

NetBackup™ for NDMP Administrator's Guide

Windows, UNIX and Linux

Release 10.1



NetBackup™ for NDMP Administrator's Guide

Last updated: 2022-09-08

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introduction to NetBackup for NDMP	8
	About NetBackup for NDMP	9
	NetBackup for NDMP features	9
	NetBackup for NDMP terminology	11
	About Network Data Management Protocol (NDMP)	14
	Types of NDMP backup	14
	NDMP local backup	15
	NDMP three-way backup	15
	Backup to Media Manager storage units (remote NDMP)	16
	About NDMP policies in NetBackup	17
	About NetBackup storage units	18
	About assigning tape drives to different hosts	18
	About robotics control	19
	About the NDMP backup process	20
	About the NDMP restore process	22
	About Direct Access Recovery (DAR)	24
	Snapshot Client assistance	25
	About NDMP multiplexing	25
	About NDMP support for Replication Director	26
	Limitations of Replication Director with NDMP	26
	About NDMP support for NetApp clustered Data ONTAP (cDOT)	27
Chapter 2	Installation Notes for NetBackup for NDMP	30
	NetBackup for NDMP installation prerequisites	30
	About existing NetApp cDOT configurations before you upgrade	31
Chapter 3	Configuring NDMP backup to NDMP-attached devices	36
	About configuring NDMP-attached devices	36
	Authorizing NetBackup access to a NAS (NDMP) host	37
	About access for three-way backups and remote NDMP	39
	About Media and Device Management configuration	40
	Adding a robot directly attached to an NDMP host	41
	Adding a tape drive	42

	Checking the device configuration	43
	Using the Device Configuration Wizard to configure an NDMP filer	43
	About adding volumes	47
	About verifying NDMP password and robot connection	48
	Adding NDMP storage units	48
	About creating an NDMP policy	50
	Attributes tab options for an NDMP policy	50
	Schedules tab options for an NDMP policy with Accelerator for NDMP enabled	51
	Clients tab options for an NDMP policy	52
	Backup selection options for an NDMP policy	52
	About environment variables in the backup selections list	58
	About appropriate host selection for NetApp cDOT backup policies	60
	About backup types in a schedule for an NDMP policy	61
	About enabling or disabling DAR	61
	Disabling DAR for file and directory restores	62
	Disabling DAR for directory restores only	63
	Configuring NetBackup for NDMP in a clustered environment	63
Chapter 4	Configuring NDMP backup to NetBackup media servers (remote NDMP)	65
	About remote NDMP	65
	Configuring NDMP backup to Media Manager storage units	66
Chapter 5	Configuring NDMP DirectCopy	68
	About NDMP DirectCopy	68
	Prerequisites for using NDMP DirectCopy	69
	NDMP DirectCopy with VTL	69
	NDMP DirectCopy without VTL	71
	Configuring NDMP DirectCopy	72
	Using NDMP DirectCopy to duplicate a backup image	73
	Requirements to use NDMP DirectCopy for image duplication	74
	Initiating NDMP DirectCopy with the NetBackup Administration Console	74
Chapter 6	Accelerator for NDMP	76
	About NetBackup Accelerator for NDMP	76
	About the track log for Accelerator for NDMP	79

	How to redirect track logs for Accelerator for NDMP	80
	Accelerator messages in the NDMP backup job details log	82
	NetBackup logs for Accelerator for NDMP	85
Chapter 7	Remote NDMP and disk devices	87
	About remote NDMP and disk devices	87
	Configuring remote NDMP	88
Chapter 8	Using the Shared Storage Option (SSO)	90
	About the Shared Storage Option (SSO) with NetBackup for NDMP	90
	Setting up SSO with NetBackup for NDMP	91
	Using the NetBackup Device Configuration Wizard for NDMP hosts	92
Chapter 9	Backup and restore procedures	94
	Performing a manual backup with an NDMP policy	94
	Perform an NDMP restore	95
Chapter 10	Troubleshooting	97
	About NetBackup for NDMP logs	97
	Viewing NetBackup for NDMP logs	97
	NDMP backup levels	99
	General NetBackup for NDMP operating notes and restrictions	100
	NetBackup for NDMP troubleshooting suggestions	102
	Troubleshooting NDMP media and devices on Windows	103
	Troubleshooting NDMP media and devices on UNIX	103
	Troubleshooting NDMP DirectCopy	104
	Troubleshooting Direct Access Recovery (DAR) with NetBackup for NDMP	104
	About robot tests	105
	TLD robot test example for UNIX	106
Chapter 11	Using NetBackup for NDMP scripts	107
	About the NetBackup for NDMP scripts	107
	ndmp_start_notify script (UNIX)	108
	ndmp_start_notify.cmd script (Microsoft Windows)	110
	ndmp_end_notify script (UNIX)	112
	ndmp_end_notify.cmd script (Microsoft Windows)	114
	ndmp_start_path_notify script (UNIX)	116

ndmp_start_path_notify.cmd script (Microsoft Windows)	119
ndmp_end_path_notify script (UNIX)	121
ndmp_end_path_notify.cmd script (Microsoft Windows)	123
ndmp_moving_path_notify script (UNIX)	125
ndmp_moving_path_notify.cmd script (Microsoft Windows)	127

Introduction to NetBackup for NDMP

This chapter includes the following topics:

- [About NetBackup for NDMP](#)
- [About Network Data Management Protocol \(NDMP\)](#)
- [Types of NDMP backup](#)
- [About NDMP policies in NetBackup](#)
- [About NetBackup storage units](#)
- [About assigning tape drives to different hosts](#)
- [About the NDMP backup process](#)
- [About the NDMP restore process](#)
- [About Direct Access Recovery \(DAR\)](#)
- [Snapshot Client assistance](#)
- [About NDMP multiplexing](#)
- [About NDMP support for Replication Director](#)
- [Limitations of Replication Director with NDMP](#)
- [About NDMP support for NetApp clustered Data ONTAP \(cDOT\)](#)

About NetBackup for NDMP

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems.

NetBackup for NDMP features

The following table describes the NetBackup for NDMP features.

Table 1-1 NetBackup for NDMP features

Feature	Description
Support for NDMP protocol	Supports the NDMP protocol versions V2, V3, and V4.
Centralized backup policy management	Scheduling, catalog management, and other backup tasks are managed from a NetBackup primary server. NetBackup for NDMP can be installed on a NetBackup primary or media server.
Accelerator for NDMP	NetBackup's Accelerator option makes NDMP backups for NetApp and Isilon filers run faster than normal NDMP backups. NetBackup Accelerator increases the speed of full backups by using the filer's change detection techniques to identify the modifications that occurred since the last backup. More information about the feature is available: See "About NetBackup Accelerator for NDMP" on page 76.
Support for NetApp cDOT filers	NetBackup for NDMP supports NetApp clustered Data on Tap (cDOT) filers. More information about configuring NetBackup to work with NetApp cDOT filers is available: See "Using the Device Configuration Wizard to configure an NDMP filer" on page 43.
Support for wildcards in NDMP backup policy selections	Wildcard characters in regular expressions or directives are valid for streaming and non-streaming NDMP backups.
Device and media management	NetBackup software provides complete management and control of the devices and media that are used for backups and restores of NDMP hosts. The NetBackup Device Configuration Wizard discovers and configures the storage devices that are attached to an NDMP host. (This function requires NDMP protocol V3 or V4.) Note that wizard-based discovery depends upon a number of device-specific features, such as SCSI inquiry and serialization, which some NAS vendors may not support.
High-speed local backup of NDMP hosts	Backup data travels between the disk drives and tape drives that are directly attached to the same NDMP host. This transfer provides high-speed backup but does not slow network throughput.

Table 1-1 NetBackup for NDMP features (*continued*)

Feature	Description
Backup of network-attached NDMP hosts to a tape device on another NDMP host or to advanced tape libraries with an embedded NDMP server	Backup data travels across the network from a disk on an NDMP host to tape on another NDMP host. This backup is referred to as a three-way backup. This data movement option requires support from the NAS/NDMP host.
Backup of a network-attached NDMP host to a tape device on a NetBackup media server	Backup data travels across the network from a disk on an NDMP host to tape on a NetBackup media server. This backup is a form of three-way backup also known as remote NDMP. This feature supports NDMP V2, V3, and V4 on the NDMP hosts.
Shared tape libraries	Tape libraries can be shared between NDMP hosts and NetBackup servers or between multiple NDMP hosts. Robotic control can be on an NDMP host or on a NetBackup server.
Shared tape drives with the Shared Storage Option	Tape drives can be shared between servers (both NetBackup servers and NDMP hosts). This setup requires the Shared Storage Option (SSO) license. For a list of the features and software releases for each NAS vendor, for SSO support, and for the NetBackup versions that support these vendors, see the NetBackup Compatibility List for all Versions.
Snapshots of data on NDMP hosts	NetBackup can take point-in-time data snapshots on an NDMP (NAS) host without interrupting client access to data, using the NDMP V4 snapshot extension. The snapshot is stored on the same device that contains the NDMP client data. From the snapshot, you can restore individual files or roll back a file system or volume by means of Snapshot Client Instant Recovery. A NetBackup Snapshot Client license is required, in addition to the NetBackup for NDMP license. This Snapshot Client feature uses the NAS_Snapshot method and the NDMP method. For more information about the Snapshot Client, refer to NetBackup Snapshot Client Administrator's Guide. For more information about the NDMP snapshot method, refer to the NetBackup Replication Director Solutions Guide
NDMP DirectCopy	NetBackup can copy virtual tape library (VTL) images directly from the VTL to physical tape or to another VTL. This function occurs without using media server I/O resources or network bandwidth. NetBackup can copy NDMP backup images directly from one NDMP-attached tape drive to another NDMP tape drive that is attached to the same NDMP host. Note that the operation does not use media server I/O. Note: The VTL must have an embedded NDMP tape server.
Direct Access Recovery (DAR)	For NDMP hosts that support DAR, this feature greatly reduces the time to restore a directory, a single file, or a small number of files.

Table 1-1 NetBackup for NDMP features (*continued*)

Feature	Description
Path-based file history	The NDMP server can send catalog information consisting of complete path names to NetBackup. Some vendors do not support this feature. Up-to-date information is available on the vendors that support path-based history. For a list of the features and software releases for each NAS vendor, for SSO support, and for the NetBackup versions that support these vendors, see the NetBackup Compatibility List for all Versions .
Support for NetBackup for NDMP servers in a NetBackup-clustered environment	The NetBackup for NDMP servers are supported in a NetBackup-clustered environment.
Enhanced ability to run customized scripts during a backup	The enhanced ability to run customized scripts during a backup, especially for relational databases residing on NAS devices.
NDMP multiplexing	NDMP multiplexing enables NDMP backups to be multiplexed to Media Manager storage units. Only remote NDMP multiplexing is supported.
NDMP to disk	NetBackup can write NDMP backups to disk storage units.
IPv6 support	NDMP supports 128-bit IPv6 address data connections in addition to the 32-bit IPv4 address data connections. NDMP data connections are made between filers or between a NetBackup media server and a filer that is used to transfer the backup image. By default the NetBackup media server is enabled for IPv6 data communication. Consider the following general items when using NDMP IPv6 address data connections. ■ The filer needs to be enabled for IPv6 data communication. ■ The filer vendor must support connection address extension or full IPv6.
NDMP support for Replication Director	NDMP support for Replication Director enables NetBackup to use NDMP for the following functions: backup from snapshots, restore from snapshot backups, live browse snapshots, and restore from snapshots (for copy back method). For more information about Replication Director, refer to the NetBackup Replication Director Solutions Guide.

NetBackup for NDMP terminology

The following table describes the NetBackup for NDMP terminology. For explanations of other NetBackup terms, consult the NetBackup online glossary in NetBackup Help.

Table 1-2 Terminology

Term	Definition
DAR (Direct Access Recovery)	DAR is an optional capability of NDMP data and tape services where only relevant portions of the secondary media are accessed during recovery operations. The NDMP host positions the tape to the exact location of the requested file(s), reading only the data that is needed for those files. Restore times can be reduced from hours to minutes.
NDMP (Network Data Management Protocol)	NDMP is a widely used protocol through which an NDMP-conformant backup application can control the backups and restores for an NDMP host.
NDMP client	An NDMP client is an NDMP-compliant backup application (also known as a Data Management Application or DMA) that is an NDMP server application client. An NDMP client sends commands to the NDMP server application to control the backups and restores on an NDMP host. NetBackup for NDMP allows NetBackup to act as an NDMP client.
NetBackup for NDMP server	A NetBackup for NDMP server is a NetBackup primary or media server on which NetBackup for NDMP software is installed.
NDMP host	An NAS system that serves files to clients using HTTP, FTP, CIFS, or NFS protocols. It also runs an NDMP server application that communicates with NDMP client backup software to configure and perform backup and restore tasks. NAS systems provide fast, multi-protocol file access and cost effective data storage to workstations and servers in the network or across the Internet. In a NetBackup configuration, the NDMP host is considered a client of NetBackup. However, NetBackup client software is never installed on an NDMP host.
NDMP multiplexing	NDMP multiplexing concurrently writes multiple backup streams to the same Media Manager tape storage device from the same client or different clients. NDMP multiplexing improves overall NetBackup performance by more efficient use of the storage unit drives. State of the art storage devices can typically stream data faster than client agents can create backup streams. Therefore, multiple data streams can be sent to and effectively processed by a given storage unit. Only remote NDMP multiplexing is supported.

Table 1-2 Terminology (*continued*)

Term	Definition
NDMP server application	An NDMP server application runs on an NDMP host and runs backup, restore, and device control commands that it receives from an NDMP-conformant backup application. The backup application (NetBackup) is considered an NDMP client. A separate instance of an NDMP server process exists for each connection to an NDMP client. That is, if two backups are in progress, an NDMP server process exists for each backup.
NDMP storage unit	An NDMP storage unit stores the backup data for an NDMP host. The tape drives in this storage unit attach directly to the NDMP host or can be configured on a SAN. Note that NDMP storage units cannot be used to store data for non-NDMP hosts, and NetBackup disk storage units cannot be used for NDMP tasks.
Redirected restore (to a different client)	In a redirected restore, files are restored to a client other than the one from which they were originally backed up. In NetBackup for NDMP, the restore data travels from an NDMP host (or NetBackup media server) with a locally attached storage device to another NDMP host on the network.
Remote NDMP	A form of three-way backup and restore also known as NDMP backup to Media Manager storage units. Data travels from an NDMP host to a tape drive that is attached to a NetBackup media server. See “Configuring NDMP backup to Media Manager storage units” on page 66.
Three-way backup and restore	In a three-way backup or restore, data travels between an NDMP host and a storage device that is attached to another NDMP host or to a NetBackup media server. This backup contrasts with local NDMP backup or restore where the data travels between an NDMP host’s disk and a storage device directly attached to the same NDMP host.
Virtual Tape Library (VTL)	A virtual tape library is a storage system that uses disk-based technology to emulate a tape library and tape drives. For secondary storage, NetBackup can copy VTL images directly to a physical tape or to another VTL by means of NDMP DirectCopy.

About Network Data Management Protocol (NDMP)

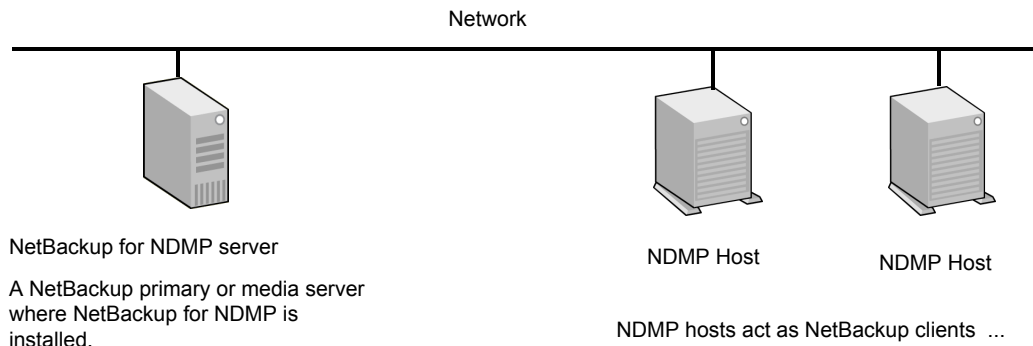
NDMP is a widely used protocol through which an NDMP-conformant backup application controls the backups and restores of any NDMP host that runs an NDMP server application.

NDMP architecture follows the client and server model:

- The NetBackup primary or media server where NetBackup for NDMP is installed is called a NetBackup for NDMP server.
- The host where the NDMP server application resides is called an NDMP host.
- The NetBackup software is a client of the NDMP server application. NetBackup for NDMP lets NetBackup act as an NDMP client. The NDMP hosts, on the other hand, act as NetBackup clients.

The following figure shows an example of NDMP and NetBackup hosts as clients of each other.

Figure 1-1 NDMP and NetBackup hosts as clients of each other



The NetBackup for NDMP server acts as an NDMP client.

NOTE: NetBackup software is NOT installed on NDMP hosts.

Types of NDMP backup

The NDMP server application on the NDMP host performs backups and restores of the NDMP host, directed by commands from an NDMP client (NetBackup). Backups can be conducted in any of the following ways:

- NDMP local backup
 See [“NDMP local backup”](#) on page 15.

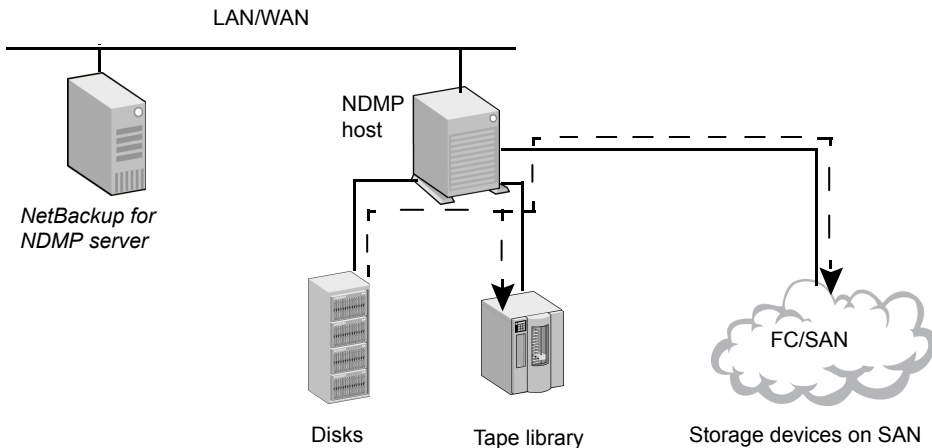
- NDMP three-way backup
See “[NDMP three-way backup](#)” on page 15.
- Backup to a Media Manager storage unit on the NetBackup server
See “[Backup to Media Manager storage units \(remote NDMP\)](#)” on page 16.

NDMP local backup

If you use the NDMP local backup, the NetBackup for NDMP server initiates the backup. The data travels from the NDMP host's disk to a storage device that is attached to the same host or is available on a SAN.

The following figure shows an example of an NDMP local backup and restore.

Figure 1-2 NDMP local backup and restore



Local NDMP backup

Data travels from disk to tape on same NDMP host, or from disk to tape device on SAN. *Backup data is NOT sent over local network.*

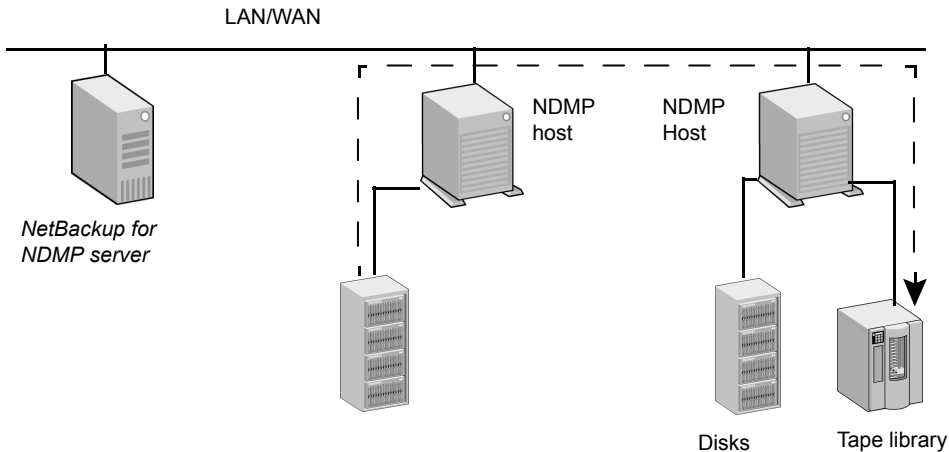
The tape drives must be in NDMP-type storage units.

