following conditions:

- ◆ When there is sufficient memory, swap space, and disk space, as described in the *EMC NetWorker Module for Documentum Administration Guide*.
- ◆ When there is no or minimal disk write activity on the storage area file systems.

9.3. Other optimization

The following provide more information on optimization settings:

- ◆ [“6. Configuration overview” on page 19](#)
- ◆ [Appendix A, “NMD Consulting Pre-site Qualifier \(CPSQ\)”](#)

10. Special use case recommendations

10.1. Backups

The following sections provide recommendations for special use cases that involve NMD backups.

10.1.1. Scheduling repository backups

The recommended NetWorker schedule for repository backups is as follows:

- ◆ Level full on late Saturday or early Sunday, with a default file report dump.
- ◆ Level incr (also known as level 1) on all other days, with a default incremental file report dump.

10.1.2. Scheduling separate backups of installation and configuration files

NMD can back up the installation and configuration files, either as part of a repository system backup or as a separate backup, depending on the setting of the parameter `NMD_ICF_INCLUDED`.

Unless your environment requires the backup of the installation and configuration files to be part of the system backup, configure the backup of those files to occur separately.

For a backup of the installation and configuration files, the `NMD_ICF_SUBDIRS` parameter must be set in the NMD configuration file, to specify the installation and configuration files to be included in the backup. NMD does *not* autodiscover any part of the installation and configuration files during a backup.

The schedule of installation and configuration file backups should be infrequent because the files do not change as often as other repository components. An installation and configuration file backup should be in its own savegroup session, and should *not* overlap with a regular NMD backup.

A level full save set is always generated for an installation and configuration file backup.

In a distributed storage area configuration, the installation and configuration files are backed up on the primary host only, *not* on any remote hosts.

10.1.3. File report generation and purging

If the `NMD_FILEREPORT_INCLUDED` and `NMDDE_METADATA_OUTPUT_DEST` parameters are set properly in the configuration file before a storage area backup, Documentum file reports containing content file metadata are generated at the end of storage area backup. `NMD_FILEREPORT_INCLUDED` must *not* be set to `NO`. The backup must be of scope `ALL`, `SA`, or `SA_ALL`. A separate file report is generated for *each* storage area backed up.

An extra file system of sufficient disk space should be used for the file reports. The amount of space required depends on the number of repository documents and the frequency of full and incremental dumps. Typically, at least 2 GB of extra space should be reserved. The Documentum Server administrator needs to handle the periodic purging of old documents.

To browse the content file metadata in the file reports, enter the `nsrnmddcr` command at the operating system command line. “7.5. Content file restore” on page 26 provides more information.

A file report filename has the following format:

`DCB_repository-name_storage-area-name_level_data-ticket_timestamp.txt`

Chapter 3 of the *EMC NetWorker Module for Documentum Administration Guide* provides examples of a file report filename and the contents of a file report.

10.1.4. LAN, SAN, and local backup devices

For the best performance in backing up and restoring a repository, use a local NetWorker device or a SAN NetWorker device.

Backups to a remote NetWorker device (on a remote NetWorker server or storage node) are limited by the network bandwidth, for example, approximately 8 MB/s for a 100 Mb/s LAN.

10.2. Restores

The following sections provide recommendations for special use cases that involve restores of NMD backups.

10.2.1. Repository and disaster recovery

The *EMC NetWorker Module for Documentum Release 1.2 Multiplatform Version Administration Guide* provides information on repository and disaster recovery.

10.2.2. Intentionally inconsistent restore

An inconsistent repository restore occurs when only part of a repository is restored. This type of restore introduces inconsistencies in the repository. The *EMC NetWorker Module for Documentum Administration Guide* provides information about consistency in repository backups.

For instance, to avoid the need to restore the entire repository, you decide to restore a single storage area. The restored storage area does not contain documents that the database refers to.

Documentum application errors should be expected and manually resolved. For example, run a DQL script to remove all bad references to nonexistent documents. The relevant users should also be notified.