NDMP three-way backup

If you use the NDMP three-way backup, the NetBackup for NDMP server initiates the backup. Data travels over the network by going from an NDMP host to a storage device that is attached to another NDMP host on the local network or is available on a SAN.

The following figure shows an example of an NDMP three-way backup and restore.

Figure 1-3 NDMP three-way backup and restore



Three-Way NDMP backup

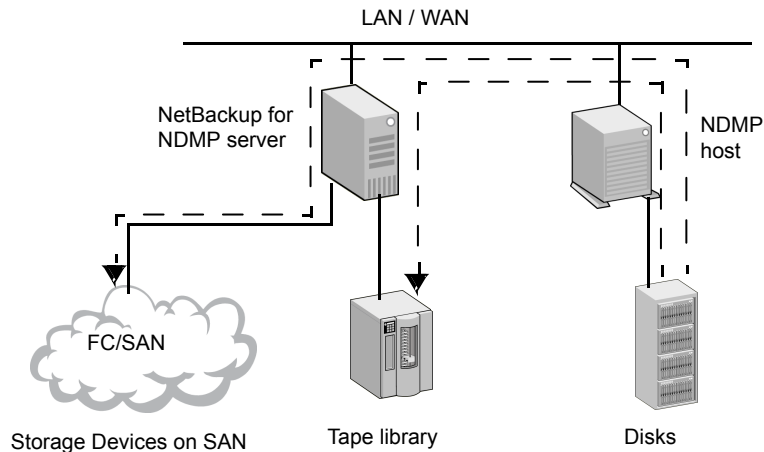
Data travels from disk on an NDMP host to tape device on another NDMP host. *Backup data is sent over the local network.*

The tape drives must be in NDMP-type storage units.

Backup to Media Manager storage units (remote NDMP)

With this backup method, the data travels over the network by going from an NDMP host to a Media Manager-type storage device that is attached to a NetBackup media server or is available on the SAN. The NetBackup drives must be in Media Manager storage units not in NDMP storage units.

The following figure shows an example of an NDMP backup to a Media Manager device (remote NDMP).

Figure 1-4 NDMP backup to a media manager device (remote NDMP)

To NetBackup Server-Attached Media Manager Storage Units

Data travels from NDMP host to a drive on a NetBackup media server or on a SAN. *Backup data is sent over the local network.*

NOTE: The NetBackup drive(s) must be in Media Manager type storage units.

About NDMP policies in NetBackup

After you install and configure NetBackup for NDMP, you can schedule backups by creating an NDMP policy in NetBackup.

An NDMP policy can have one or more NetBackup clients. Each NetBackup client must be an NDMP host.

See [Figure 1-1](#) on page 14.

Note that you do not install any NetBackup software on the NDMP hosts.

The allowable backup types for schedules in an NDMP policy are: Full, Cumulative Incremental, or Differential Incremental. User-initiated backups and archives are not allowed because the NDMP protocol does not permit these tasks.

Restores of NDMP host backups can be initiated from any NetBackup media server that meets the following criteria:

- Resides within the same overall NetBackup storage domain
- Uses the same NetBackup primary server that the media server uses to perform the backup

The data can be restored to the NDMP host where it was backed up, or to another NDMP host.

NDMP policies can use either NDMP storage units or Media Manager storage units.

About NetBackup storage units

NetBackup uses either one of the following storage units:

- NDMP-type storage units (for local or three-way backup)

NetBackup requires NDMP-type storage units when you back up NDMP host data to the devices that are as follows:

- Attached to an NDMP host
- Available to the NDMP host on a SAN

An NDMP storage unit can contain standalone or robotic drives. Robotic controls can be in a TLD (tape library DLT) or ACS robot type.

- Media Manager storage units (for backup to devices that are attached to a NetBackup media server)

You can use the drives that were configured in Media Manager-type storage units when you back up NDMP host data to devices that are as follows:

- Attached to a NetBackup for NDMP server
- Available to the server on a SAN

For NDMP backup, drives in Media Manager-type storage units do not have to be dedicated to NDMP data. They can store backups of regular (non-NDMP) NetBackup clients as well as of NDMP clients.

About assigning tape drives to different hosts

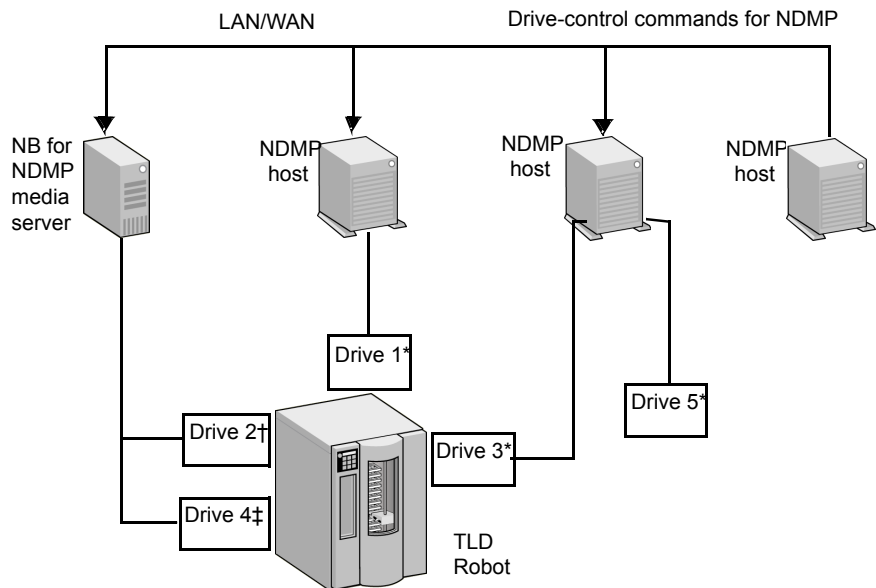
The robotic tape drives can be divided up among NDMP hosts and NetBackup servers.

The following figure shows the NDMP and non-NDMP storage units with the following configuration:

- Tape drives 1, 3, and 5 are attached to NDMP hosts. They are in the NDMP storage units that can be used for NDMP backups (local or three-way). The commands that control these drives originate on the NetBackup for NDMP server and are sent through the NDMP connection on the network. The NDMP server application on each NDMP host translates the NDMP commands into SCSI commands for the local drives.

- Tape drives 2 and 4 are attached to a NetBackup server. They are in non-NDMP storage units and are controlled in the same way as other drives on NetBackup servers. Depending on the type of storage unit, these drives can be used for the following:
 - Non-NDMP clients of NetBackup
 - In the case of tape drives in Media Manager storage units, they can be used for both NDMP (local or three-way) and non-NDMP backups.
- In the following figure, all of the tape drives are used for NDMP backup except drive 4.

Figure 1-5 NDMP and non-NDMP storage units



- * In NDMP storage unit
- † In NetBackup Media Manager storage unit
- ‡ In another type of NetBackup storage unit (not NDMP or Media Manager)

Drives 1, 3, and 5 (in NDMP storage units) can be used for NDMP backups.

Drive 2 (in Media Manager storage unit) can be used for NDMP or non-NDMP backup.

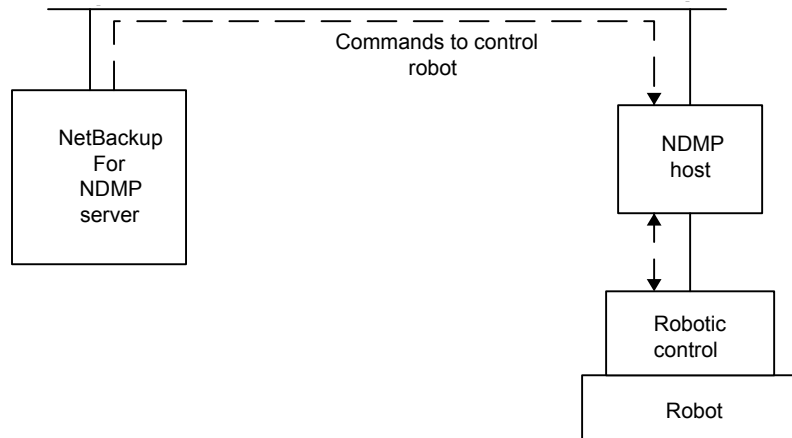
Drive 4 (in different type of NetBackup storage unit) cannot be used for NDMP backup.

About robotics control

Robotics control can be attached to an NDMP host or to a NetBackup server.

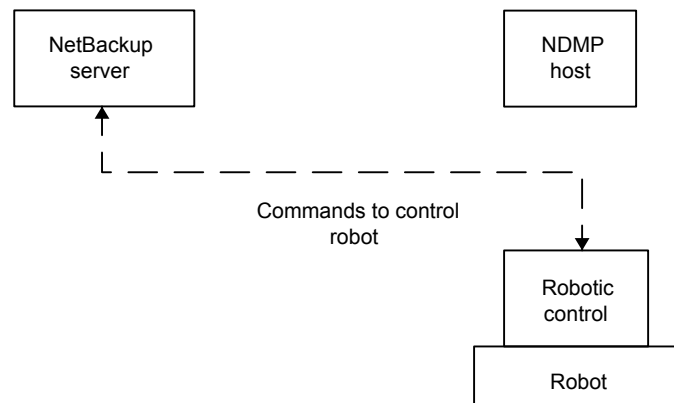
The following figure shows how NetBackup sends commands over the network to the NDMP host, which in turn sends them to the robot.

Figure 1-6 Robotics control that is attached to an NDMP host



The following figure shows how the robot is controlled in the same way as the other robots on NetBackup servers.

Figure 1-7 Robotics control that is attached to a NetBackup server



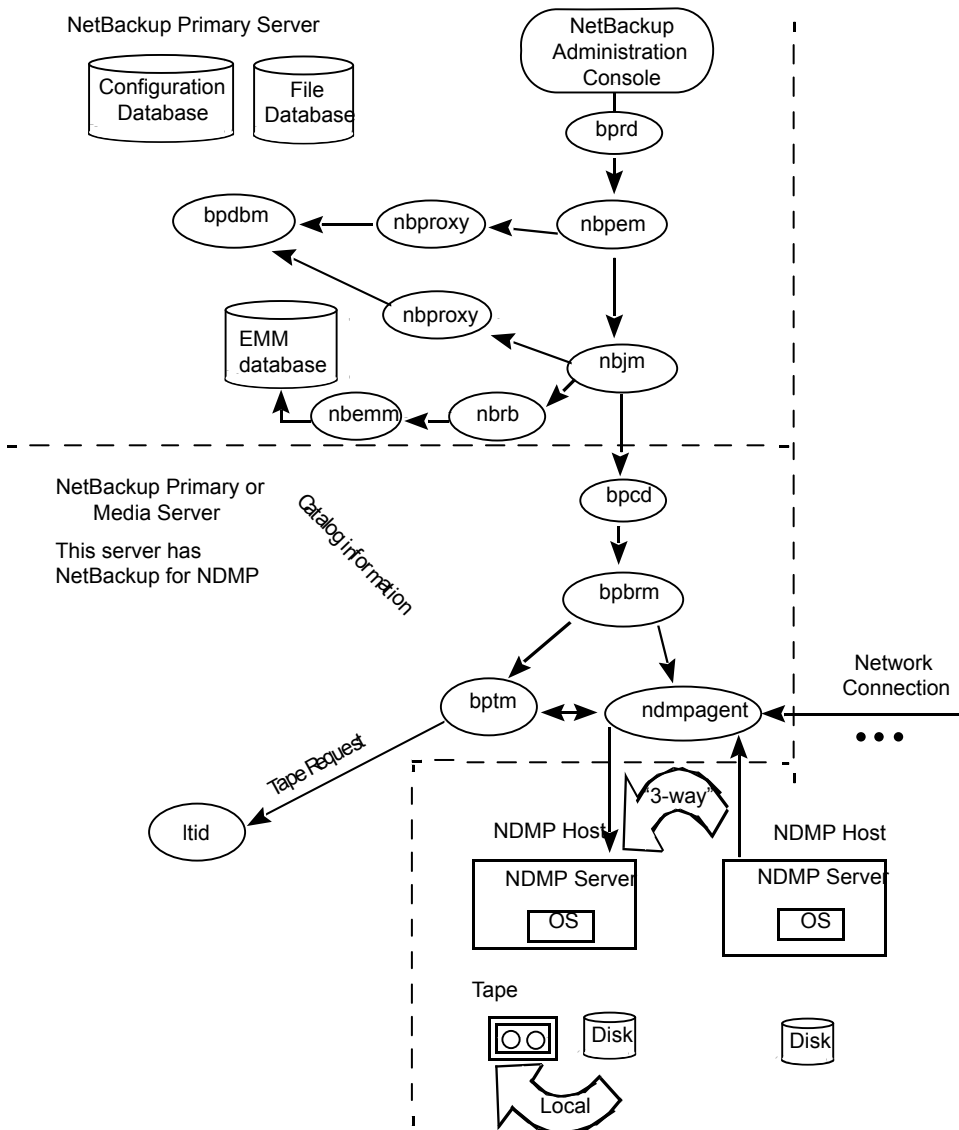
About the NDMP backup process

During a backup, the following events occur in this order:

- From the Enterprise Media Manager (EMM), NetBackup obtains a media ID for the tape that is used for the backup. It then sends a tape-mount request to `ltid`.
- `ltid` on the NetBackup for NDMP server sends the necessary NDMP (SCSI robotic) commands to mount the requested tape on the storage device.
- NetBackup sends the NDMP commands that are necessary to have the NDMP server application perform a backup to the tape. The backup data travels in one of two ways:
 - Between the local disk and tape drives on an NDMP host.
 - Over the network, data travels from an NDMP host without its own storage device to an NDMP host (or NetBackup media server) with a locally attached storage device (three-way back up).
- The NDMP server application sends information to the NetBackup for NDMP server about the files that were backed up. This information is stored in the NetBackup file database.
- The NDMP server application sends status about the backup operation to the NetBackup for NDMP server.

The following figure shows the NetBackup processes that are involved in the NDMP backups.

Figure 1-8 NetBackup backup processes



About the NDMP restore process

Because of the design of the NDMP protocol, only an administrator on a NetBackup server (primary or media) can restore files from NDMP backups. During a restore,

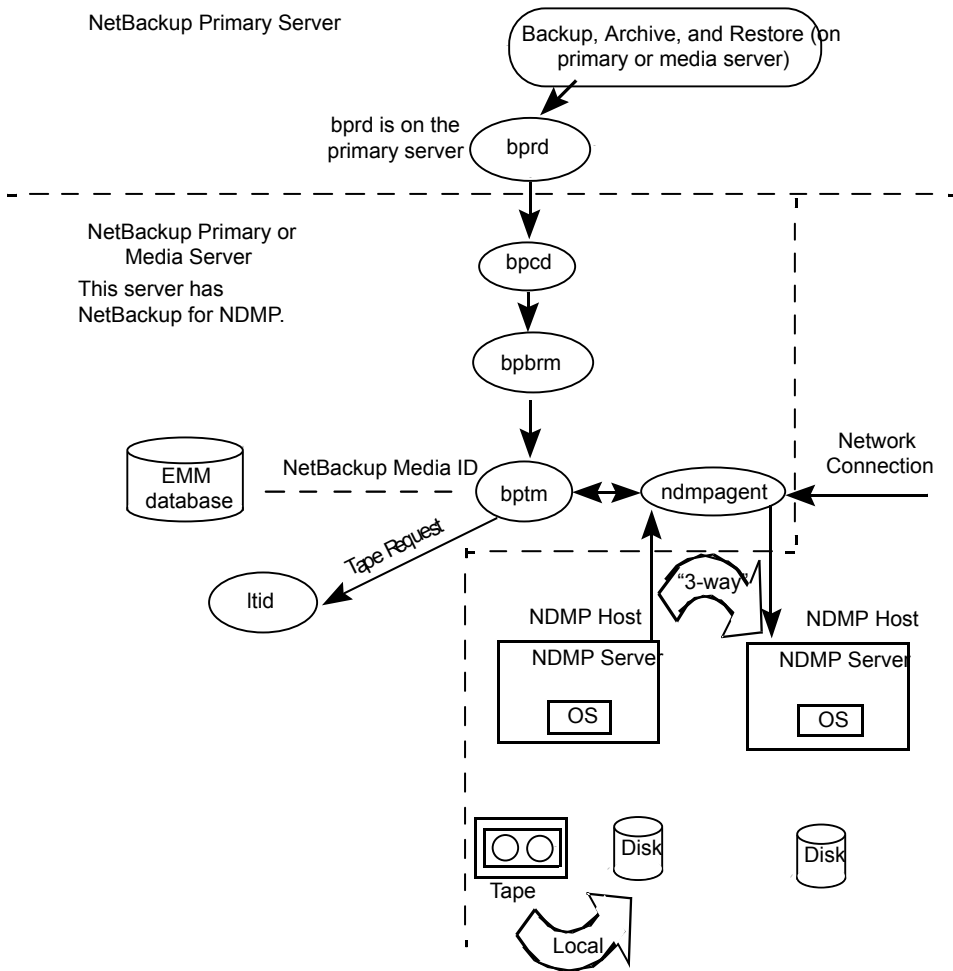
the administrator browses the file catalog and selects files from NDMP images in the same manner as for standard backup images.

The following events occur during a restore, in this order:

- The NetBackup for NDMP server looks in its Enterprise Media Manager (EMM) database for the tape that contains the backup, and asks `ltid` to mount that tape.
- `ltid` on the NetBackup for NDMP server sends the necessary NDMP commands to load the requested tape on the storage device.
- NetBackup sends the NDMP commands that are necessary to have the NDMP server application perform a restore operation to the disk. The restore data travels in one of two ways:
 - From a tape drive to a local disk (tape drive and disk are on the same NDMP host)
 - Over the network, from an NDMP host (or NetBackup media server) with a locally attached storage device to another NDMP host (three-way backups or restores)
- The NDMP server application sends status about the restore operation to the NetBackup for NDMP server.

The following figure shows the NetBackup processes involved in NDMP restores.

Figure 1-9 NetBackup restore processes



About Direct Access Recovery (DAR)

NetBackup uses Direct Access Recovery (DAR) to restore a directory or individual files from a backup image. DAR can greatly reduce the time it takes to restore files and directories. DAR is enabled by default. No configuration is required.

DAR enables the NDMP host to position the tape to the exact location of the requested files. It reads only the data that is needed for those files. For individual file restore, NetBackup automatically determines whether DAR shortens the duration of the restore. It activates DAR only when it results in a faster restore.

The following prerequisites are necessary for using DAR with NetBackup for NDMP:

- The NDMP host must support DAR where the NDMP server application resides.
- NetBackup 4.5 GA or later, with the catalog in binary format (binary format is the default).

Further details are available as to when DAR is used and how to disable it.

See [“About enabling or disabling DAR”](#) on page 61.

Snapshot Client assistance

For Snapshot Client assistance, see the [NetBackup Snapshot Client Administrator's Guide](#).

For additional information, see the Snapshot Client Configuration document:

<http://www.veritas.com/docs/000081320>

The Snapshot Client Configuration document includes the following information:

- An up-to-date list of supported operating systems and peripherals
- A list of NAS vendors that are supported for the NAS_Snapshot method
- Sections on SAN device configuration and on setting up NetBackup for off-host data mover backups (including instructions on creating `3pc.conf` and `mover.conf` files)

About NDMP multiplexing

NDMP multiplexing concurrently writes multiple backup streams to the same tape storage device from the same client or different clients. NDMP multiplexing supports only remote NDMP and improves overall NetBackup performance by better using tape storage devices. State-of-the-art tape storage devices can typically stream data faster than client agents can create backup streams. Therefore multiple data streams can be sent to and effectively processed by a given tape storage unit.