10.2.3. Using NetWorker directly

For diagnostic purposes or workarounds to problems encountered, an EMC Customer Support Representative may ask you to use the NetWorker **recover** program to restore repository data, although it is not supported by NMD.

The *EMC NetWorker Module for Documentum Administration Guide* provides information on how NMD interfaces with NetWorker software, which includes details on save set formations and the **recover** commands to use.

Alternatively, you can use the **recover** command to browse for backup history and perform actual restores. This type of operation is *not* supported by NMD.

Note: If all of the following conditions apply, you must manually restore the storage areas with the **nsrndmp_recover** command to a staging file system, as described in the *EMC NetWorker Module for Documentum Administration Guide*:

- One or more storage areas from the same file system were backed up by the SnapImage Module.
 - The storage areas contain a total of approximately one million or more files.
 - The SnapImage hotfix for EMC bugs LGTpa73035 and LGTpa79120 is *not* installed on Solaris or HP-UX.
-

10.3. UNIX symbolic links and mount points

NMD automatically expands and follows symbolic links that are in a root directory path of the storage area, full-text index, or installation and configuration file component. (This is any path listed in the NMD log files when tracing is turned on.)

NMD does *not* follow symbolic links that are *under* the root directory path of a storage area, full-text index, or installation and configuration file component. These types of "inner" symbolic links should never occur for a storage area or full-text index component, unless a user manually creates them. NMD can indirectly handle "inner" symbolic links for the installation and configuration file component when the fully expanded directory and file paths are listed in the parameter NMD_ICF_SUBDIRS.

Similar to symbolic links, NMD does not follow mount points during a backup if they are *under* the root directory path of a storage area, full-text index, or installation and configuration file component. Again, these types of mount points should never occur, unless a user manually creates them.

11. Related documentation

The information in this guide may be supplemented with the following resources:

- ◆ Appropriate versions of the documentation for the following EMC products:
 - NetWorker software
 - NetWorker Module for DB2
 - NetWorker Module for Documentum
 - NetWorker Module for Microsoft SQL Server
 - NetWorker Module for Oracle
 - NetWorker Module for Sybase
 - NetWorker SnapImage Module
- ◆ UNIX man pages (for NetWorker and NetWorker Module commands)
- ◆ Documentum Content Server documentation
- ◆ Appropriate database (IBM DB2, Oracle, Microsoft SQL Server, or Sybase) backup and recovery documentation

The complete set of EMC documentation is provided in PDF form on the Documentation Suite CD-ROM shipped with the EMC software. The *most* up-to-date EMC documentation is available on the EMC Powerlink® website at <http://Powerlink.EMC.com>.

NMD Consulting Pre-site Qualifier (CPSQ)

The information provided on this form will assist EMC in planning for project initiation. It is important that all questions are answered completely and accurately to ensure site readiness before consultants arrive on site. Please complete this form in its entirety and submit electronically as a Microsoft Word file to the required address.

Business Assessment		
Installation environment	Production ____	Test ____
What is the target installation date?		

Account Information			
Date:			
Company Name:			
City, State:			
Country, if not U.S.:			
Site ID:			
	Name	Telephone	Email
Customer Project Leader:			
ESG Account Executive:			
ESG SE:			
ESG Consultant:			
EMC Account Executive:			
EMC TC/CSL:			

Existing NetWorker Backup Solution	
General	Completed?
Create or designate a Group to use for NMD backup.	
Create or designate a Pool to use for NMD backup.	
Create or designate a Schedule to use for NMD backup.	