A network-attached storage (NAS) device with an NDMP server is an agent that produces a backup stream that is similar to a NetBackup client. Multiplexing is desired for NDMP backups because NAS devices are limited in the rate at which they create backup streams. These backup streams are often much slower than the tape storage device consuming and writing the stream.

NDMP multiplexing provides the following benefits:

- Several backups can be run at the same time writing to the same tape. This process can reduce the need for many tape devices.

- Backup time is reduced by writing concurrent backups to a single tape storage device.
- Many tape storage devices require that data is streamed to them at high transfer rates. When data is not streamed fast enough, they do not work efficiently and are subject to possible excessive wear.

Consider the following general items when implementing NDMP multiplexing:

- Only media manager tape storage units can be used for NDMP multiplexing.
- Multiplexing of NDMP backups and restores supports only remote NDMP. The remote NDMP processes backup streams by going through the media server.
- NDMP local and NDMP three-way backups and restores are not supported for NDMP multiplexing. Each method processes backup streams without going through the media server.
- Synthetic backups are not supported.
- Only tape devices are supported.
- Disk storage devices are not supported.
- A mix of NDMP and non-NDMP backups can be present in the same MPX backup group.
- File and directory DAR are allowed.
- NDMP multiplexing works with both VTL and PTL. However, VTL users typically do not use NDMP multiplexing because they can add more virtual tape devices to accommodate additional streams.
- For NDMP multiplexed backups the storage unit and policy schedule multiplex value must be set to a value greater than one.

About NDMP support for Replication Director

NDMP can be used to back up, browse, and restore snapshots. The advantage to using Replication Director and creating a backup policy that uses NDMP is that NetBackup needs to mount only the primary data to perform these actions.

For additional information about NDMP with Replication Director, see the [NetBackup Replication Director Solutions Guide](#).

Limitations of Replication Director with NDMP

Consider the following limitations before configuring NDMP to be used with Replication Director:

- The Solaris_x86 operating system is not supported.
- The **Multiple copies** NetBackup policy option is not supported for image copies in the NDMP data format.
- The **Restore the file using a temporary filename** restore option is not supported on Windows clients.
- Restores to a local file system are not supported with an **MS-Windows** or a **Standard** policy that has the NDMP **Data Mover** enabled.
- Do not include both the qtree and the volume on which the qtree resides in the same **Backup Selection** list.
- Only one NDMP backup of a snapshot per `backupid` is allowed.
- The **Index From Snapshot** operation is supported only in a Replication Director configuration, however, a Standard or MS-Windows policy with NDMP Data Mover enabled is also not supported.

Note: The **Index From Snapshot** operation is not supported for NetApp ONTAP 7-mode.

- When you make changes to the NDMP policy after the last full or incremental schedule (for example, if you add or delete a backup selection), the content for the next incremental retrieves the entire content of the snapshot rather than retrieving only the content that has changed. The next incremental schedule however, after only retrieves content that has changed as expected.

About NDMP support for NetApp clustered Data ONTAP (cDOT)

The following table describes the terminology that is used in this topic.

Table 1-3 NetApp cDOT terminology

Term	Definition
CAB	Specifies the Cluster Aware Backup (CAB) NDMP API extension. The CAB enables support of a NetApp cDOT system for optimal, node-transparent backups.
cDOT	Specifies the clustered Data ONTAP (cDOT); the NetApp clustered filer storage solution.

Table 1-3 NetApp cDOT terminology (*continued*)

Term	Definition
Cluster-management LIF	Specifies a single management interface for the entire cluster. This is the only logical interface (LIF) that NetBackup supports for device configuration.
Data LIF	Specifies the data logical interface (LIF) that is associated with the Vserver.
Intercluster LIF	Specifies a logical interface (LIF) that is used for intercluster communication.
LIF	Specifies a logical interface (LIF); an IP address and port that is hosted on a node of a NetApp cDOT system.
Node-management LIF	Specifies a dedicated IP address that is used to manage a node.
SVM	Specifies the Storage Virtual Machine (SVM); a NetApp clustered Data ONTAP construct that is a virtualization layer that includes volumes and LIFs. This allows for non-disruptive user and NDMP operations when the physical cluster resources change. Multi-tenancy is achieved by multiple SVMs (see the data LIF). The cluster itself is also an SVM (see cluster-management LIF).
Vserver	Specifies the virtual storage server; contains data volumes and one or more LIFs through which it serves data to the clients.

It is recommended to run a NetApp cDOT cluster in SVM-scoped NDMP mode (also called Vserver aware mode).

NetBackup supports optimal backup, restore, and duplication of NetApp cDOT FlexVol volumes using the CAB extension. The NetApp cDOT server (that runs in Vserver aware mode) provides unique location information (affinity) about volumes and tape drives. Using this affinity information, NetBackup performs a local backup instead of a three-way or remote backup if a volume and a tape drive share the same affinity. If multiple volumes that are hosted on different nodes are backed up or restored using the same job, NetBackup may switch drive paths if necessary (and possible) to perform the local backup.

Note: The NetApp Infinite volumes can be backed up and restored by using the standard policy types.

Note: There should be at least one intercluster LIF for each node of the cluster that does not host a cluster-management LIF. This is required for three-way and remote backups. If you do not specify an intercluster LIF, all of the three-way and remote backups for volumes that are not hosted on the same node as the cluster-management LIF fail. NetBackup does not access these LIFs directly, so it does not need credentials for them.

Installation Notes for NetBackup for NDMP

This chapter includes the following topics:

- [NetBackup for NDMP installation prerequisites](#)
- [About existing NetApp cDOT configurations before you upgrade](#)

NetBackup for NDMP installation prerequisites

Note the following items before installing NetBackup and adding the NetBackup for NDMP license:

- NetBackup for NDMP functionality installs when the NetBackup server software is installed. No separate installation procedure is required. However, you must enter a valid license to use NetBackup for NDMP.

Note: If your NetBackup for NDMP server is not your primary server, install your NDMP license on the primary server.

In a clustered environment, perform the steps to add the license on each node in the cluster. First, freeze the active node so that migrations do not occur during installation. Unfreeze the active node after the installation completes. For information about freezing or unfreezing a service group, see the clustering section in the [NetBackup High Availability Administrator's Guide](#) for the cluster software you are running.

For more information about administering licenses, see the [NetBackup Administrator's Guide, Volume I](#).

Note: NetBackup for NDMP cannot be uninstalled separately from the full NetBackup product.

If you uninstall the full NetBackup product, make sure that no NetBackup for NDMP backups are active or running for the client. On the primary server, check the Activity Monitor in the **NetBackup Administration Console**. If the **Job State** for the backups indicates `Done`, you can then perform the uninstall procedure that is described in the [NetBackup Installation Guide](#).

- For lists of supported operating systems, hardware platforms, and NAS vendor features and software releases, see the [NetBackup Compatibility List for all Versions](#).

For a list of NAS platforms that NetBackup for NDMP supports, see the [NetBackup for NDMP: NAS Appliance Information](#) document.

- The drives and robots that are attached to the NDMP host must be the types that the NDMP host and NetBackup support. A list of supported robot types is available.

See “[About robotics control](#)” on page 19.

For more information about storage devices, see the [NetBackup Administrator's Guide, Volume I](#).

About existing NetApp cDOT configurations before you upgrade

This topic describes how to upgrade NetBackup with a NetApp cDOT system. If you use a NetApp cDOT system, review the following information before you upgrade to NetBackup 7.7 or later.

If your NetApp cluster is set to **node-scope-mode** and you have not yet installed NetBackup 7.7 or later, your environment should be set up as follows before the upgrade:

- The client name that is used in the backup policy is the node-management LIF.
- Only the volumes that are hosted by the node that hosts the LIF are available for backup or restore. Each node must have a node-management LIF in the client list of the policy.
- Tape devices that are attached to a node are available for backup or restore.
 - The NDMP host name that is used for the device configuration is the node name (node-management LIF).
 - The tape devices are available only to the nodes to which they are connected.

After you upgrade to NetBackup 7.7 or later, everything works as it did before the upgrade until you enable the NetBackup cDOT capabilities by disabling node-scope mode.

To start using the NetBackup cDOT capabilities, do the following:

1. Back up the catalog.
2. (Optional) Create a detailed image catalog report that provides the following:
 - Collects information, such as NDMP host names, policies, and backup selections, that can be used when you create the new cDOT backup policies.
 - Determines the client names to search for when you restore the pre-cDOT backups in the new cDOT environment.
3. Upgrade all of the NetBackup media servers that are authorized to access the cluster. Upgrades do not have to occur at the same time, but must be done before the following step.
4. Enable the Vserver aware mode on the cluster by disabling node-scope-mode. Please see your specific cluster documentation.
5. If there are tape devices attached to the cluster, you must reconfigure your tape devices to use the cluster-management LIF as the NDMP host for the device configuration. See [“About Media and Device Management configuration”](#) on page 40.

Caution: NetBackup only supports the use of the cluster-management LIF for device configurations.

Note: For each node in the cluster that will have tape devices, be sure to configure all of the tape devices available to the cluster on that node. Any node that has access to a tape device should also have access to all of the tape devices.

6. Enable the NDMP service on the cluster for each data LIF that will be used for backups. See the NetApp documentation for more information.
7. Authorize the data LIF as needed for NetBackup access. See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 37.
8. Add, delete, or update the old storage units that are using the node names of the cluster.
9. Add, delete, or update the old policies that back up the cluster.

- You must use either the data LIF or the cluster-management LIF as the client name. NetBackup does not support use of the node name for the client name.
- Backup selections may also need to be adjusted.

Note: The use of the data LIF as a client will protect and catalog all volumes associated with the data LIF's Vserver under this client. The use of the cluster-management LIF as a client will protect and catalog all volumes on the entire cluster under this client.

10. To read the old images, you may have to use alternate client restore. For more information about alternate client restores, see the [NetBackup Administrator's Guide for UNIX, Windows, and Linux, Volume I](#)

If your NetApp cluster is set to **Vserver aware mode**, and you have not yet installed NetBackup 7.7 or later, your environment should be set up as follows before the upgrade:

- The cluster is in Vserver aware mode. The Cluster Aware Backup (CAB) extension is enabled on the filer. NetBackup does not use the CAB extension.
- The client name used in the backup policy is the data LIF associated with a Vserver or the cluster-management LIF.
- Only volumes (that belong to the Vserver) hosted by a node that hosts the data LIF are available for backup or restore.
- The tape devices that are attached to the cluster are not available for backup or restore.

After you upgrade to NetBackup 7.7 or later, the behavior is different and you need to make some changes. NetBackup now uses the CAB extension and enables it by default. Because of this, the following occurs:

- NetBackup uses all of the volumes that belong to the Vserver.
- NetBackup uses the volume affinities.

As a result of this change, the following occurs:

- When the `ALL_FILESYSTEMS` directive is in use by multiple policies for the same Vserver, NetBackup may back up the same volume multiple times under different policies. And further incremental backups may not be reliable.
- Multi-streamed backup jobs will start failing with status code 99. The following message is displayed in the job details for the failed jobs:

```
12/10/2014 14:42:11 - Error ndmpagent (pid=29502) NDMP backup failed,
path = /vs02/vol1:PARAMETER:AFFINITY=4ac6c4b6-7e99-11e4-b3b6-1779f43af917
```

This happens because some components of NetBackup are not told to use the cluster in the Vserver aware mode. It is highly recommended to upgrade and enable the cDOT capabilities as soon as possible.

To start using the cDOT capabilities, you must do the following:

1. Back up the catalog.
2. Create a detailed image catalog report (it can be referenced later for read operations).
3. Upgrade all of the NetBackup media servers that are authorized to access the cluster. All media servers should be upgraded at the same time to avoid inconsistent behavior.
4. Run the `tpautoconf -verify ndmp_host` command for each pre-existing LIF that is configured in NetBackup. This command must be run from the media servers that have credentials to the LIF. After the command is successfully run, the `nbemmcmd` command should display output similar to the following example:

```
servername1@/>nbemmcmd -listsettings -machinename machinenam123 -machinetype ndmp
NBEMMCMD, Version: 7.7
The following configuration settings were found:
NAS_OS_VERSION="NetApp Release 8.2P3 Cluster-Mode"
NAS_CDOT_BACKUP="1"
Command completed successfully.
```

NAS_OS_VERSION displays the NetApp Version.
 NAS_CDOT_BACKUP tells us if NetBackup uses the new cDOT capabilities.

Note: The `tpautoconf -verify ndmp_host` command is not required when a new Vserver is added.

5. You can now add devices to the NDMP cluster and access them using the cluster-management LIF. If you add devices, you must discover the devices.
6. Add storage units for the newly discovered devices.
7. Add, delete, or update the policies that reference the cluster as needed. Start using the cluster in Vserver aware mode.

If you do not want to enable the cDOT functionality immediately; for example, you want to upgrade the media servers in phases, you can disable the cDOT capabilities by doing the following:

1. Create the following touch file on all of the media servers that are authorized to access the NDMP host. This causes NetBackup to disable the CAB extension for all of the NDMP hosts for that media server.
 - On Windows: `install_path\NetBackup\db\config\DISABLE_NDMP_CDOT`
 - On UNIX: `/usr/opensv/netbackup/db/config/DISABLE_NDMP_CDOT`
2. You can disable the CAB extensions for specific NDMP hosts by creating the following file on the media servers with one or more NDMP host names (one per line):
 - On Windows:


```
install_path\NetBackup\db\config\DISABLE_NDMP_CDOT_HOST_LIST
```
 - On UNIX:


```
/usr/opensv/netbackup/db/config/DISABLE_NDMP_CDOT_HOST_LIST
```

An example of the content of the file is as follows. NetBackup disables the CAB extension only for Filer_1 and Filer_2.

```
Filer_1
```

```
Filer_2
```

To enable the cDOT functionality, these files must be deleted and you must follow all of the steps explained in the previous upgrade procedure.

Configuring NDMP backup to NDMP-attached devices

This chapter includes the following topics:

- [About configuring NDMP-attached devices](#)
- [Authorizing NetBackup access to a NAS \(NDMP\) host](#)
- [About access for three-way backups and remote NDMP](#)
- [About Media and Device Management configuration](#)
- [Using the Device Configuration Wizard to configure an NDMP filer](#)
- [About adding volumes](#)
- [About verifying NDMP password and robot connection](#)
- [Adding NDMP storage units](#)
- [About creating an NDMP policy](#)
- [About enabling or disabling DAR](#)
- [Configuring NetBackup for NDMP in a clustered environment](#)

About configuring NDMP-attached devices

This topic explains how to configure backups on the storage devices that are attached to NDMP hosts. Only the NDMP-specific steps are described.

You can also use the NetBackup **Device Configuration Wizard** to discover and configure the robots and drives that are attached to an NDMP host. The wizard requires NDMP protocol versions V3 or V4.

To configure and use the NAS_Snapshot method, see the [NetBackup Snapshot Client Administrator's Guide](#).

See [“About adding volumes”](#) on page 47.

Authorizing NetBackup access to a NAS (NDMP) host

Before NetBackup can perform backups using NDMP, it must have access to the NAS (or NDMP) host.

Note: Perform the following procedure on the primary server (not media server) if you plan to create snapshots using Replication Director.

To authorize NetBackup access to the NDMP host

- 1 On the NetBackup server **NetBackup Administration Console**, expand **Media and Device Management > Credentials > NDMP Hosts**.
- 2 Under the **Actions** menu, select **New > New NDMP Host**.
- 3 In the **Add NDMP Host** dialog box, enter the name of the NDMP server for NetBackup to back up.

If you are using NetApp's Clustered Data ONTAP, the NDMP host must be a Storage Virtual Machine (SVM).

The NDMP host name is case-sensitive. The name must match the name that is entered here whenever this host name is used.

Note: If you do not plan to use Replication Director and you add NDMP host credentials using the fully qualified domain name (FQDN), you must also indicate the fully qualified domain name on the client for lookups. That is, the server list in the **Backup, Archive, and Restore** client interface must list the NDMP host by the FQDN as well.

If you add NDMP host credentials using a short name, you can use either the short name or the FQDN in the client server list.

- 4 Click **OK**.
- 5 In the **New NDMP Host** dialog box, specify the following:

(The term credentials refers to the user name and password that NetBackup uses to access the NDMP host.)

Use global NDMP credentials for this NDMP host

Note: The **Use global NDMP credentials for this NDMP host** option is not available from the NetBackup web UI.

Enables all NetBackup media servers under the primary server to access this NDMP host using a predefined global NDMP logon.

To create this logon, click **Host Properties > Master Server > Properties > NDMP** in the **NDMP Global Credentials** dialog box.

Note: Because NetApp generates a separate, encrypted password for each SVM, this option cannot be used with NetApp's Clustered Data ONTAP.

Use the following credentials for this NDMP host on all media servers

Enables all NetBackup media servers that are connected to the NDMP host to access the NDMP host using the logon you specify:

- **User name:** The user name under which NetBackup accesses the NDMP server. This user must have permission to run NDMP commands.
You can find out whether your NDMP host vendor requires a particular user name or access level.
- **Password and Confirm Password:** Enter the password for this user.

For information about passwords for NAS devices, see the *NetBackup for NDMP: NAS Appliance Information* from the Veritas Support website:
<http://www.veritas.com/docs/000027113>

Use different credentials for this NDMP host on each media server

Specifies NDMP logons for particular NetBackup servers. Then click **Advanced Configuration**.

- In the **Advanced NDMP Credentials** dialog box, click **Add**.
- In the **Add Credentials** dialog box, select a NetBackup server and specify the user name and password it uses to access the NDMP host.
- Click **OK**. NetBackup validates the user name and password.
- The NetBackup server and user name appear in the **Advanced NDMP Credentials** dialog box.
- If necessary, click **Add** again to specify other servers and user

6 Repeat this procedure for each NDMP host that NetBackup backs up.

See [“About access for three-way backups and remote NDMP”](#) on page 39.

See [“About configuring NDMP-attached devices”](#) on page 36.

See [“Configuring NDMP backup to Media Manager storage units”](#) on page 66.

See [“Configuring NetBackup for NDMP in a clustered environment”](#) on page 63.

About access for three-way backups and remote NDMP

To perform three-way backups, you must authorize access to the NDMP host as described in the previous section.

Note the following points:

- Three-way backups; for the **NDMP host name**, specify the NDMP host that has no attached tape drive.
- NDMP to Media Manager storage units (remote NDMP); for the **NDMP host name**, specify the NDMP host to back up to the Media Manager storage unit that is defined on the NetBackup server.

See [“About remote NDMP”](#) on page 65.

See [“About configuring NDMP-attached devices”](#) on page 36.

About Media and Device Management configuration

On the NetBackup for NDMP server, use **Media and Device Management** in the **NetBackup Administration Console** to add drives and robots. As an alternative, you can use the NetBackup **Device Configuration Wizard**.

Note: It is recommended to connect any tape drive that is attached to a NetApp cDOT system to all of the cluster nodes. If you do not follow this recommendation, NetBackup may not be able to find the optimal path for data transfer.

The following procedures and examples treat NDMP configuration issues only.

- See [“Using the Device Configuration Wizard to configure an NDMP filer”](#) on page 43.
- See [“Adding a robot directly attached to an NDMP host”](#) on page 41.
- See [“Adding a tape drive”](#) on page 42.
- See [“Checking the device configuration”](#) on page 43.

See the [NetBackup Administrator's Guide for UNIX, Windows, and Linux, Volume I](#), for general information on configuring NetBackup media.

More information on configuring storage devices for specific NDMP hosts is available.

- For information about supported NDMP operating systems and NAS vendors, access *NetBackup for NDMP: NAS Appliance Information* from the Veritas Support website. The topic also contains configuration and troubleshooting help for particular NAS systems:
<http://www.veritas.com/docs/000027113>
- For a list of the features and software releases for each NAS vendor, for SSO support, and for the NetBackup versions that support these vendors, see the [NetBackup Compatibility List for all Versions](#).

These procedures do not apply to setting up the devices that are attached to the NetBackup media server. To back up NDMP data to media servers, you must configure storage units in the same way as ordinary NetBackup (non-NDMP) devices. More information is available:

See [“About remote NDMP”](#) on page 65.

See [“About adding volumes”](#) on page 47.

See [“About configuring NDMP-attached devices”](#) on page 36.

Adding a robot directly attached to an NDMP host

This procedure describes how to configure a robot that is attached to an NDMP host.

To add a robot directly attached to an NDMP host

- 1
- Start the **NetBackup Administration Console** on the NetBackup for NDMP server as follows:

Windows	In the Windows Start menu, click Programs > Veritas NetBackup > NetBackup Administration Console .
UNIX	Enter the following: <code>/usr/opensv/netbackup/bin/jnbSA &</code>

- 2
- Expand **Media and Device Management > Devices** in the left pane.
- 3
- On the **Actions** menu, select **New**. Then select **New Robot** from the pop-up menu.
- 4
- In the **Add Robot** dialog box, select the following:

Media Manager host	Specify the host that manages the Enterprise Media Manager (EMM) data in the NetBackup database. (By default, this host is the NetBackup primary server.)
Device host	Use the pull-down to select the NetBackup media server.
Robot type	Specify type.
Robot number	Specify number.
Robot control	Select Robot control is attached to an NDMP host .
Robot device path	Enter the device name of the robot. You do not need to include the NDMP host name as part of the device path.
NDMP host name	Enter the name of the NDMP host to which the robot is attached
Bus, Target, and LUN values	Specify these values if the NDMP host requires them. By default, the bus, target, and LUN values are 0.

For further assistance with the **Add Robot** dialog box, refer to the online Help. The following steps explain the portions that are unique to configuring NetBackup for NDMP.

- 5 Click **OK**.
- 6 In the pop-up message that asks if you want to stop and restart the device manager service (or daemon), click **Yes**.

See [“About configuring NDMP-attached devices”](#) on page 36.

Adding a tape drive

This procedure describes how to configure a tape drive.

To add a tape drive

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Devices > Drives**.
- 2 Select **Add a New Drive**. In the dialog box, click **Add**.
- 3 In the **Add a New Drive** dialog box, enter the name of the drive in the **Drive Name** box.
- 4 Click **Add** to specify a drive path.
- 5 In the **Add Path** dialog box, select the host and the path information as follows:

Device host Select the name of the NetBackup media server. Use the pull-down to select media servers already defined, or click **Add** to enter a new one.

Path Enter the device file name of the tape drive, such as `nrst2a`. Refer to the NAS vendor documentation for your drive for the correct format of the device file name.

An alternate method is to use the following command to find the device file name for the drive, if the NDMP host is running NDMP protocol V3 or later:

```
tpautoconf -probe ndmp_host_name
```

- 6 Click **This path is for a Network Attached Storage device**.
- 7 In the **NDMP Host** drop-down list, select the name of the NAS filer to which the drive is attached.
- 8 Click **OK**.
- 9 Return to the **Add a New Drive** dialog box and enter the drive information as required. Repeat this procedure for each drive that must be added.

When you are prompted to restart the Media Manager device daemon and all robotic daemons, click **Yes**.

See [“About configuring NDMP-attached devices”](#) on page 36.

Checking the device configuration

On the NetBackup for NDMP server, use the following procedure to check the device configuration.

To check the device configuration

- 1 On UNIX:
 - Execute `/usr/opensv/volmgr/bin/vmps`.
 - Verify that `ltid`, `vmd`, `avrd`, and any required robotic daemons are active.

On Windows:

 - From the **NetBackup Administration Console**, select **Activity Monitor**.
 - In the right pane, select the **Processes** tab.
 - Verify that `ltid`, `vmd`, `avrd`, and any required robotic daemons processes are active.
- 2 From the **NetBackup Administration Console**, click **Device Monitor**.
 Ensure that the drive status is in the UP state.

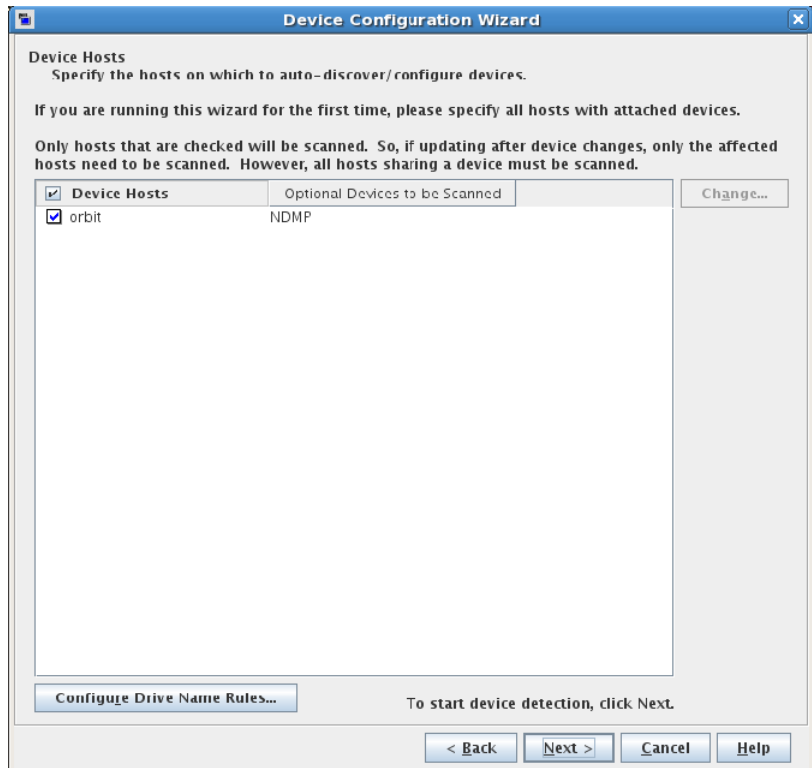
See [“About configuring NDMP-attached devices”](#) on page 36.

Using the Device Configuration Wizard to configure an NDMP filer

This procedure shows how to use the **Device Configuration Wizard** of the NetBackup Administration Console to configure NetBackup to an NDMP filer. This wizard provides the most convenient way to configure devices and storage units for NDMP hosts.

To use the Device Configuration Wizard

- 1 In the **NetBackup Administration Console**, click **Configure Storage Devices** in the right panel to launch the **Device Configuration Wizard**.
- 2 Click **Next** on the **Welcome** window. The **Device Hosts** window appears.



- 3 Under **Device Hosts**, put a check by the NetBackup media server that accesses the NDMP host.
- 4 Select the server name and click **Change**.

- 5 In the **Change Device Host** window, place a check beside **NDMP server**, then click **OK**.

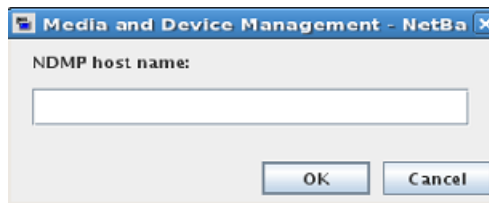


In the **Device Hosts** window, NDMP is now listed in the **Optional Devices to be Scanned** column for the media server.

- 6 Click **Next** to display the **NDMP Hosts** panel.

Note: For a NetApp cDOT system, the NDMP host must be a cluster-management LIF. NetBackup does not support any other LIF type as the NDMP host name for storage device configuration.

- 7 To add a new NDMP host, click **New**. The following window appears:



- 8 Enter the new NDMP host name and click **OK**. The **NDMP Host Credentials** window appears.

Change NDMP Host - na3250cm1cl

NDMP host: na3250cm1cl

NDMP Host Credentials

☐ Use global NDMP credentials for this NDMP host

☒ Use the following credentials for this NDMP host on all media servers

User name:
admin

Password:
.....

Confirm Password:
.....

☐ Use different credentials for this NDMP host on each media server
(Use Advanced Configuration)

To configure individual media server credentials or to override global and NDMP host level credentials, use Advanced Configuration.

Advanced Configuration...

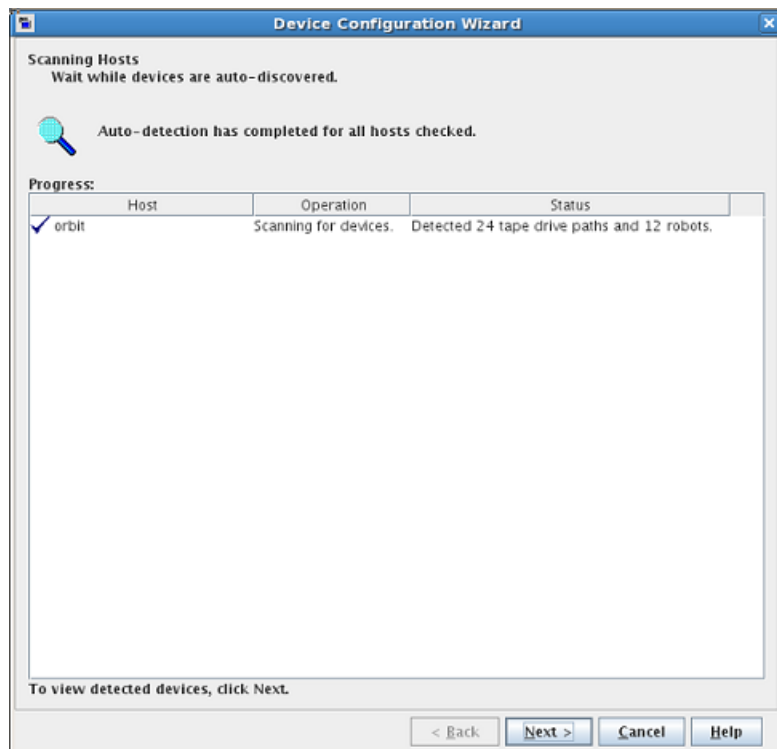
OK Cancel Help

- 9 Select **Use the following credentials for this NDMP host on all media servers**. Enter the User name and password for the desired NDMP filer.

For information about credentials for your specific NDMP filer, refer to the *NetBackup for NDMP: NAS Appliance Information* from the Veritas Support website:

<http://www.veritas.com/docs/000027113>

The **Scanning Hosts** window appears. NetBackup scans the host to discover all attached tape and disk devices. When completed, the **Scanning Hosts** window looks like the following example:



- 10 Follow the remaining prompts in the wizard to complete the configuration.

About adding volumes

Use the NetBackup **Media and Device Management** utility to add the volumes that you plan to use for the NDMP host backups.

See the [NetBackup Administrator's Guide, Volume I](#), for instructions.

When you specify the **Robot control host** for a volume that is in a robot, specify the host name for the NetBackup for NDMP server. Do not specify the NDMP host.

See [“About configuring NDMP-attached devices”](#) on page 36.

About verifying NDMP password and robot connection

When you authorize NetBackup access to the NDMP host and configure robots using the **NetBackup Administration Console**, NetBackup automatically verifies the NDMP credentials and the robotic configuration. If you want, you can re-verify them. For example:

```
tpautoconf -verify ndmp_host_name
```

A successful verification looks like the following:

```
Connecting to host "stripes" as user "root"...
Waiting for connect notification message...
Opening session--attempting with NDMP protocol version n...
Opening session--successful with NDMP protocol version n
  host supports MD5 authentication
Getting MD5 challenge from host...
Logging in using MD5 method...
Host info is:
  host name "stripes"
  os type "NetApp"
  os version "NetApp Release n.n.n.n"
  host id "0033625811"
Login was successful
Host supports LOCAL backup/restore
Host supports 3-way backup/restore
```

Adding NDMP storage units

On the NetBackup primary server, add an NDMP-type storage unit for the devices that contain the backup data. Most of the requirements are the same as for adding a Media Manager storage unit. The following procedure explains how to add an NDMP storage unit.

See the [NetBackup Administrator's Guide, Volume I](#), for more information on storage units.

The NDMP-type storage units are not used for backups to devices that are attached to NetBackup media servers. Use a non-NDMP storage unit instead.

See [“About remote NDMP”](#) on page 65.

To add NDMP storage units

- 1 In the **NetBackup Administration Console**, select **NetBackup Management > Storage**.
- 2 On the **Actions** menu, select **New > New Storage Unit**.
- 3 In the **New Storage Unit** dialog box, enter the following:

Storage unit name	Enter a unique name for the storage unit.
Storage unit type	Select NDMP .
On demand only	Specify whether the storage unit is available only when a policy or schedule specifically requests it. If this option is not used, the storage unit is available to any NDMP policy or schedule.
Storage Device	Select the type of device for this storage unit.
NDMP Host	Specify the NDMP host; for NetApp cDOT systems, you must specify a cluster-management LIF. NetBackup does not support any other LIF type as the NDMP host name for storage device configuration.
Media server	Select the media server associated with this storage unit.
Maximum concurrent write drives	Select the maximum number of drives for concurrent writing.
Reduce fragment size to	Enter the minimum fragment size for this storage unit.
Enable multiplexing	Enter 1 as multiplexing is not allowed with NDMP storage units.
Maximum streams per drive	Select the maximum number of data streams to use with NDMP multiplexing.
Note: You must select at least two data streams.	

The remaining fields are described in the [NetBackup Administrator's Guide, Volume I](#) and the online Help.

See [“About configuring NDMP-attached devices”](#) on page 36.

About creating an NDMP policy

On the NetBackup primary server, you must create an NDMP policy to configure backups of the NDMP host.

Note: You can use the **Backup Policy Configuration Wizard** to create NDMP policies.

Creating an NDMP policy is very similar to creating other NetBackup policy types. The following topics explain the differences when creating NDMP policies.

- See [“Attributes tab options for an NDMP policy”](#) on page 50.
- See [“Schedules tab options for an NDMP policy with Accelerator for NDMP enabled”](#) on page 51.
- See [“Clients tab options for an NDMP policy”](#) on page 52.
- See [“Backup selection options for an NDMP policy”](#) on page 52.
- See [“About appropriate host selection for NetApp cDOT backup policies”](#) on page 60.

See the [NetBackup Administrator’s Guide, Volume I](#), for more information on NetBackup policies and the Policy utility.

To configure an NDMP policy for the NDMP Snapshot and Replication method, see the [NetBackup Replication Director Solutions Guide](#).

To configure a policy for the NAS_Snapshot method, see the [NetBackup Snapshot Client Administrator’s Guide](#).

Attributes tab options for an NDMP policy

The following policy attributes are applicable when you create an NDMP policy:

Policy Type: NDMP Do not select any other policy type.

Policy Storage Unit	■ To direct backups for this policy to a specific storage unit if the NDMP host has multiple storage units, specify that storage unit name. ■ For policies that use Accelerator for NDMP, the storage unit groups are supported only if the storage unit selection in the group is Failover. See the Use Accelerator attribute. ■ For a three-way backup , specify a storage unit that was defined for the target NDMP host with attached tape. ■ For NDMP backup to Media Manager storage units, specify a Media Manager storage unit that is defined for a device that is connected to a NetBackup media server. See “About remote NDMP” on page 65.
Use Accelerator	Select Use Accelerator to enable Accelerator for NDMP. See the Policy Storage Unit attribute. See “About NetBackup Accelerator for NDMP” on page 76. for more information.
Replication Director	Select the Replication Director to configure an NDMP policy for Replication Director.
Allow multiple data streams	Set the value to a number greater than 1.

Schedules tab options for an NDMP policy with Accelerator for NDMP enabled

In the schedules list under the **Attributes** tab, the following parameter is optional for an NDMP policy with Accelerator for NDMP enabled.

Accelerator forced rescan

Select this option to enable an Accelerator forced rescan. This option is available only for the NDMP policies that use Accelerator for NDMP.

An Accelerator forced rescan provides a safety net by establishing a new baseline for the next Accelerator backup. When you include this option, all the data on the filer is backed up. This backup is similar to the first full Accelerator backup: it provides a new baseline for the backups that follow. If you set up a weekly full backup schedule with the **Use Accelerator** option, you can supplement the policy with another schedule that enables **Accelerator forced rescan**. You can set the schedule to run every 6 months or whenever it is appropriate for your environment. Expect backups with **Accelerator forced rescan** to run slightly longer than accelerated full backups.

More information about Accelerator for NDMP is available:

See [“About NetBackup Accelerator for NDMP”](#) on page 76.

Clients tab options for an NDMP policy

In the client list, the following options are required for each client in an NDMP policy:

Hostname

Name of the NDMP host. If you use a NetApp cDOT system, the NDMP host name can only be a Vserver (a data LIF or a cluster-management LIF). NetBackup does not support any other LIF type as the NDMP host name.

Hardware and operating system

NDMP NDMP. If you use a NetApp cDOT system, NetBackup changes the operating system name from NDMP to cDOT.

Backup selection options for an NDMP policy

The backup selections list must specify directories from the perspective of the NDMP host.

For example:

```
/vol/home/dir1/  
/vol/vol1
```

If you have a Windows primary server or media server, you cannot specify a directory that contains unsupported characters in its name. For example, Windows does not support the following characters in file and folder names and therefore they cannot be used in backup selection specifications:

- ~ (tilde)

- # (number sign)
- % (percent)
- & (ampersand)
- * (asterisk)
- [] (braces)
- / (backslash)
- : (colon)
- < > (angle brackets)
- ? (question mark)
- \ (slash)
- | (pipe)
- " (quotation mark)

Refer to your Windows documentation for a complete list of unsupported characters.

You can also use wildcard characters in regular expressions or the directive `ALL_FILESYSTEMS` to specify path names in NDMP policy backup selections.

See [“Wildcard characters in backup selections for an NDMP policy”](#) on page 53.

See [“ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives”](#) on page 56.

See [“About environment variables in the backup selections list”](#) on page 58.

See [“About configuring NDMP-attached devices”](#) on page 36.

Wildcard characters in backup selections for an NDMP policy

You can use wildcard characters in regular expressions or the directive `ALL_FILESYSTEMS` to specify path names in NDMP policy backup selections.

Wildcard characters in regular expressions or directives are valid for streaming and non-streaming NDMP backups.

Note: Directory-level expansion is not supported for some NDMP servers. Some NDMP filer vendors do not have the APIs that NetBackup uses to support wildcard characters lower than the volume level.

If you specify a backup selection using wildcard characters lower than the volume level for these filers, status code 106 is generated. The following message is displayed: **Invalid file pathname found, cannot process request**.

Currently, only NetApp filers support wildcard characters for backup selections lower than the volume level. This support is not available in NetApp clustered Data ONTAP version 8.2.

To see the versions of NetApp Data ONTAP that support wildcard characters for backup selections lower than the volume level, refer to the [NetBackup Compatibility List for all Versions](#).

You cannot use any wildcard characters that also match file names. For example, a backup selection might include `/vol/vol_archive_01/autoit*`. This specification might match a path name such as `/vol/vol_archive_01/autoit_01/`. However, if this specification also matches a file name like `/vol/vol_archive_01/autoit-v1-setup.exe`, the backup job fails with status code 99 because wildcards can specify only path names. The following message is displayed: **NDMP backup failure (99)**.

Table 3-1 Valid wildcard characters for NDMP policy backup selections

Wildcard character	Description
*	Specifies a string match. For example: <pre>/vol/vol_archive_*</pre> This form of the path specification matches all paths that begin with the literal characters <code>/vol/vol_archive_</code> and end with any characters. The string match wildcard can also specify multiple variable characters between literal characters as in the following examples: <pre>/vol/ora_*archive or /vol/ora_*archive*</pre> <pre>/vol/ora_vol/mtree_*archive or /vol/ora_vol/mtree_*archive*</pre>
?	Specifies a single-character match. <pre>/fs?</pre> This path specification matches all paths that begin with the literal characters <code>/fs</code> and end with any single character. For example, <code>/fs1</code>, <code>/fs3</code>, <code>/fsa</code>, <code>/fsd</code> and so on match the specified pattern <code>/fs?</code>.