NetWorker Module for Documentum	
General	Completed?
Is all the required licensing available and ready for installation?	
What is the operating system version?	
What is the database version?	
Is there any clustering or failover involved?	
Database layout: One repository per server? Or more than one repository per server?	
Is the database on the same server as Documentum?	
Will NetWorker SnapImage be used for backups? (If yes, complete the SnapImage section)	
Verify hardware compatibility in the EMC Hardware Compatibility Guide and release notes for all modules.	
Upgrade and patch all existing software to supported versions.	
Upgrade and test any required hardware patches.	
Configure and test all new backup media, for example, jukeboxes, arrays, NAS devices.	
Set network interfaces on Documentum and NetWorker servers to Full Duplex.	
Documentum server name:	
NetWorker server name (if different):	
NetWorker storage node name (if used):	
NetWorker installation path:	
Documentum installation path:	
Database installation path:	
NetWorker server Administrator name:	
Documentum installation owner username:	
Database user with SA rights name:	
NetWorker Group:	
NetWorker Pool:	
NetWorker Schedule:	

NetWorker SnapImage Module	
General	Completed?
What is the operating system version where the Documentum storage area resides?	
Total number of files in the storage area?	
What is the average file size in the storage area?	
Does the total file system size for the storage area exceed 2 terabytes?	

NetWorker Module for Oracle ^a	
General	Completed?
Register the database name in the Recovery Catalog.	
Verify that the database is in archivelog mode.	
Create or designate a user with SA rights to use with RMAN.	

- a. Please note that all operating system, database, and application versions that exist in the customer environment must meet the minimum required revision levels in order for this solution to be supported by EMC. To ensure that all EMC software components in this solution meet the necessary compatibility requirements, review the requirements listed in the *EMC Information Protection Software Compatibility Guide* on the EMC Powerlink website at <http://Powerlink.EMC.com>.

This appendix describes the best practices for using the NetWorker software that works with the NMD software solution.

Note: The *Software Compatibility Guide* on the EMC Powerlink website at <http://Powerlink.EMC.com> provides details on the NetWorker software releases that NMD supports.

This appendix includes the following sections:

◆ B.1. Solution methodology: An industry best practice	40
◆ B.2. Datazones	40
◆ B.3. Single datazone	41
◆ B.4. Network best practices.....	45
◆ B.5. SAN best practices	45
◆ B.6. Business best practices	46
◆ B.7. NetWorker best practices	46
◆ B.8. NetWorker 7.x best practices.....	47

B.1. Solution methodology: An industry best practice

The primary components of a best practices-based solution methodology are as follows:

- ◆ Define requirements — Determine the Service Level Objectives (SLOs) for backup and restore and the roles and responsibilities of personnel, as well as DR/BC processes.
- ◆ Design and architecture — Based on SLOs, design a solution in the environment to meet defined requirements (template design for repeatable deployment).
- ◆ Implement — Execute a pilot in order to demonstrate that the design meets requirements.
- ◆ Roll out — Roll pilot into production, and train personnel to support the environment.
- ◆ Document — Create runbook documentation that details operations and restore scenarios so that the backup/restore solution is supportable and meets SLOs.
- ◆ Knowledge transfer — Perform hands-on transfer of knowledge with the customer and designated personnel for the critical administrative tasks and required functions.
- ◆ Continuous improvement — Engage EMC Professional Services (health checks) at regular intervals to validate that the deployment:
 - Continues to meet requirements
 - Scales
 - Integrates new environments

B.2. Datazones

B.2.1. Datazone requirements

Application and technology specific requirements are as follows:

- ◆ SAP
- ◆ Oracle
- ◆ EMC TimeFinder®/SRDF®
- ◆ Library sharing and tape rotation
- ◆ Availability
- ◆ Budget and available technology
- ◆ Operations staff and skill set (roles and responsibilities)

B.2.2. Datazone keys to success

The four most often neglected keys to success are as follows:

- ◆ Perform detailed implementation planning.
- ◆ Define use requirements first, then market, then build.

- ◆ Run a pilot.
- ◆ Document the design and operation.

B.3. Single datazone

Consider the following data protection solutions for a single datazone:

- ◆ LAN-based — Distributed application servers require LAN backups.
- ◆ LAN-free — High-capacity data application servers require local backups that would overwhelm LAN-based backups. Application servers have CPU and I/O resource capacity to handle data protection overhead.
- ◆ Serverless — Business-critical application servers have little CPU and I/O capacity to handle data protection overhead that compromises business application availability.