Table 3-1 Valid wildcard characters for NDMP policy backup selections
(continued)

Wildcard character	Description
[...]	Specifies an alphanumeric pattern match. For example: <pre>/fs[1-9]</pre> This path specification matches all paths that begin with the literal characters <code>/fs</code> and end with any single numeric character from 1 through 9. For example, <code>/fs1</code>, <code>/fs2</code>, and so on up to <code>/fs9</code> match the specified pattern <code>/fs[1-9]</code>. However, <code>/fs0</code> and <code>/fsa</code> do not match the specified pattern; 0 is out of the specified numeric range, and <code>a</code> is a non-numeric character. The pattern match wildcard can also specify alphanumeric patterns such as <code>/fs[1-5a]</code>. This specification matches <code>/fs1</code>, <code>/fs2</code>, and so on up to <code>/fs5</code> as well as <code>/fsa</code>. Similarly, the pattern match wildcard can also specify patterns like <code>/fs[a-p4]</code>. This specification matches <code>/fsa</code>, <code>/fsb</code>, and so on up to <code>/fsp</code> as well as <code>/fs4</code>. You must use multiple backup selection specifications if the pattern can match more than 10 volume names in a numeric series. For example, you may want to back up 110 volumes that begin with the literal characters <code>/vol/ndmp</code> and are numbered 1 through 110. To include these volumes in a backup selection with wildcards, specify three backup selections with the following wildcard patterns: ■ <code>/vol/ndmp[0-9]</code> This pattern matches any volume name that begins with <code>/vol/ndmp</code> and ends with a single numeric character 0 through 9. ■ <code>/vol/ndmp[0-9][0-9]</code> This pattern matches any volume name that begins with <code>/vol/ndmp</code> and ends with the two-digit numeric characters 00 through 99. ■ <code>/vol/ndmp[0-9][0-9][0-9]</code> This pattern matches any volume name that begins with <code>/vol/ndmp</code> and ends with the three-digit numeric characters 000 through 999. Do not specify <code>/vol/ndmp[1-110]</code> in this example. This pattern produces inconsistent results.
{...}	Curly brackets can be used in the backup selection list and the <code>VOLUME_EXCLUDE_LIST</code> directive for NDMP policies. A pair of curly brackets (or braces) indicates multiple volume or directory name patterns. Separate the patterns by commas only; no spaces are permitted. A match is made for any or all entries. For example: <pre>{*volA,*volB} or {volA*,volB*}</pre>

Note the following restrictions and behaviors regarding wildcard expressions:

- It is not recommended that you use a single forward-slash character (/) in an NDMP policy backup selection. This method of including all the volumes on an NDMP filer in the selection is not supported. Instead, use the `ALL_FILESYSTEMS` directive:

See “[ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives](#)” on page 56.

- Nested wildcard expressions can result in recursive path name expansion operations that can impact performance, especially for directories that have a very large number of files or directories. An example of nested wildcard expansion is as follows:

```
/vol/fome06/*/*private
```

- Wildcard expressions do not span or include a path separator (/).
- All backup selections that contain a wildcard expression must start with a path separator (/). An example of a correct wildcard expression is as follows:

```
/vol/archive_*
```

An example of an incorrect wildcard expression is as follows:

```
vol/archive_*
```

ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives

The `ALL_FILESYSTEMS` directive provides a method to include all file systems and volumes on an NDMP filer in an NDMP backup policy.

You can exclude specific volumes from an `ALL_FILESYSTEMS` backup selection if you do not want to back up every volume on an NDMP filer. Use the `VOLUME_EXCLUDE_LIST` directive for this purpose. You may use valid wildcard characters in the `VOLUME_EXCLUDE_LIST` statement.

Note: The following examples use selections that are specific to NetApp Data ONTAP 7-mode. For specific examples of backup selections for other configurations, refer to the appropriate documentation.

The `VOLUME_EXCLUDE_LIST` statements must precede `ALL_FILESYSTEMS` statement. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Hr_allfiles_vol01  
ALL_FILESYSTEMS
```

or

```
VOLUME_EXCLUDE_LIST=/vol/testvol*  
ALL_FILESYSTEMS
```

To specify multiple values in a `VOLUME_EXCLUDE_LIST` statement, separate the values with a comma. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Hr_allfiles_vol01,/vol/testvol*  
ALL_FILESYSTEMS
```

You can also specify more than one `VOLUME_EXCLUDE_LIST` statement with an `ALL_FILESYSTEMS` directive. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Hr_allfiles_vol01  
VOLUME_EXCLUDE_LIST=/vol/testvol*  
ALL_FILESYSTEMS
```

A `VOLUME_EXCLUDE_LIST` statement may include a maximum of 256 characters. Create multiple `VOLUME_EXCLUDE_LIST` statements if necessary to avoid exceeding the limit of 256 characters. If you specify more than 256 characters, the volume list is truncated. A truncated statement may result in a backup job failure, and the error message `Invalid command parameter(20)` is displayed.

If the backup selection includes read-only volumes or full volumes, an NDMP backup job fails with the status code 20 (`Invalid command parameter(20)`). If you encounter a similar NDMP backup job error, review the `ostfi` logs to identify the volumes for which the failure occurred. You can use `VOLUME_EXCLUDE_LIST` statements with the `ALL_FILESYSTEMS` statement to exclude the read-only volumes and the volumes with insufficient space.

In a NetBackup Replication Director environment where snapshots are replicated to a secondary filer, it is recommended that you use storage lifecycle policies to control backups on the secondary filer.

On NetApp 7-mode storage systems, it is generally not recommended for users to store files in `/vol/vol0` because the volume contains filer system files. For this reason, `vol0` should be excluded from the backup if the `ALL_FILESYSTEMS` directive is used in the backup policy. The following is a backup selection list that excludes `/vol/vol0`:

```
VOLUME_EXCLUDE_LIST=/vol/vol0  
ALL_FILESYSTEMS
```

- Do not use `ALL_FILESYSTEMS` to backup all volumes on a secondary filer. Inconsistencies may occur when automatically created NetApp FlexClone volumes are backed up or restored. Such volumes are temporary and used as

virtual copies or pointers to actual volumes and as such do not need to be backed up.

- If you must back up all volumes on a secondary filer, it is recommended that you exclude the FlexClone volumes as well as replicated volumes. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Clone_*
VOLUME_EXCLUDE_LIST=/vol/*_[0-9]
VOLUME_EXCLUDE_LIST=/vol/*_[0-9][0-9]
VOLUME_EXCLUDE_LIST=/vol/*_[0-9][0-9][0-9]
ALL_FILESYSTEMS
```

This example assumes all FlexClone volumes and only FlexClone volumes begin with `/vol/Clone_`. Adjust the volume specifications appropriately for your environment.

- `VOLUME_EXCLUDE_LIST` applies only to `ALL_FILESYSTEMS`. It does not apply to explicit backup selections or wildcard-based backup selections.

If you use the `ALL_FILESYSTEMS` directive in an NDMP policy for Clustered Data ONTAP, you must exclude each selected SVM's root volume using the `VOLUME_EXCLUDE_LIST` directive. Otherwise the backups fail.

For more information about creating backup policies for Clustered Data ONTAP with Replication Director, see the [NetBackup Administrator's Guide, Volume I](#).

Backups from snapshots for NDMP policies fail when the import of a snapshot fails for volumes where logical unit numbers (LUNs) reside with status code 4213 (Snapshot import failed). To avoid this error, use the `VOLUME_EXCLUDE_LIST` directive to exclude any volumes that are used to create LUNs accessed through a storage area network (SAN).

About environment variables in the backup selections list

NDMP lets you use environment variables to pass configuration parameters to an NDMP host with each backup. NDMP environment variables can be one of the following types:

- Defined as optional by the NDMP protocol specification.
You can set these variables.
- Specific to an NDMP host vendor.
You can set these variables.

To obtain up-to-date information on environment variables relating to particular NAS vendors, refer to [NetBackup for NDMP: NAS Appliance Information](#) from the Veritas Support website. The topic also contains configuration and troubleshooting help for particular NAS systems.

For Isilon filers only, note the following behaviors with environmental variables:

- With Isilon filers, if you set the `HIST` environment variable in a NetBackup NDMP backup policy with Accelerator enabled, you may specify only the value `D` (that is, `SET HIST=D`). `D` specifies a directory/node file history format. If you specify any other value for the `HIST` variable, NetBackup generates a message that asks you to change the value to `D`. If you do not use a `HIST` variable in the policy, the backup should complete successfully.
- If you change any of the variables in a NetBackup NDMP backup policy with Accelerator enabled, the Accelerator optimization will be 0% until you run a second full backup with the same variables. When the policy's variables change, a new baseline image is created with the first full backup. You will see Accelerator optimization only after the second full backup with the same variables.
- Reserved for use by NetBackup:
 - `FILESYSTEM`
 - `DIRECT`
 - `EXTRACT`
 - `ACL_START`

In NetBackup, environment variables can be set within the backup selections list by specifying one or more `SET` directives.

Note: In the backup selections list, the `SET` directive must be the first in the list, followed by the file systems or volumes to back up.

In general, the syntax of a `SET` directive is as follows:

```
SET variable = value
```

Where *variable* is the name of the environment variable and *value* is the value that is assigned to it. The value can be enclosed in single or double quotes, and must be enclosed in quotes if it contains a space character. For example:

```
SET ABC = 22
SET DEF = "hello there"
```

Setting a variable equal to no value removes any value that was set previously for that variable. For example:

```
SET ABC =
SET DEF =
```

Variables accumulate as the backup selections list is processed. For example, a backup selection may contain the following entries:

```
/vol/vol1  
SET HIST = N  
/vol/vol2  
SET DEF = 20  
SET SAMPLE = all  
/vol/vol3
```

In this example, directory `/vol/vol1` is backed up without any user-specified environment variables. The second directory (`/vol/vol2`) is backed up with the variable `HIST` set to `N`. The third directory (`/vol/vol3`) is backed up with all three of the environment variables set (`HIST = N`, `DEF = 20`, and `SAMPLE = all`).

Note: You cannot restore a single file if `HIST = N` is set. Only full volume restores are available when the `HIST` variable is set to `N`.

If an environment variable appears again later in the list, the value of this variable overrides the previous value of the variable.

The values that each backup uses are saved and provided to subsequent restores of the directory. The NDMP host may have some environment variables that are set internally and these are also saved for restores.

See [“About configuring NDMP-attached devices”](#) on page 36.

About appropriate host selection for NetApp cDOT backup policies

When configuring a backup policy to protect NetApp cDOT systems, use either the cluster-management LIF or the data LIF. Consider the following when using the cluster-management LIF as the backup policy client.

Advantages:

- Everything is cataloged under the cluster-management LIF.
- You only have to validate the cluster-management LIF.
- It is easier to back up everything using a few policies.

Disadvantages:

- If the cluster is in use by multiple departments in the same organization, it may be difficult to isolate the data between divisions. This may also be a security concern for some organizations if they want to share data between divisions.
- There is a limited granularity in the choice of volume pools and destination storage.
- Finding the appropriate data may be more difficult at the time of restore.

Consider the following when using the data LIF as the backup policy client.

Advantages:

- Everything is cataloged under the data LIF.
- If the cluster is in use by multiple departments in the same organization, it is very easy to isolate data between divisions.
- Data from different divisions can go to different volume pools and destination storage.
- Finding the appropriate data is easier at the time of restore.

Disadvantages:

- You need to add credentials for each data LIF.
- You need multiple policies to backup up the entire cluster.

About backup types in a schedule for an NDMP policy

You can specify any of the following backup types in a schedule for an NDMP policy:

- Full
- Cumulative Incremental
- Differential Incremental

Specify **Override policy storage unit** only if the client of NetBackup (the NDMP host) has more than one storage unit and you want to use a specific storage unit for this schedule. In this case, the client must be the only client in this NDMP policy.

See [“About configuring NDMP-attached devices”](#) on page 36.

About enabling or disabling DAR

By default, NetBackup for NDMP is configured to use Direct Access Recovery (DAR) to restore files or directories. DAR is used somewhat differently for file restore than for directory restore.

The following table describes how DAR is used for file and directory restores.

Table 3-2 How DAR is used for file and directory restores

Type of restore	Description
File restore	For each restore of files (not of directories), NetBackup automatically determines if the use of DAR speeds up the restore. NetBackup uses DAR only when it results in a faster restore.
Directory restore	For restore of directories, by default DAR is always used to restore a subdirectory but never used to restore the directory containing an entire image. For example, if <code>/vol/vol0</code> contains the entire image, and <code>/vol/vol0/dir1</code> is a subdirectory, DAR is used by default to restore <code>/vol/vol0/dir1</code>. But it is not used to restore <code>/vol/vol0</code>. For restore of subdirectories, NetBackup does not attempt to gauge the effectiveness of using DAR. Unless DAR is manually disabled, NetBackup always uses DAR to restore subdirectories. See “Disabling DAR for file and directory restores” on page 62.

Note: You may have to disable DAR if you have problems with DAR and your NDMP host is an older computer or is not running the latest NAS OS version.

See [“About configuring NDMP-attached devices”](#) on page 36.

Disabling DAR for file and directory restores

This procedure disables DAR for both file and directory restores, for all NDMP policies.

To disable DAR

- 1 In the **NetBackup Administration Console**, expand **Host Properties** and click **Master Servers** or **Media Servers**.
- 2 Right-click the name of the server and select **Properties**.
- 3 Click **General Server**.
- 4 Uncheck the **Use direct access recovery for NDMP restores** box and click **Apply**.

This action disables DAR on all NDMP restores.

- 5 Click **OK**.

See [“About configuring NDMP-attached devices”](#) on page 36.

Disabling DAR for directory restores only

This procedure disables DAR for directory restores only. It leaves DAR enabled for individual file restores.

To disable DAR on restores of directories only, for all NDMP policies

- 1 Enter the string NDMP_DAR_DIRECTORY_DISABLED in the following file:

```
/usr/opensv/netbackup/db/config/ndmp.cfg
```

- 2 To turn on directory DAR, remove (or comment out) the NDMP_DAR_DIRECTORY_DISABLED string from the `ndmp.cfg` file.

See [“About configuring NDMP-attached devices”](#) on page 36.

Configuring NetBackup for NDMP in a clustered environment

The following must be installed on each node of the cluster before you can configure NetBackup for NDMP in a clustered environment:

- The NetBackup server
See the [NetBackup Installation Guide](#).
- NetBackup for NDMP software.
See [“NetBackup for NDMP installation prerequisites”](#) on page 30.
For Windows servers, only the NetBackup for NDMP license has to be installed.

To configure NetBackup for NDMP in a clustered environment

- 1 Configure NDMP-attached robots and drives. Then configure storage units and policies as in a normal, non-clustered environment:
 - You can use the NetBackup **Device Configuration Wizard**, or configure the devices manually.
See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 37.
 - To use the same robotic libraries throughout a cluster, the robot numbers must be consistent. The **Device Configuration Wizard** attempts to ensure this configuration. If you configure robots manually, be sure to use the same robot number for a given robot, from one host to another in the cluster.
- 2 When you finish configuring devices and policies for NetBackup for NDMP, failover to the next node in the cluster and configure the drives and robots.

Select the same robot number that you used when configuring the robot for the first node.

After NetBackup is configured in a clustered environment, most configuration information is available to all nodes in the cluster. The information is available by means of a shared hard drive. However, in the **NetBackup Administration Console**, if you make changes to **NetBackup Management > Host Properties**, they are not available on the shared drive. Such changes apply only to the active node. You must manually duplicate on each node the changes to **Host Properties** that are made on the active node. This action lets NetBackup perform exactly the same way in case of failover to another node.

Refer to the [NetBackup High Availability Guide](#) for further assistance.

See [“About configuring NDMP-attached devices”](#) on page 36.

Configuring NDMP backup to NetBackup media servers (remote NDMP)

This chapter includes the following topics:

- [About remote NDMP](#)
- [Configuring NDMP backup to Media Manager storage units](#)

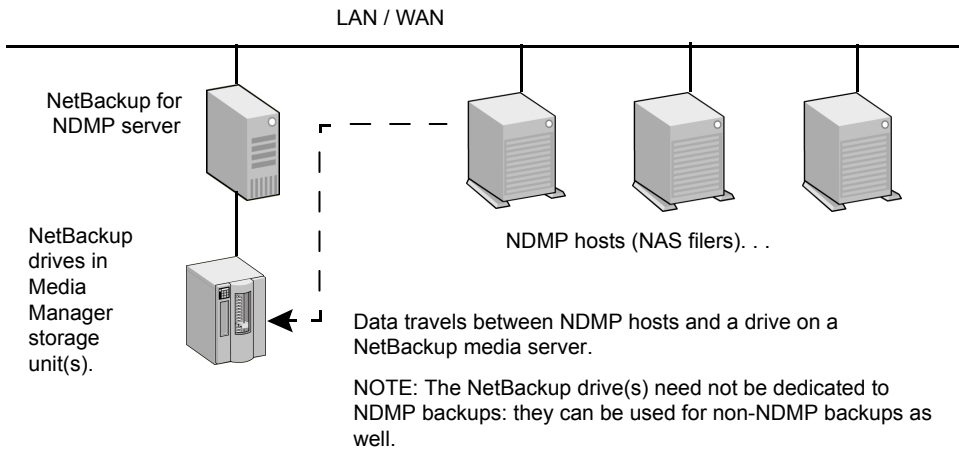
About remote NDMP

This topic describes how to configure NetBackup for NDMP to make backups to Media Manager storage units (remote NDMP). Only NDMP-specific steps are described.

Using remote NDMP, you can back up NDMP data to a configured drive in a Media Manager storage unit on a NetBackup media server. The drive can be used for both NDMP backups and for non-NDMP backups.

An added feature to remote NDMP is NDMP multiplexing. NDMP multiplexing works with remote NDMP. It concurrently writes multiple backup streams to the same storage device from the same client or different clients.

Figure 4-1 NDMP backup to a Media Manager storage unit



Configuring NDMP backup to Media Manager storage units

This section describes how to configure NDMP backups to Media Manager storage units.

To configure NDMP backups to Media Manager storage units

- 1 Authorize the NetBackup server to access the NDMP hosts you want to back up.
 Perform the following steps on the primary server (not media server) if you plan to create snapshots using the Snapshot Client NAS_Snapshot method:
 - Under **Media and Device Management > Credentials**, click **NDMP Hosts**. From the **Actions** menu, choose **New > New NDMP Host** to display the **Add NDMP Host** dialog.
 - Fill in the values.
 See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 37.
 - Repeat these steps for each NDMP host that the NetBackup server backs up.
- 2 Use the NetBackup **Device Configuration Wizard** to configure the drive(s) and robot(s).

Note the following:

- Do not use the "Configuring NDMP backup to NDMP-attached devices" topic in this guide. Configure the robots and drives as ordinary NetBackup devices, not as NDMP-attached devices.
See the [NetBackup Administrator's Guide, Volume I](#).
 - Drives can be shared using the NetBackup Shared Storage Option (SSO). The drives can be shared as both NDMP drives and non-NDMP drives.
See "[About the Shared Storage Option \(SSO\) with NetBackup for NDMP](#)" on page 90.
- 3** Create a Media Manager storage unit for the drive(s). The storage unit type must be Media Manager, not NDMP.
- For NDMP multiplexing, do the following steps:
- Select the **Enable Multiplexing** check box on the **New Storage Unit** menu.
 - Set the **Maximum streams per drive** entry to a value greater than one.
- For details on storage units, refer to the [NetBackup Administrator's Guide, Volume I](#).
- 4** Create an NDMP-type policy. On the **New/Change Policy** display, be sure to specify the storage unit that was created in the previous step.
- Note the following for NDMP multiplexing:
- Set the **Media multiplexing** attribute on the **Add New Schedule** menu to a value greater than one.

Configuring NDMP DirectCopy

This chapter includes the following topics:

- [About NDMP DirectCopy](#)
- [Configuring NDMP DirectCopy](#)
- [Using NDMP DirectCopy to duplicate a backup image](#)

About NDMP DirectCopy

NetBackup supports virtual tape libraries (VTLs). A virtual tape library uses disk-based technology to emulate a tape library (robot) and drives. The backup image is written to one or more disks in the VTL. The VTL allows the image to be treated as though it resides on tape, but with the access speed of a disk.

For additional storage (such as for disaster recovery), NetBackup copies backup images from the VTL disk to a physical tape in an NDMP storage unit. It copies without using media server I/O or network bandwidth. NetBackup can also copy NDMP images directly between NDMP tape drives attached to an NDMP host.

In both cases, this function is called NDMP DirectCopy. This function also enables NetBackup to restore data directly from either the image in the VTL or from the physical NDMP tape. NDMP DirectCopy supports backup to tape and restore from tape for NDMP data as well as non-NDMP data. Tape-to-tape duplications of backup images are also supported.

NDMP DirectCopy does not support multiplexed backup, synthetic backup, or multiple copies. It also does not support storage unit groups for the destination device. If you select a storage unit group, NDMP DirectCopy is disabled. The data transfer takes place over the network by means of the NetBackup server.

To initiate the NDMP DirectCopy, you can use the NetBackup duplication feature in the **NetBackup Administration Console**, the `bpduplicate` command, or NetBackup Vault.

NDMP DirectCopy operates in the following environments:

- A NetBackup media server that is connected to a VTL that has access to a physical tape library. The steps for configuring NDMP DirectCopy are described in this topic.
- A NetBackup for the NDMP server that is connected to an NDMP host that has access to a tape library (no VTL). This NDMP backup environment is described in other topics of this guide. In this environment, no additional configuration is required for NDMP DirectCopy.

If your NDMP host and storage devices are correctly configured, NetBackup uses NDMP DirectCopy when you duplicate an NDMP backup that NetBackup had created.

Prerequisites for using NDMP DirectCopy

Note the following prerequisites for using NDMP DirectCopy:

- NetBackup for NDMP software must be installed. NetBackup for NDMP is enabled by the Enterprise Disk Option license. It requires the NDMP protocol version V4 or higher.
- The [NetBackup Compatibility List for all Versions](#) indicates which VTL software supports this functionality.
- If your environment includes a VTL, the VTL must be installed and set up according to the vendor's instructions. The NetBackup Enterprise Disk Option license(s) are required. The Enterprise Disk Option license enables NDMP DirectCopy functionality.
- The VTL must have the NDMP capabilities needed to support NDMP DirectCopy.
- To make direct copies from one NDMP tape drive to another (no VTL), the NetBackup for NDMP license is required.

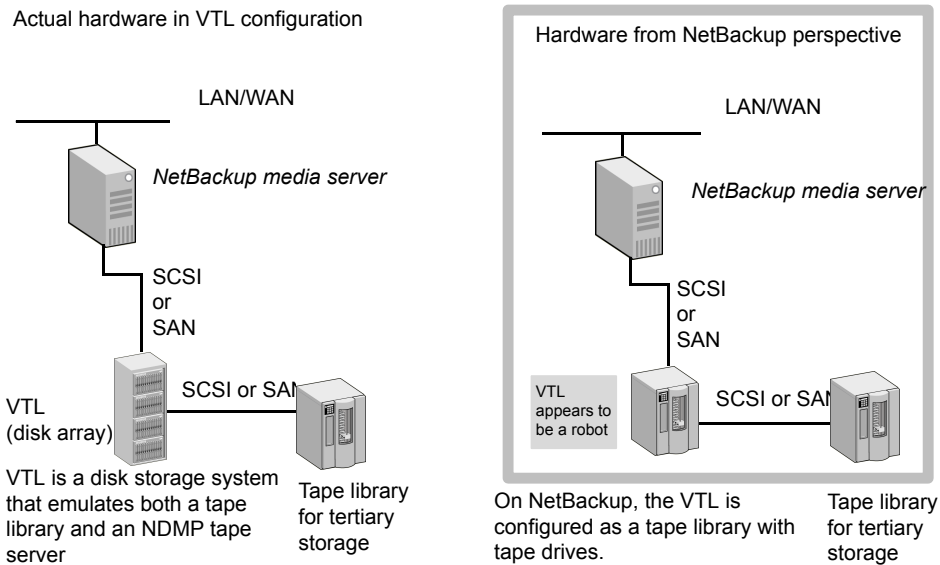
NDMP DirectCopy with VTL

The NDMP DirectCopy feature uses a VTL that has an embedded NDMP tape server using the NDMP protocol. The embedded NDMP tape server moves the image from the VTL disk directly to a physical tape. The image does not pass through the NetBackup media server or travel over the network.

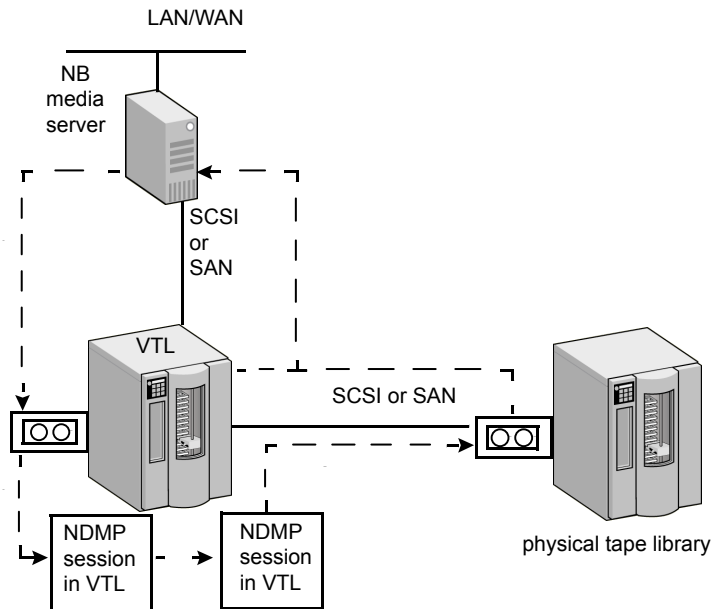
Note: In a VTL environment, a NAS appliance is not required. The VTL emulates a NAS (NDMP) host. The VTL requires NDMP tape server functionality.

The following figure represents a VTL from two perspectives. It shows the actual hardware present in a VTL configuration and the configuration from the perspective of NetBackup.

Figure 5-1 Overview of NDMP DirectCopy with VTL



The following figure shows the data flow and control for a VTL.

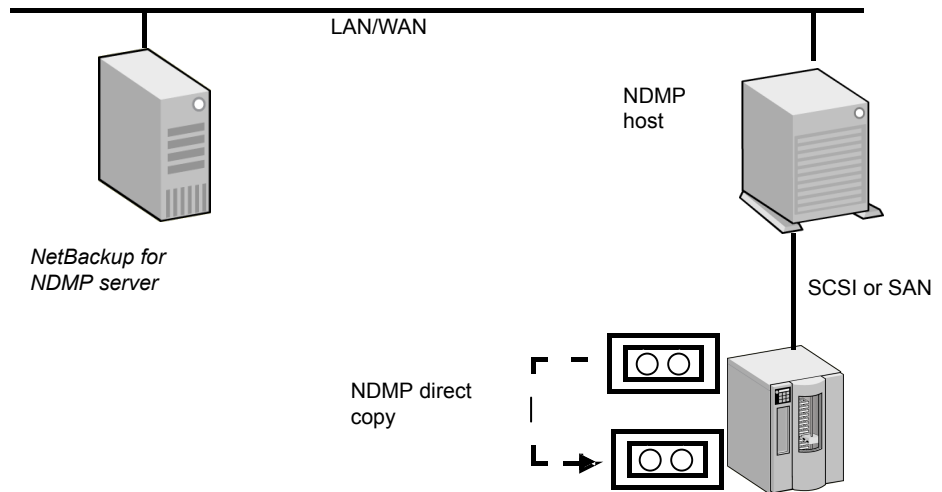
Figure 5-2 NDMP DirectCopy with VTL data flow and control

1. NetBackup media server sends the backup over a direct device path (SCSI or SAN) to the VTL.
2. NetBackup selects an NDMP device path to the VTL and creates an NDMP control session for the device.
3. NetBackup selects a tape volume from the physical tape library. It then selects an NDMP device path from the library and creates a second NDMP control session for the device.
4. By means of the NDMP protocol, the backup image in the VTL is copied directly to the physical tape library (not sent over the network).
5. The image can be restored directly to the media server from either the VTL or the physical tape.

NDMP DirectCopy without VTL

By means of the NetBackup duplication feature, NetBackup can copy NDMP images between tape drives attached to an NDMP host. A typical usage is to copy images between tape drives within the same tape library. (Images can also be copied between tape libraries.) Like NDMP DirectCopy with a VTL, the copied data does not pass through the NetBackup media server or travel over the network.

Figure 5-3 NDMP DirectCopy between tape drives accessible to an NDMP host



Configuring NDMP DirectCopy

Use the following procedure to configure NDMP DirectCopy from the backups that were made to a VTL.

To configure NDMP DirectCopy from the backups that were made to a VTL

- 1 Configure the VTL as an NDMP host. You can use the NetBackup **Device Configuration Wizard**, as follows. In the **NetBackup Administration Console**, click **Media and Device Management** and, in the right panel, click **Configure Storage Devices**.
 - In the **Device Hosts** dialog box of the wizard, choose the device host, then click **Change**.
 - In the **Change Device Host** dialog box, select **NDMP server** and click **OK**.
 - Click **Next**. The VTL appears in the **NDMP Host** window of the **NDMP Hosts** dialog box.
See ["Using the NetBackup Device Configuration Wizard for NDMP hosts"](#) on page 92.
- 2 Authorize NetBackup access to the VTL. Note that the VTL emulates an NDMP host.
See ["Authorizing NetBackup access to a NAS \(NDMP\) host"](#) on page 37.

- 3 Configure the VTL as a robot, then configure one or more tape drives in a Media Manager storage unit.

You can use the NetBackup **Device Configuration Wizard**. Additional help configuring devices and Media Manager storage units is also available.

See the [NetBackup Administrator's Guide Volume I](#).

- 4 Configure one or more tape drives in the VTL as Network Attached Storage devices, and create one or more NDMP storage units for the drives.

See ["Adding a tape drive"](#) on page 42.

See ["Adding NDMP storage units"](#) on page 48.

The drives can be the same as those that were selected in the previous step. NetBackup supports sharing of drives among media servers and NDMP hosts.

- 5 Configure one or more NDMP tape drives in the physical tape library, and add the drives to NDMP storage units. Use the same procedures as those mentioned in the previous step.

You can also use these drives in Media Manager storage units, if they are shared on a SAN.

Using NDMP DirectCopy to duplicate a backup image

NetBackup uses NDMP DirectCopy when you duplicate a backup image. To run a duplication, you can use any of the following methods:

- Initiate the duplication from the **NetBackup Administration Console**.
In the **NetBackup Administration Console**, select **NetBackup Management > Catalog** and then, in the right pane, in the **Action** list box select the **Duplicate** action.
See ["Initiating NDMP DirectCopy with the NetBackup Administration Console"](#) on page 74.
- NetBackup Vault
Refer to the [NetBackup Vault Administrator's Guide](#) for more information.
- The `bpduplicate` command
Refer to the [NetBackup Commands Guide](#) for detailed information about this command.
- A storage lifecycle policy (SLP)
In the **NetBackup Administration Console**, select **NetBackup Management > Storage > Storage Lifecycle Policies**.

Refer to the [NetBackup Administrator's Guide, Volume I](#) for more information about SLPs.

If you use a NetApp cDOT system in SVM-scoped NDMP mode, NetBackup tries to match the affinity for the source and the destination tape drive path, if possible, so the duplication can be performed optimally.

Requirements to use NDMP DirectCopy for image duplication

When NetBackup uses NDMP DirectCopy to duplicate an image, note the following:

- For the destination for the duplication, you must designate an NDMP storage unit in a VTL or in a physical tape library.
- An NDMP tape drive must be available to mount the source image. The NDMP tape drive can be one that was defined in the VTL, or it can be a physical tape drive in a tape library.

Setup instructions are available.

See [“About NDMP DirectCopy”](#) on page 68.

If these two requirements are met, NDMP DirectCopy is enabled. NetBackup copies the image directly to the designated storage unit without using media server I/O or network bandwidth.

NetBackup policy type for image duplication

You can duplicate an image that any NetBackup policy created. The policy need not be an NDMP policy.

See [“About NDMP DirectCopy”](#) on page 68.

The backup can be made to a storage unit in the VTL or to a storage device that is attached to an NDMP host. You can then copy the backup directly to a tape drive using the NetBackup Duplicate feature, as follows.

Initiating NDMP DirectCopy with the NetBackup Administration Console

Use the following procedure to initiate NDMP DirectCopy.

To initiate NDMP DirectCopy

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Catalog**.
- 2 Set up the search criteria for the image that you want to duplicate. Click **Search Now**.
- 3 Right-click the images you want to duplicate and select **Duplicate** from the shortcut menu.

You must designate an NDMP storage unit as the destination for the duplication. Use the **Storage unit** field in the **Setup Duplication Variables** dialog box.

See *Duplicating backup images* in the [NetBackup Administrator's Guide, Volume I](#).

Accelerator for NDMP

This chapter includes the following topics:

- [About NetBackup Accelerator for NDMP](#)
- [About the track log for Accelerator for NDMP](#)
- [Accelerator messages in the NDMP backup job details log](#)
- [NetBackup logs for Accelerator for NDMP](#)

About NetBackup Accelerator for NDMP

Note: Currently only NetApp filers and Isilon filers are supported with the NetBackup Accelerator for NDMP option. (See the [NetBackup Compatibility List for all Versions](#) for the most recent list of supported versions of each NAS vendor.)

For NetApp filers, Accelerator for NDMP supports only the DUMP format. Consult your NetApp documentation for specific details about its DUMP format.

NetBackup's Accelerator option makes NDMP backups for NetApp and Isilon filers run faster than normal NDMP backups. NetBackup Accelerator increases the speed of full backups by using the filer's change detection techniques to identify the modifications that occurred since the last backup. After an initial full backup that protects all data from the filer, NetBackup Accelerator backs up only the changed data from the filer to the media server. The media server combines the changed data with any previous backup images to create a new full backup image; if a file or portion of a file is already in storage and has not been changed, the media server uses the copy in storage rather than reading it from the filer to complete the backup image. The end result is a faster NetBackup NDMP backup.

Note: For NetApp filers, you can expect to see Accelerator optimization in both full backups (regular and forced rescan) and incremental backups. For Isilon filers, you can expect to see Accelerator optimization only in full backups (regular – not forced rescan).

Accelerator for NDMP has the following advantages:

- Supports all NetBackup NDMP features, such as replication, DAR restores, and multiplexing.
- Creates a compact backup stream that uses less network bandwidth between the filer and NetBackup servers.
- Reduces the I/O and CPU overhead on the media server.

To configure Accelerator for NDMP, select the **Use Accelerator** check box that is found on the NDMP policy **Attributes** tab. No change to the filer is required.

Note: For Isilon filers only, note the following behaviors with environmental variables:

With Isilon filers, if you set the `HIST` environment variable in a NetBackup NDMP backup policy with Accelerator enabled, you may specify only the value `D` (that is, `SET HIST=D`). `D` specifies a directory/node file history format. If you specify any other value for the `HIST` variable, NetBackup generates a message that asks you to change the value to `D`. If you do not use a `HIST` variable in the policy, the backup should complete successfully.

If you change any of the variables in a NetBackup NDMP backup policy with Accelerator enabled, the Accelerator optimization will be 0% until you run a second full backup with the same variables. When the policy's variables change, a new baseline image is created with the first full backup. You will see Accelerator optimization only after the second full backup with the same variables.

More information about environmental variables in NDMP policies is available:

See [“About environment variables in the backup selections list”](#) on page 58.

Note: If you include the `smtape` environment variable for NetApp filers in an NDMP backup policy, no optimization is seen with Accelerator for NDMP enabled. The `smtape` environment variable always backs up an entire volume as if it is a full backup of a single file. Consult your NetApp filer documentation for specific details about `smtape`. More information about `smtape` in a NetBackup backup policy is available in the NetApp section of [NetBackup for NDMP NAS Appliance Information](#).

If your NDMP policies include combinations of filers from NetApp, Isilon, and filers from other vendors, only the NetApp and Isilon filers use the Accelerator option. Messages in the job details identify which filers use the Accelerator option and when the option is used. More information about these job detail messages is available:

See [“Accelerator messages in the NDMP backup job details log”](#) on page 82.

Note: Unlike non-accelerated NDMP backups, accelerated NDMP backups do not use NDMP dump levels 0-9 to determine changed files. Instead, `BASE_DATE` and `DUMP_DATE` are used to determine changed files. `BASE_DATE` provides the timestamp of the most recent full or incremental backup. `DUMP_DATE` provides the timestamp of the currently running backup. Only the data that has changed between the `BASE_DATE` and the `DUMP_DATE` is backed up when Accelerator for NDMP is enabled.

Dump level messages from the filer continue to be included in the job detail log. However, the message `please ignore references to LEVEL in future messages` also appears in the job details as a reminder that dump levels are not used with Accelerator for NDMP.

How Accelerator works with NDMP backups:

- **First full backup with Accelerator**
The first full NDMP backup job with the Accelerator option enabled is similar to a normal full backup. It may run slightly longer than a non-Accelerator backup. It backs up all of the data from the filer, provides a baseline backup image, and creates an initial track log.

Note: If you first enable Accelerator when the next scheduled backup is an incremental backup, NetBackup does not automatically trigger a full backup image, as is the case with NetBackup Accelerator for non-NDMP policies. With Accelerator for NDMP, incremental backups continue to run as scheduled. An initial track log is also created after the **Use Accelerator** option is enabled, and with NetApp filers, you should see faster incremental backups. The next full backup runs only when it is scheduled.

- **Incremental backups with Accelerator**
Subsequent incremental backup jobs back up only the data that changed since the last backup job.
- **Next full backups with Accelerator**

Subsequent full backup jobs back up only the data that changed since the last backup job. The track log is used to determine what data can be included from previous backups, including the previous full backup and all of the incremental backups that follow it. NetBackup then creates a full backup image that includes all of the filer's data.

- Forced rescan full backups with Accelerator
The **Accelerator forced rescan** option provides a safety net by establishing a new baseline for the next Accelerator backup. When you include this option, which is found on the policy's **Schedules** tab, all the data on the filer is backed up. This backup is similar to the first full backup with Accelerator; it provides a new baseline for the backups that follow. If you set up a weekly full backup schedule with the **Use Accelerator** option, you can supplement the policy with another schedule that enables **Accelerator forced rescan**. You can set the schedule to run every 6 months or whenever it is appropriate for your environment. With NetApp filers, expect backups with **Accelerator forced rescan** to run slightly longer than accelerated full backups. With Isilon filers, backups with **Accelerator forced rescan** may run as long as a first full backup with Accelerator. More information about these options is available:
 - See [“Attributes tab options for an NDMP policy”](#) on page 50.
 - See [“Schedules tab options for an NDMP policy with Accelerator for NDMP enabled”](#) on page 51.

About the track log for Accelerator for NDMP

The track log is a binary file that you should not attempt to edit. On occasion, Veritas Technical Support may request the track log for troubleshooting purposes. Two copies of the track log exist in the following locations:

- Primary server:
UNIX: `/usr/openv/netbackup/db/track`
Windows: `install_path\NetBackup\db\track`
- Media server:
UNIX: `/usr/openv/netbackup/track`
Windows: `install_path\NetBackup\track`

You can manually delete track logs safely if any of the follow situations occur:

- You disable the **Use Accelerator** option.
- The backup selections are changed.
- The policy is renamed.

- The NDMP filer is removed from the policy.
- The storage server that is used to perform the backup is changed.
- The primary server that is used to control the backups is changed.

Navigate to the following locations to manually delete track logs for specific backup selections:

- Primary server:

UNIX:

```
/usr/opensv/netbackup/db/track/primary_server/storage_server/filer_name/  
policy/backup_selection
```

Windows:

```
install_path\NetBackup\db\track\primary_server\storage_server\filer_name\  
policy\backup_selection
```

- Media server:

UNIX:

```
/usr/opensv/netbackup/track/primary_server/storage_server/filer_name/  
policy/backup_selection
```

Windows:

```
install_path\NetBackup\track\primary_server\storage_server\filer_name\  
policy\backup_selection
```

How to redirect track logs for Accelerator for NDMP

Track log size is relative to the size and number of files in a backup. In some cases, you may need to relocate the track logs to a different volume because of space issues. In these cases, it is recommended that you "redirect" the track logs to a volume where there is sufficient disk space.

One copy of the track log exists on the primary server and another copy exists on a media server in the following directories:

- Primary server:

UNIX: `/usr/opensv/netbackup/db/track`

Windows: `install_path\NetBackup\db\track`

- Media server:

UNIX: `/usr/opensv/netbackup/track`

Windows: `install_path\NetBackup\track`

To redirect these directories, complete the appropriate procedures in this topic. After completion, the next Accelerator-enabled backup that is executed redirects the track logs it creates to the directory you specified.