B.3.1. LAN clients, single datazone

LAN-based data protection issues are as follows:

- ◆ Client data structure limitations
- ◆ High-density file system
- ◆ Large amounts of data
- ◆ Network attached storage
- ◆ NetApp
- ◆ EMC Celerra®

B.3.2. LAN network, single datazone

LAN-based data protection issues are as follows:

- ◆ Network
- ◆ High-speed switched network is required to maximize throughput
- ◆ 100 base -T
- ◆ Gigabit
- ◆ Backup server or storage node
- ◆ NICs limited by server backplane capacity and CPU resources or network bandwidth
- ◆ Devices limited by CPU and I/O resources (backplane bandwidth and number of buses)

B.3.3. Client optimization, single datazone

A performance improvement strategy is as follows:

- ◆ Use application modules to improve data protection efficiency
- ◆ Oracle RMAN support
- ◆ SAP
- ◆ Informix

- ◆ Microsoft SQL Server
- ◆ Microsoft Exchange Server
- ◆ Use NDMP-based backup for NAS clients
- ◆ NetWorker SnapImage tape server

B.3.4. Host optimization, single datazone

A performance improvement strategy (non-NDMP) is as follows:

- ◆ Optimize the server or storage node configuration
- ◆ Immediate save versus TCP/IP (CPU is 400 MHz Sparc, tape is DLT7K)
- ◆ $n + 1$ CPUs ($n = (\text{number of tape devices}) / 2$)
- ◆ 50 percent CPU utilization (immediate save/recover, one stream)
- ◆ Add CPUs for NICs and HBAs as needed
- ◆ 256 MB per CPU (scale up for recovery operations, if needed)
- ◆ $(\text{Memory bandwidth}) * (.70) * (.25) = \text{maximum backplane I/O}$
- ◆ Two tape devices per CPU
- ◆ One tape per SCSI bus
- ◆ RAID 1 + 0 (or RAID 10) index and media database disk for maximum scalability
- ◆ Local host tables before DNS name resolution
- ◆ Kernel and resource requirements (file descriptors, memory heap)

B.3.4.1. Considerations

- ◆ Treat the CPU speeds and tape speeds as base lines and extrapolate out for your environment.
- ◆ For memory bandwidth, multiply the speed of the memory times the width.
- ◆ The reference SCSI bus here was 20 MB/s. In other words, 1XDLT7K per 20 MB/s bus. To extrapolate this, identify what the maximum compressed throughput is for a tape drive and use that as the capacity requirement. For example, the DLT7K internal bus is about 18 MB/s, which is the maximum throughput you get with highly compressible data and hardware compression enabled, thus the recommendation for a minimum dedicated 20 MB/s bus.
- ◆ The host files recommendation is a troubleshooting step, not necessarily (unless DNS performance issues cannot be resolved, which is frequently the case) the production deployment requirement.

B.3.5. NDMP optimization, single datazone

Note: The following considerations are for NetWorker pre-7.2. For NetWorker 7.2, the memory requirement is less by at least a factor of 10.

A performance improvement strategy (NDMP) is as follows:

- ◆ Optimize the server or storage node configuration
- ◆ $n + 1$ CPUs ($n = \text{CPU for NDMP indexing}$)
- ◆ RAID 1 + 0 (or RAID 10) for the index and media database

- ◆ Local host tables before DNS name resolution
- ◆ 256 MB per CPU
- ◆ NDMP Backup — 150 MB memory/wwap per 1 million files
- ◆ NDMP Recover — 300 MB memory/wwap per 1 million files
- ◆ DAR for efficient tape recovery operations

B.3.6. Server configuration, single datazone

A performance improvement strategy is as follows:

- ◆ Use multiplexing (non-NDMP).
- ◆ Maximize the data protection device usage for disk or network source limited clients.
- ◆ Balance the total data. Stagger the backup schedule so that a nightly backup reduces the total amount of data per backup window.
- ◆ Optimize **savegrp** usage. Minimize the number of groups and group overlap while keeping the number of clients per group consistent with the capacity of the datazone (server parallelism and savegrp parallelism).
- ◆ Use storage nodes to improve NetWorker server capacity and data protection performance.
- ◆ Increase the number of datazone devices by using local application server data protection devices.