To redirect the track log directories on UNIX systems:

1 Rename the track log directories to make backup copies:

- On the primary server:

```
# mv /usr/opensv/netbackup/db/track  
/usr/opensv/netbackup/db/track.sv
```

- On the media server:

```
# mv /usr/opensv/netbackup/track /usr/opensv/netbackup/track.sv
```

2 Copy the backup to a new location:

- On the primary server:

```
# cp -rp /usr/opensv/netbackup/db/track.sv/* <path to new  
destination directory for track logs>
```

- On the media server:

```
# cp -rp /usr/opensv/netbackup/track.sv/* <path to new  
destination directory for track logs>
```

3 Create symbolic links from track log directories to the desired locations. For example, if the desired directory is /voll/track, enter the following command:

- On the primary server:

```
# ln -s /voll/track /usr/opensv/netbackup/db/track
```

- On the media server:

```
# ln -s /voll/track /usr/opensv/netbackup/track
```

4 After you have verified that everything works properly, you can remove the backup track.sv directory to free up space on the original volume.

To redirect the track log directories on systems with Windows Server:

1 Rename the track log directories to make backup copies:

- On the primary server:

```
> move "install_path\NetBackup\db\track"  
"install_path\NetBackup\db\track.sv"
```

- On the media server:

```
> move "install_path\NetBackup\track"  
"install_path\NetBackup\track.sv"
```

2 Copy the backup to a new location:

- On the primary server:

```
> xcopy /e "install_path\NetBackup\db\track.sv" "<path to new destination directory for track logs>"
```
- On the media server:

```
> xcopy /e "install_path\NetBackup\track.sv" "<path to new destination directory for track logs>"
```
- 3 Before performing an Accelerator-enabled backup, use `mklink` to link the `<install_dir>\NetBackup\track` directory to the desired directory. For example, if the desired directory is `E:\track`, enter the following command:

```
> mklink /D "<install_dir>\NetBackup\track" E:\track
```
- 4 After you have verified that everything works properly, you can remove the backup `track.sv` directory to free up space on the original volume.

More information about Accelerator for NDMP is available:

See [“About NetBackup Accelerator for NDMP”](#) on page 76.

See [“About the track log for Accelerator for NDMP”](#) on page 79.

Accelerator messages in the NDMP backup job details log

This topic provides explanations of some specific messages that appear in an NDMP job details log when Accelerator for NDMP is enabled.

The messages in the NetBackup job details include messages that are generated directly from the filer. To find the messages from the filer, look for the NDMP host name in the message following the PID number as in the following example:

```
mm/dd/yyyy hh:mm:ss - Info ndmpagent (pid=10780) [NDMP_host_name]:  
Filetransfer: Transferred 146841088 bytes in 2.855 seconds  
throughput of 50231.929 KB/s
```

Note: Some messages that are generated directly from the filer, such as `filer volume is full`, may require your immediate attention. Consult the documentation for the filer to determine how to resolve any issues with the filer that are indicated by a message from the filer in the job details.

First Accelerator-enabled full backup

Messages similar to the following appear in the job details log for the first full NDMP backup that uses Accelerator for NDMP.

```
mm/dd/yyyy 1:28:47 PM - Info bpbrm(pid=3824) accelerator enabled
...
mm/dd/yyyy 1:28:53 PM - Info ndmpagent(pid=10556) accelerator
optimization is <off>, unable to locate accelerator tracklog
...
mm/dd/yyyy 1:29:05 PM - Info ndmpagent(pid=10556) accelerator sent
1310720 bytes out of 1310720 bytes to server, optimization 0.0%
```

Note the following items about messages for the first Accelerator-enabled full backup:

- `accelerator enabled`
This message indicates that the Accelerator option is being used.
- `accelerator optimization is <off>, unable to locate accelerator tracklog`
Because this is the first full backup, NetBackup creates a new track log. More information about the locations of the track log is available:
See [“NetBackup logs for Accelerator for NDMP”](#) on page 85.
- `accelerator sent 1310720 bytes out of 1310720 bytes to server, optimization 0.0%`
Because this is the first full backup, all data is backed up and no optimization occurs yet.

Subsequent Accelerator-enabled incremental backup

Messages similar to the following appear in the job details log for subsequent incremental NDMP backups that use Accelerator for NDMP.

```
mm/dd/yyyy 2:01:58 PM - Info ndmpagent(pid=8652) accelerator
optimization is <on>
mm/dd/yyyy 2:01:58 PM - Info ndmpagent(pid=8652) BASE_DATE will be
used to determine changed files for accelerator
mm/dd/yyyy 2:01:58 PM - Info ndmpagent(pid=8652) please ignore
references to LEVEL in future messages
...
mm/dd/yyyy 2:14:14 PM - Info ndmpagent(pid=10044) accelerator sent
1104896 bytes out of 100310720 bytes to server, optimization 15.7%
```

Note the following items about messages for the subsequent incremental accelerator backups:

- `accelerator optimization is <on>`

This message indicates that a track log exists and the backup shall perform with the Accelerator option.

- `BASE_DATE` will be used to determine changed files for accelerator and please ignore references to `LEVEL` in future messages

These messages are a reminder that Accelerator for NDMP uses `BASE_DATE` and `DUMP_DATE` rather than dump levels to identify changed data. Messages that refer to dump levels come from the filer. However, the message to ignore references to `LEVEL` also appears in the job detail logs as a reminder that dump levels are not used with Accelerator for NDMP.

- `accelerator sent 1104896 bytes out of 100310720 bytes to server, optimization 15.7%`

This message provides the amount of data that was sent to the server and the percentage of optimization that was realized.

Next Accelerator-enabled full backups

Messages similar to the following appear in the job details log for subsequent full NDMP backups that use Accelerator for NDMP.

```
mm/dd/yyyy 2:01:58 PM - Info ndmpagent(pid=8652) accelerator
optimization is <on>
mm/dd/yyyy 2:01:58 PM - Info ndmpagent(pid=8652) BASE_DATE will be
used to determine changed files for accelerator
mm/dd/yyyy 2:01:58 PM - Info ndmpagent(pid=8652) please ignore
references to LEVEL in future messages
...
...
mm/dd/yyyy 1:40:27 PM - Info ndmpagent(pid=12244) accelerator sent
887296 bytes out of 1159725056 bytes to server, optimization 99.9%
```

Note the following items about messages for the subsequent incremental accelerator backups:

- `accelerator optimization is <on>`
This message indicates that a track log exists and the backup shall perform with the Accelerator option.
- `BASE_DATE` will be used to determine changed files for accelerator and please ignore references to `LEVEL` in future messages

These messages are a reminder that Accelerator for NDMP uses `BASE_DATE` and `DUMP_DATE` rather than dump levels to identify changed data. Messages that refer to dump levels come from the filer. However, the message to ignore references to `LEVEL` also appears in the job detail logs as a reminder that dump levels are not used with Accelerator for NDMP.

- accelerator sent 887296 bytes out of 1159725056 bytes to server, optimization 99.9%
 This message provides the amount of data sent to the server and the percentage of optimization that was realized.

Accelerator-enabled forced rescan full backup

Messages similar to the following appear in the job details log for full NDMP backups that use Accelerator for NDMP with the **Accelerator forced rescan** option.

```
mm/dd/yyyy 2:13:43 PM - Info bpbrm(pid=8628) Accelerator enabled
backup with "Accelerator forced rescan", all data will be scanned and
processed.Backup time will be longer than a normal Accelerator enabled
backup.
...
...
mm/dd/yyyy 2:13:46 PM - Info ndmpagent(pid=10044) accelerator
optimization is <on> but 'forced rescan' is enabled
```

Note the following items about messages for accelerator forced rescan backups:

- Accelerator enabled backup with "Accelerator forced rescan", all data will be scanned and processed. Backup time will be longer than a normal Accelerator enabled backup **and** accelerator optimization is <on> but 'forced rescan' is enabled
 These messages indicate that a forced rescan is enabled and that the job shall run longer than a normal Accelerator full backup. Though accelerator optimization is on, the job may run slightly longer than accelerated full backups.

NetBackup logs for Accelerator for NDMP

Accelerator for NDMP does not require its own log directory. Instead, messages appear in standard NetBackup log files. [Table 6-1](#) lists the standard NetBackup log files in which messages for Accelerator for NDMP appear.

Table 6-1 NetBackup logs that may contain Accelerator for NDMP information

Log directory	Resides on
UNIX: /usr/opensv/netbackup/logs/ndmpagent Windows: install_path\NetBackup\logs\ndmpagent	NetBackup media server

Table 6-1 NetBackup logs that may contain Accelerator for NDMP information (*continued*)

Log directory	Resides on
UNIX: /usr/opensv/netbackup/logs/bpbrm Windows: <i>install_path</i> \NetBackup\logs\bpbrm	NetBackup media server
UNIX: /usr/opensv/netbackup/logs/bptm Windows: <i>install_path</i> \NetBackup\logs\bptm	NetBackup media server
UNIX: /usr/opensv/netbackup/logs/bpfis Windows: <i>install_path</i> \NetBackup\logs\bpfis	NetBackup media server
UNIX: /usr/opensv/netbackup/logs/bpcd Windows: <i>install_path</i> \NetBackup\logs\bpcd	NetBackup primary server
UNIX: /usr/opensv/netbackup/logs/bprd Windows: <i>install_path</i> \NetBackup\logs\bprd	NetBackup primary server
UNIX: /usr/opensv/netbackup/logs/bpdbm Windows: <i>install_path</i> \NetBackup\logs\bpdbm	NetBackup primary server

To create the log directories, run the following command on the NetBackup servers and backup host:

On Windows:

```
install_path\NetBackup\logs\mklogdir.bat
```

On UNIX/Linux:

```
/usr/opensv/netbackup/logs/mklogdir
```

Remote NDMP and disk devices

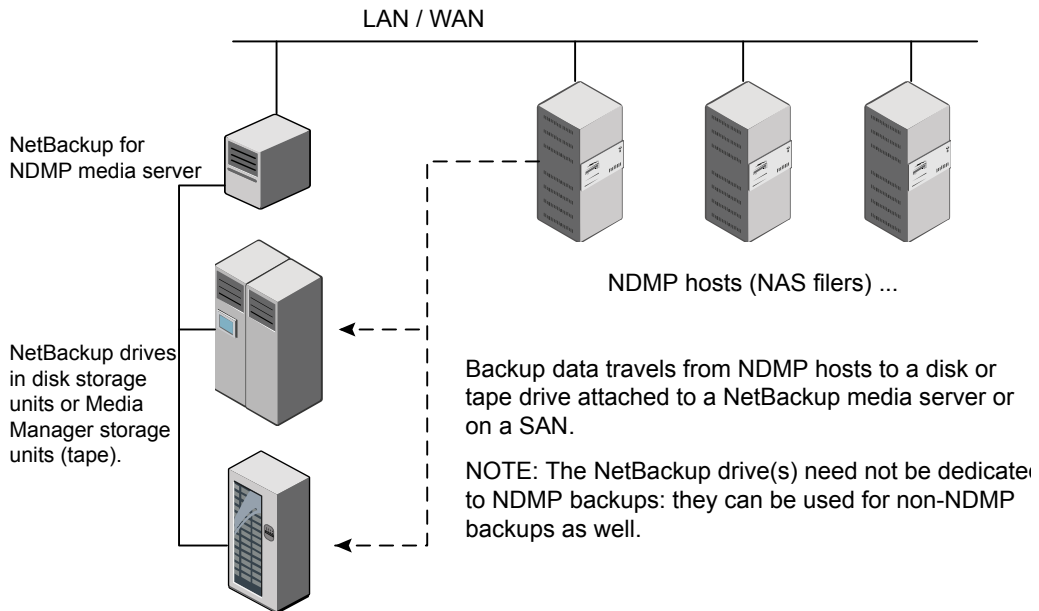
This chapter includes the following topics:

- [About remote NDMP and disk devices](#)
- [Configuring remote NDMP](#)

About remote NDMP and disk devices

This remote NDMP feature involves backing up NAS data (Network Attached Storage) to a storage device that is configured on a NetBackup media server. NetBackup supports disk devices on the media server.

The following figure shows the main components for NDMP backup to disk storage.

Figure 7-1 NDMP backup to a storage unit on media server (remote NDMP)

Configuring remote NDMP

Configure NetBackup to back up data to either disk storage or tape storage units that are attached to a NetBackup media server. Only NDMP-specific steps are described.

To configure NDMP backups to disk storage or tape storage units

- 1 Authorize the NetBackup server to access the NDMP hosts that you want to back up.

Do the following on the NetBackup media server:

- Expand **Media and Device Management > Credentials > NDMP Hosts**. Under the **Actions** menu, choose **New > New NDMP Host** to display the **Add NDMP Host** dialog box.
- Enter the name of the NDMP server (NAS filer) to back up. This NDMP host name is case-sensitive.

- Repeat the previous step for each NDMP host that the NetBackup server backs up.
 - If you plan to create snapshots using the Snapshot Client NAS_Snapshot method, do the previous step on the primary server (not on the media server).
- 2** Use the NetBackup **Device Configuration Wizard** to configure devices for remote NDMP (disks, or tape drives and robots, on the media server).

Note the following items:

- Do not use the device configuration procedure that is described for configuring NDMP-attached devices. Instead, configure the disk, robots, and drives the same way as the ordinary NetBackup devices are configured. See the [NetBackup Administrator's Guide, Volume I](#).
 - Tape drives can be shared using the Shared Storage Option (SSO) of NetBackup. The drives can be shared as both NDMP drives and non-NDMP drives. See ["About the Shared Storage Option \(SSO\) with NetBackup for NDMP"](#) on page 90.
- 3** Create a disk or Media Manager storage unit for the drive(s). The storage unit type must be Disk or Media Manager, not NDMP.
- For details on storage units, refer to the [NetBackup Administrator's Guide, Volume I](#).
- 4** Create an NDMP-type policy.
- See ["About creating an NDMP policy"](#) on page 50.

Using the Shared Storage Option (SSO)

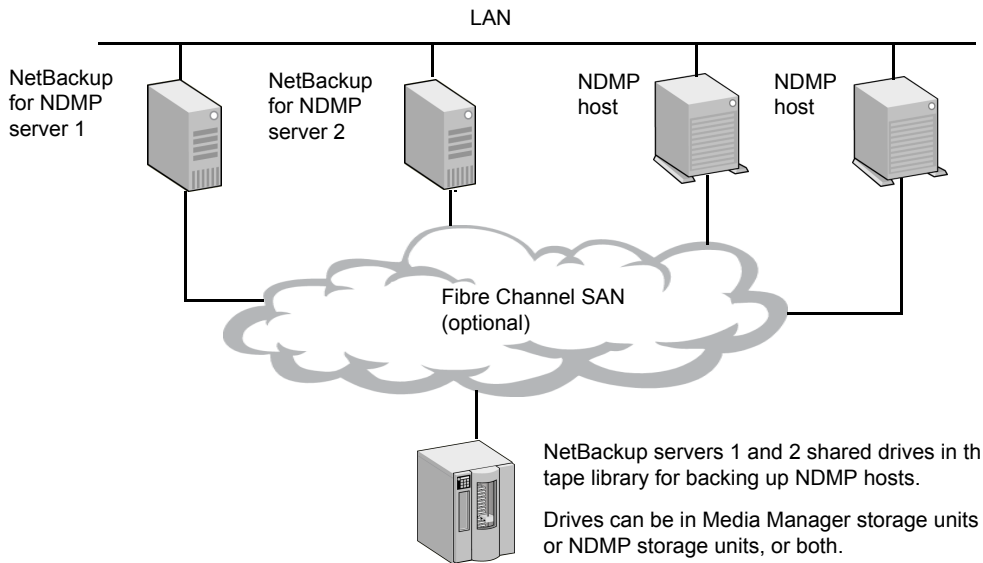
This chapter includes the following topics:

- [About the Shared Storage Option \(SSO\) with NetBackup for NDMP](#)
- [Setting up SSO with NetBackup for NDMP](#)
- [Using the NetBackup Device Configuration Wizard for NDMP hosts](#)

About the Shared Storage Option (SSO) with NetBackup for NDMP

The following figure shows a robotic library on a SAN that can share its drives between two NetBackup for NDMP servers and two NDMP hosts. Drive sharing requires a license for the Shared Storage Option. A SAN is not required.

Figure 8-1 NDMP backup using Shared Storage Option



For each robot, either a NetBackup media server or an NDMP server (not both) can handle robotic control.

Setting up SSO with NetBackup for NDMP

This topic describes the steps for setting up access to a drive that is shared between NDMP and NetBackup servers.

For a more complete discussion of SSO, refer to the [NetBackup Administrator's Guide, Volume II](#).

This procedure assumes that the following conditions are true:

- The prerequisites for SSO have been met, as described in the [NetBackup Administrator's Guide, Volume II](#).
- All physical devices, including the NDMP host, are correctly connected to the network.
- NetBackup for NDMP supports the NDMP host.
 For information about supported NDMP operating systems and NAS vendors, access *NetBackup for NDMP: NAS Appliance Information* from the Veritas Support website. The topic also contains configuration and troubleshooting help for particular NAS systems:

<http://www.veritas.com/docs/000027113>

The [NetBackup Compatibility List for all Versions](#) indicates which versions of vendor software support SSO for NDMP. The NAS systems (hardware) do not provide the support; the proper software version provides it. For a list of the features and software releases for each NAS vendor, for SSO support, and for the NetBackup versions that support these vendors, refer to the *NetBackup Compatibility List for all Versions*.

To set up an SSO with NetBackup for NDMP

- 1 Configure NetBackup access to the NDMP host.

See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 37.

- 2 Verify that the NDMP host can access the required robots and drives.

To verify NDMP host access to the required devices, run the following commands on a NetBackup media server that is authorized to access the host:

```
tpautoconf -verify ndmp_host_name
tpautoconf -probe ndmp_host_name
```

The `-verify` option verifies that the NetBackup server can access the NDMP host. The `-probe` option lists the devices that are visible to the NDMP host.

- 3 From the **NetBackup Administration Console**, use the **Device Configuration Wizard** to configure the devices and storage units.

See [“Using the NetBackup Device Configuration Wizard for NDMP hosts”](#) on page 92.

You must define an NDMP storage unit for each NDMP host that shares a drive. If all hosts have access to the shared drive(s), the **Device Configuration Wizard** can create these storage units automatically.

Using the NetBackup Device Configuration Wizard for NDMP hosts

The NetBackup **Device Configuration Wizard** provides the most convenient way to configure devices and storage units for NDMP hosts (with or without SSO).

To use the Device Configuration Wizard

- 1 In the **NetBackup Administration Console**, click **Configure Storage Devices** in the right panel to launch the **Device Configuration Wizard**.
- 2 Click **Next** on the **Welcome** window. The **Device Hosts** window appears.
- 3 Under **Device Hosts**, place a check beside the NetBackup media server that accesses the NDMP host.

- 4 Select the server name and then click **Change**.
- 5 In the **Change Device Host** window, place a check beside **NDMP server**.
- 6 Click **OK**.
- 7 In the **Device Hosts** window, NDMP is now listed in the **Optional Devices to be Scanned** column for the media server.
- 8 Click **Next** to continue.
- 9 In the **NDMP Hosts** window that shows the NDMP host(s) where you can configure devices, click **Next** to configure the NDMP-attached devices.
- 10 Follow the remaining prompts in the wizard to complete the configuration.

Backup and restore procedures

This chapter includes the following topics:

- [Performing a manual backup with an NDMP policy](#)
- [Perform an NDMP restore](#)

Performing a manual backup with an NDMP policy

The following procedures explain how the NetBackup administrator can perform the backup manually. Only a NetBackup administrator can initiate an NDMP backup. In the NetBackup web UI, a user must have the **Administrator** role.

Perform a manual backup of NDMP (NetBackup web UI)

To perform a manual backup of NDMP with the web UI

- 1 On the primary server, open the NetBackup web UI.
- 2 On the right, open **Protection > Policies**.
- 3 Locate and select the NDMP policy. Then click **Manual Backup**.
- 4 Select a schedule and then select the clients that you want to back up.