B.3.7. Client options, single datazone

A performance improvement strategy is as follows:

- ◆ NAS
- ◆ NetApp
- ◆ Celerra
- ◆ NetWorker SnapImage
- ◆ Snapshot — Local block image backup
- ◆ Three-party copy
- ◆ Application modules
 - Oracle
 - SAP
 - IBM Informix, DB2
 - Microsoft SQL Server, Microsoft Exchange Server
 - NMO
 - NMES

B.3.8. Storage nodes, single datazone

Consider the following LAN-free data protection implementation issues related to storage nodes.

- ◆ Deciding when storage nodes should be used.
- ◆ Protecting large amounts of application server data (immediate save and recover).
- ◆ Application servers are isolated by slow or multiple protocol network configurations.
- ◆ Poor LAN performance requires local tape support.
- ◆ CPU load for the LAN backup must be reduced.

B.3.9. Storage node design, single datazone

B.3.9.1. Single or multiple datazones

Consider the capacity of the datazone design:

- ◆ Are there datazone split/consolidation questions?
- ◆ Does the number of clients exceed the NetWorker server capacity (*nsr.res* and *nsrd* performance issues)?
- ◆ Does the number of LAN storage nodes exceed the server capacity (number of active sessions or remote devices)?
- ◆ Is the NetWorker server index and media database within the design capacity?
- ◆ Allow for growth over the life of the design.

B.3.9.2. NDMP, single datazone

Consider the following items in a single datazone with NDMP:

- ◆ When vendor application specific
- ◆ NAS
- ◆ NetApp — NW 6.0.1-001 supported
- ◆ Celerra — NW 6.0.1-001 supported
- ◆ NDMP devices required
- ◆ NetWorker SnapImage
- ◆ Local block-image backups for NDMP and non-NDMP based application servers

B.3.10. Serverless design, single datazone

Consider the following in a serverless backup implementation:

- ◆ Secondary host or data mover workstation
- ◆ EMC TimeFinder Modules (SAP and Oracle) — Secondary host
- ◆ More coming with NetWorker 7.x Advanced file type device
- ◆ Block-level backup performance
- ◆ Connected by using FC- or SCSI-attached devices

B.3.11. Single datazone review

- ◆ Use a LAN-based, LAN-free, and serverless solution where each fits the requirements.
- ◆ A one-size solution does not solve all problems.
- ◆ If the NetWorker server is already at capacity for LAN-based backups, do not add storage nodes or consolidate datazones. Use multiple datazones.
- ◆ A blend of each type of solution is usually required to provide the best solution.
- ◆ Using this approach will achieve the big picture.

B.4. Network best practices

- ◆ All NICs and switches should be hard-set to 100 Mb/s full-duplex where appropriate.
- ◆ Local host tables for NetWorker servers and storage nodes (minimum)
- ◆ Connect lower performance NICs (100 Base-T) to a switch and high-performance NICs (Gb) between a switch and the NetWorker server/storage node (minimum).
- ◆ Configure Windows servers larger than 70-100 GB and UNIX servers larger than 100-150 GB as storage nodes on a 100 Mb/s LAN or upgraded to GB Ethernet.

B.4.1. Consideration

The issue of autonegotiation and autosensing is a controversial one. For more information, go to the Network World website, www.networkworld.com, and search on those keywords.

B.5. SAN best practices

- ◆ Check for compatibility between SAN components.
- ◆ Multivendor is acceptable, but dependencies become complex quickly.
- ◆ With less than the current JNI/EMULEX/QLogic, any two of the three work fine together, but all three may need to be zoned to isolate QLogic. The latest firmware/drivers may not have this problem.
- ◆ Observe the SAN power-up sequence.
- ◆ Run a pilot before deploying.
- ◆ Separate the SAN for disk and tape.
- ◆ Set the data router (Crossroads, ADIC, and so on) to block SCSI resets.
- ◆ Use persistent binding for tape devices.

B.5.1. Consideration: Recommended power up sequence

- ◆ SCSI devices — Tape and disk devices that reside behind a FC-to-SCSI bridge/router
- ◆ FC switch and/or hub devices
- ◆ FC-to-SCSI bridge or routing devices

- ◆ FC RAID or other disk devices
- ◆ Host systems

B.6. Business best practices

- ◆ Test business continuity.
- ◆ Validate backups.
- ◆ Cross-check compatibility.
- ◆ Use the NetWorker disaster recovery guide.
- ◆ Use the NetWorker performance tuning guide.
- ◆ Engage EMC Professional Services.
- ◆ Train personnel at all sites.

B.6.1. Considerations

- ◆ Test once a year and understand your business continuity plan.
- ◆ Validate backups by testing recovers.
- ◆ Cross-check hardware and software with the current compatibility guides on the EMC Powerlink website.
- ◆ Use the NetWorker disaster recovery guide and performance tuning guide practices where they apply.
- ◆ Train personnel at all sites in business continuance processes.

B.7. NetWorker best practices

Follow these best practices in addition to configuring and running the NetWorker software:

- ◆ Use automatic cloning for light cloning requirements only.
- ◆ Keep a printed copy of the daily bootstrap.
- ◆ Keep an offsite bootstrap and bootstrap printout.
- ◆ Schedule indexing outside the backup window (**savegrp -O -G group_name**).
- ◆ Keep the configuration simple.

B.7.1. Considerations

- ◆ Do not use automatic cloning if your groups overlap (to prevent drive and tape contention).
- ◆ Keep a printed copy of the daily bootstrap.
- ◆ Send a copy of the bootstrap tape and printout offsite for disaster recovery along with your offsite data shipment.
- ◆ Save the bootstrap and index to the same pool and make a copy (clone) to simplify DR.
- ◆ Turn indexing off to increase backup performance (eliminates indexing overhead on backup server).

- ◆ Create a superset Group (for example, NeverRun) that you never run, to consolidate the index backups (`savegrp -O -G group_name`). In high utilization environments, this needs to be run separately (just as with cloning).
- ◆ Keep your configuration simple for ease of management and less administrative overhead.

B.8. NetWorker 7.x best practices

- ◆ Advanced file type devices should be dedicated and partitioned or zoned to the desired size.
- ◆ Advanced file type device auto staging should be enabled.
- ◆ Turn on the resource logging and ensure that users login by using their own ID, *not* the root ID.
- ◆ The number of save sets on a volume directly impacts bulk volume operations.
 - Purge (save set operations performed in series).
 - Label volumes.
 - Media database migration.
- ◆ Follow the NetWorker 7.x disaster recovery guide for the new **mmrecov** operation.
- ◆ All NDMP devices must be identified as remote devices

B.8.1. File type device configuration on NetApp FAS960 (December 16, 2003)

The best practices are simple:

- ◆ Using one file device per LUN or file system makes it more easy to calculate throughput.
- ◆ Do not mix file devices in one file system, to prevent one from filling up the file system.
- ◆ Use as many file devices as concurrent recovery sessions. For example, to recover three servers simultaneously, use at least three file devices and back up each server to a separate file device.
- ◆ Use a journaling file system. If a crash did not occur, a reboot can take a lot of time with its checking.
- ◆ One pool per file device is a general rule.
- ◆ If you perform cloning or staging, consider the read throughput of each file device. It should be similar to the tape drive throughput.
- ◆ Use a large file system (1 to 3 TB) for a file device, especially for an advanced file device that should never become full.
- ◆ An advanced file device requires two **nsrmmmd** processes and two devices for NetWorker licencing and sizing.
- ◆ Work closely with NetApp when configuring the array.