If you do not select any schedules, NetBackup uses the schedule with the highest retention level. If you do not select any clients, NetBackup backs up all configured NDMP hosts.

- 5 Click **OK** to start the backup.

Perform a manual backup of NDMP (NetBackup Administration Console)

To perform a manual backup of NDMP with the Administration Console

- 1 From the **NetBackup Administration Console**, click **Policies**.
- 2 Right-click the NDMP policy name and select **Manual Backup** from the pop-up menu.
- 3 Select a schedule and then select the clients (NDMP hosts) that you want to back up.

If you do not select any schedules, NetBackup uses the schedule with the highest retention level. If you do not select any clients, NetBackup backs up all configured NDMP hosts.

- 4 Click **OK** to start the backup.

Perform an NDMP restore

An administrator can perform a restore as follows:

- With the NetBackup web UI, from the primary server.
- With the **Backup, Archive, and Restore** interface from a NetBackup primary server or media server.

NetBackup administrators can restore files to the original NDMP host or to a different NDMP host.

Note: User-directed restores of files are not allowed, because no NetBackup client software is installed on an NDMP host.

Restore NDMP (NetBackup web UI)

To restore NDMP with the NetBackup web UI

- 1 On the primary server, open the NetBackup web UI.
- 2 On the left, select **Recovery**.
- 3 On the **Regular recovery** card, click **Start recovery**.

- 4 Select the following information and click **Next**.

Policy type	NDMP
Source client	Select the appropriate NDMP (NAS) host.
Destination client	Select the appropriate NDMP (NAS) host. The destination host must be an NDMP host that is compatible with the data format of the source. (The source and destination must be of the same NAS vendor type.)

- 5 NetBackup automatically displays the most recent backup. To select a different date range, click **Edit**.
- 6 Select the files or folders that you want to restore. Then click **Next**.
- 7 Select the recovery options that you want for the restore. Then click **Next**.

Warning: An NDMP restore always overwrites existing files.

Restore NDMP (Backup, Archive, and Restore interface)

To restore NDMP with the BAR interface

- 1 In the **Backup, Archive, and Restore** interface on a NetBackup server, click **Actions > Specify NetBackup Machines and Policy Type**.
- 2 For the server, select the NetBackup primary server.
- If your configuration has multiple primary servers, specify the primary server that has the policy for the NDMP host that you plan to restore. If the server name is not in the pull-down list, use **Edit Server List** to add it.
- 3 For the source clients and destination clients, select the appropriate NDMP (NAS) hosts.

The destination host must be an NDMP host compatible with the data format of the source. (The source and destination must be of the same NAS vendor type.)

Warning: An NDMP restore always overwrites existing files.

If the hosts that you want are not available in the pull-down menu, use **Edit Client List** to add the client.

- 4 In the policy type field, select **NDMP**.

Troubleshooting

This chapter includes the following topics:

- [About NetBackup for NDMP logs](#)
- [General NetBackup for NDMP operating notes and restrictions](#)
- [NetBackup for NDMP troubleshooting suggestions](#)
- [About robot tests](#)

About NetBackup for NDMP logs

NetBackup uses two types of logging, unified logging and legacy logging. Both logging types are described in the "Using Logs and Reports" topic in the [NetBackup Troubleshooting Guide](#).

Note the following:

- All unified logs are written to `/usr/opensv/logs` (UNIX) or `install_path\logs` (Windows). Unlike legacy logging, you do not need to create logging directories.
- Use the `vxlogview` command to examine unified logs:
See "[Viewing NetBackup for NDMP logs](#)" on page 97.
On UNIX: `/usr/opensv/netbackup/bin/vxlogview`
On Windows: `install_path\NetBackup\bin\vxlogview`
Refer to the [NetBackup Troubleshooting Guide](#) for assistance in using the `vxlogview` command.
See also the `vxlogview` man page or the [NetBackup Commands Guide](#).

Viewing NetBackup for NDMP logs

The following procedure describes how to view NetBackup logs.

Note: The legacy and unified logging files can consume a lot of disk space. Delete the log files when you are finished and set logging to a lower level of detail.

To view the NetBackup logs

- 1 In the **NetBackup Administration Console** in the left pane, expand **Host Properties > Media Servers**, and right-click on the server name in the right pane.
- 2 From the pop-up, select **Properties**, then click **Logging** and set the **Global logging level** to 5.

This increases logging detail to the highest level, for both unified logging and legacy logging.

Note: NDMP backup performance may in some cases be adversely affected when the logging level is set to 4 or 5. The performance effect may be serious enough to cause NDMP backup failures. Reduce the logging level to 3 or less if you encounter NDMP performance issues or backup failures.

- 3 Click **Apply** and then **OK**.
- 4 View the unified logging information in `/usr/opensv/logs` (UNIX) or `install_path\logs` (Windows) for the following processes:

`ndmpagent` (originator ID 134)

`ndmp` (originator ID 151)

`nbpem` (originator ID 116)

`nbjm` (originator ID 117)

`nbrb` (originator ID 118)

- 5 For `ndmpagent` logs, try the `vxlogview` command as follows:

```
/usr/opensv/netbackup/bin/vxlogview -I ndmpagent -d T,s,x,p
```

- 6** For ndmp logs, try the vxlogview command as follows:

```
/usr/opensv/netbackup/bin/vxlogview -I ndmp -d T,s,x,p
```

- 7** On the NetBackup for NDMP server, create bptm, and bpbrm legacy debug log folders in the /usr/opensv/netbackup/logs directory (UNIX) or install_path\NetBackup\logs folder (Windows):

```
bpbrm
```

```
bpfis
```

```
bpmount
```

```
bptm
```

```
bppfi
```

NetBackup writes legacy log files in these directories, if the directories exist.

NDMP backup levels

At the start of a debug log, you may see an entry titled `LEVEL`. This entry refers to an environment variable that NetBackup set based on the type of backup. Here is an example from a bptm log:

```
08:48:38.816 [22923] <2> write_data_ndmp: backup environment
values:
08:48:38.816 [22923] <2> write_data_ndmp: Environment 1:
TYPE=dump
08:48:38.816 [22923] <2> write_data_ndmp: Environment 2:
FILESYSTEM=/vol/vol0/2million
08:48:38.817 [22923] <2> write_data_ndmp: Environment 3:
PREFIX=/vol/vol0/2million
08:48:38.817 [22923] <2> write_data_ndmp: Environment 4: LEVEL=0
```

The NDMP backup level is modeled after UNIX dump levels. The backup level is a number in the range of 0 to 9.

An NDMP backup level of 0 is a full backup. A backup level greater than 0 is an incremental backup of all objects that were modified since the last backup of a lower level. For example, level 1 is a backup of all objects that were modified since the full backup (level 0). Level 3 is a backup of all objects that were modified since the last level 2 incremental.

Table 10-1 NetBackup backup types and corresponding NDMP backup levels

NetBackup backup types	NDMP backup levels
NetBackup Full	NDMP level 0
NetBackup Cumulative Incremental	NDMP level 1
NetBackup Differential Incremental	NDMP level (last level + 1, up to 9) Some vendors support level values that are greater than 9. For valid level values for your device, see the <i>NetBackup for NDMP: NAS Appliance Information</i> from the Veritas Support website: http://www.veritas.com/docs/000027113

More information is available on environment variables.

See “[About environment variables in the backup selections list](#)” on page 58.

General NetBackup for NDMP operating notes and restrictions

Before you try to troubleshoot a suspected problem, review the following operating notes:

- A tape that was created on an NDMP storage unit is in backup format. It cannot be restored from a non-NDMP storage unit. If you duplicate an NDMP backup image, the new copy is still in backup format. It cannot be used for restores on a non-NDMP storage unit.
- In the backup selections list for an NDMP policy, you can include only directory paths. Individual file names are not allowed. Wildcard characters are allowed in backup selections, though some limitations apply to some filers. More information about wildcards in NDMP backup selections is available:
See “[Wildcard characters in backup selections for an NDMP policy](#)” on page 53.
- In a NetBackup NDMP policy, you cannot include a path in the file list that is more than 1024 characters long. This limitation may be further restricted for certain vendors. See the [NetBackup NAS Appliance Information guide](#) for path name length information for specific filers.
- Observe the following restrictions to the use of the ALL_FILESYSTEM directive and the VOLUME_EXCLUDE_LIST directive:

- A `VOLUME_EXCLUDE_LIST` statement may include a maximum of 256 characters. Create multiple `VOLUME_EXCLUDE_LIST` statements if necessary to avoid exceeding the limit of 256 characters. If you specify more than 256 characters, the volume list is truncated. A truncated statement may result in a backup job failure, and the error message `Invalid command parameter(20)` is displayed. `VOLUME_EXCLUDE_LIST` applies only to `ALL_FILESYSTEMS`. It does not apply to explicit backup selections or wildcard-based backup selections.
- With NetBackup Replication Director, if the backup selection includes read-only volumes or full volumes, an NDMP backup job fails with the status code 20 (`Invalid command parameter(20)`). If you encounter a similar NDMP backup job error, review the `ostfi` logs to identify the volumes for which the failure occurred. You can use `VOLUME_EXCLUDE_LIST` statements with the `ALL_FILESYSTEMS` statement to exclude the read-only volumes and the volumes with insufficient space.

Note: This restriction applies only to NetBackup Replication Director environments.

More information about these directives is available:

See [“ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives”](#) on page 56.

- The NDMP protocol uses port 10000 for communication.
- On UNIX systems, the NetBackup `avrd` process uses Internet Control Message Protocol (ICMP) to ping NDMP hosts to verify network connectivity. This protocol is required for the NetBackup for NDMP product.
- If backup jobs or restore jobs are running slowly, verify that the network interface cards (NIC) are set to full duplex. Half-duplex often causes poor performance. For assistance viewing and resetting duplex mode for a particular NAS host, consult the documentation that the manufacturer provides. You may be able to use the `ifconfig` (or `ipconfig`) command, as explained in the [NetBackup Troubleshooting Guide](#).
- Do not perform incremental backups of the same NDMP data from two different policies. Incremental backups performed by one of the policies may be incomplete, because NDMP filers perform level-based incremental backups instead of time-based incremental backups. Consider the following example:

Policy A performs a full backup of `/vol/vol1` (level 0).

Policy B then performs a full backup of /vol/vol1 (level 0). The filer now considers the policy B backup to be the last full (level 0) backup of /vol/vol1.

Policy A performs an incremental backup of /vol/vol1 (level 1). The policy A incremental backup captures only the data that changed since the full backup that was done by policy B. The incremental backup misses any changes that occurred between the policy A full backup and the policy B full backup.

- NDMP restore jobs may complete successfully even though no data (0 KB) has been restored. This situation can occur when a target volume does not have enough space for an image you are trying to restore.
- Workaround: Check the restore job details for entries similar to the following messages:

```
mm/dd/yyyy hh:mm:ss PM - Info ndmpagent(pid=11071) fas2050c1: RESTORE: We recommend that 19
inodes and 907620 kbytes of disk space be available on the target volume order to restore
this dump. You have 466260 inodes and 5316 kbytes of disk space on volume /vol/abc_15gb
mm/dd/yyyy hh:mm:ss PM - Info ndmpagent(pid=11071) fas2050c1: RESTORE: This restore will
proceed, but may fail when it runs out of inodes and/or disk space on this volume.
```

Confirm that the target volume does not have enough space for the restore image. If it does not, either free up enough space on the volume to complete the restore job successfully or specify a different restore volume.

NetBackup for NDMP troubleshooting suggestions

Try the following troubleshooting suggestions:

- Check the NetBackup All Log Entries report for information about the failed job.
- To verify that the appropriate services are running, use one of the following: the NetBackup Activity Monitor, the Windows control panel (on Windows systems), or the `bpps` command (UNIX systems).
- If NDMP host backups terminate with a status code of 154 (storage unit characteristics mismatch requests), the problem may be one of the following:
 - Verify that the NetBackup configuration is correct.
 - There may be a conflict between the policy type and storage unit type. (For example, if the policy type is Standard and the storage unit is of type NDMP.)
- If your NDMP backup fails with a status code of 99 (NDMP backup failure), no paths in your NDMP policy backup selections list were backed up. Check the NetBackup All Log Entries report for more information. A possible cause of this status is that none of the backup paths exist on the NDMP host.

For more information about status code 99 and NDMP backup failures, refer to the following tech note:

<http://www.veritas.com/docs/000081335>

- NetBackup does not support client-side deduplication of NDMP hosts. The backup jobs fail if you try to use client-side deduplication for NDMP hosts.

Troubleshooting NDMP media and devices on Windows

To troubleshoot media and devices on Windows, try the following:

- For legacy logging, enable debug logging by creating `reqlib` and `daemon` directories in the `install_path\Volmgr\debug` directory on the NetBackup for NDMP server.
- Check the Windows Event Viewer Application log for troubleshooting clues. For more information on the **Event Viewer logging** option, refer to the [NetBackup Troubleshooting Guide](#).
- Use the **Activity Monitor** utility or the Windows control panel to verify that the **Media and Device Management** utilities are running.
- Drives can be unexpectedly set to the DOWN state.

This action is due to communication problems between `avrd` on the NetBackup for NDMP server and the NDMP server application on the NDMP host. Some possible causes for the communication problems are:

- Network cable on the NDMP host was unplugged.
- NIS (Network Information System) problems on the NetBackup for NDMP server (NDMP client).
- The NDMP host was halted for too long.

Note: Whatever the cause, if the `avrd` connection to the NDMP host fails, the drive is set to DOWN. It is not automatically set to UP when the communication problem is corrected.

Troubleshooting NDMP media and devices on UNIX

To troubleshoot media and devices on UNIX, try the following:

- Ensure that the `syslogd` logs debug messages relating to `ltid` and other device processes.

For more information on `syslogd`, refer to the [NetBackup Troubleshooting Guide](#).

- Start `ltid` with the `-v` option. Check the system's syslog for troubleshooting clues.
- Use `vmps` to make sure that the appropriate daemons are running.
- Drives can be unexpectedly set to the DOWN state. This action is due to communication problems between `avrd` on the NetBackup for NDMP server and the NDMP server application on the NDMP host.
 Further details are available.
 See ["Troubleshooting NDMP media and devices on Windows"](#) on page 103.

Troubleshooting NDMP DirectCopy

When NetBackup enables NDMP DirectCopy for a backup image duplication, the NetBackup progress log includes the message "NDMP DirectCopy should be used." If NDMP DirectCopy was not enabled for the duplication, no specific messages about NDMP DirectCopy are listed in the progress log. For detailed messages (such as why NDMP DirectCopy was not used), consult the legacy debug logs for the admin log or the `bptm` log.

Refer to the [NetBackup Troubleshooting Guide](#) for information on legacy NetBackup logs.

Troubleshooting Direct Access Recovery (DAR) with NetBackup for NDMP

Note the following points when using Direct Access Recovery (DAR):

- DAR can be used when restoring NetBackup 4.5 or later backups. Starting with NetBackup 4.5, NetBackup stores the required DAR offset information on each backup.
- Backups must have been performed with the NetBackup catalog set to binary mode. If backups were made with the catalog set to ASCII mode, restores cannot use DAR. ASCII mode did not store the required DAR offset information on each backup. Note that all backups that were made before NetBackup 4.5 used ASCII catalog mode.

Note: Starting with NetBackup 6.0, all backups are in binary mode.

- To use DAR with NetBackup, the NDMP host you want to restore must support DAR. Some NDMP host vendors do not currently support DAR.

The following table lists the messages that may appear in the unified logs for `ndmpagent` (originator ID 134) on the NetBackup media server. These messages are also written to the progress log.

Table 10-2 DAR log messages

Message	Explanation
Data host does not support DAR recovery	The current NDMP host does not support DAR.
DAR disabled—continuing restore without DAR	DAR information is not available for the file.
DAR disabled—backup was performed before NB 4.5	The DAR feature can be used to restore the backups that NetBackup 4.5GA or later made. Starting with NetBackup 4.5GA, NetBackup stores the required DAR offset information on each backup. For pre-4.5GA NetBackup backups, restores cannot use DAR because the pre-4.5 versions did not store DAR offset information.
DAR disabled—NDMP host did not provide DAR info during backup	The backup was performed with an NDMP host version that does not support DAR. Ask the NDMP host vendor if a later NAS software version is available that supports DAR.
DAR disabled—Exceeded optimal DAR parameters for this image size	NetBackup determined that the restore would take longer with DAR than without it.
DAR disabled—Directory DAR not supported	DAR is automatically disabled when a restore job specifies a directory to restore. DAR can be used to restore files, but not to restoring directories.
DAR disabled by host parameters	DAR was disabled on the Master or Media Server Properties dialog box. See “About enabling or disabling DAR” on page 61.

About robot tests

Depending on the type of robot, use the tests in the following table to exercise the robot.

Table 10-3 Robot types and tests

Robot type	Test
TLD	tldtest
ACS	acstest

TLD robot test example for UNIX

To exercise drive 1 in the TLD robot `c2t3l0` the NDMP host `stripes` controls, use the following commands on UNIX:

```
/usr/opensv/volmgr/bin/tldtest -r stripes:c2t3l0 -d1 stripes:/dev/RMT/Ocbl
```

At the prompt, enter `?` for help information.

`inquiry` (Displays the Vendor ID and Product ID. If you get a UNIT ATTENTION message, try the `mode` command and then continue your testing.)

`s s` (Checks slot status.)

`s d` (Checks drive status.)

`m s3 d1` (Moves a tape from slot 3 to drive 1.)

`unload d1` (Unloads the tape.)

`m d1 s3` (Moves the tape back to slot 3.)

Using NetBackup for NDMP scripts

This chapter includes the following topics:

- [About the NetBackup for NDMP scripts](#)
- [ndmp_start_notify script \(UNIX\)](#)
- [ndmp_start_notify.cmd script \(Microsoft Windows\)](#)
- [ndmp_end_notify script \(UNIX\)](#)
- [ndmp_end_notify.cmd script \(Microsoft Windows\)](#)
- [ndmp_start_path_notify script \(UNIX\)](#)
- [ndmp_start_path_notify.cmd script \(Microsoft Windows\)](#)
- [ndmp_end_path_notify script \(UNIX\)](#)
- [ndmp_end_path_notify.cmd script \(Microsoft Windows\)](#)
- [ndmp_moving_path_notify script \(UNIX\)](#)
- [ndmp_moving_path_notify.cmd script \(Microsoft Windows\)](#)

About the NetBackup for NDMP scripts

This topic provides information that you can use to customize the NDMP-specific notification scripts.

NetBackup for NDMP provides the following scripts (commands on Windows) for collecting information and providing notification of events.

Table 11-1 Scripts to run on the NetBackup for NDMP server

Scripts for UNIX	Scripts for Windows
ndmp_start_notify	ndmp_start_notify.cmd
ndmp_end_notify	ndmp_end_notify.cmd
ndmp_start_path_notify	ndmp_start_path_notify.cmd
ndmp_end_path_notify	ndmp_end_path_notify.cmd
ndmp_moving_path_notify	ndmp_moving_path_notify.cmd

The scripts are similar to those already included in your NetBackup server installation. To create the scripts on UNIX, copy the `bpstart_notify` and `bpend_notify` scripts from

```
/usr/opensv/netbackup/bin/goodies (UNIX)
```

to

```
/usr/opensv/netbackup/bin
```

on the NetBackup for NDMP server. Then rename the copied scripts and modify as needed.

On Windows, you must create the scripts from scratch.

ndmp_start_notify script (UNIX)

The UNIX scripts are provided as examples only. You must customize the scripts before using them. For example, the `-ne` value in the first `if` statement must be modified to reflect the number of passed parameters. For the `ndmp_start_notify` script, the `-ne` value must be set to 7.

On the UNIX media server, NetBackup calls the `ndmp_start_notify` script each time the client starts a backup operation. To use this script, create a script similar to

```
/usr/opensv/netbackup/bin/goodies/bpstart_notify
```

on the server, and copy it to

```
/usr/opensv/netbackup/bin/ndmp_start_notify
```

on the UNIX NetBackup for NDMP server. Then, modify the script and ensure that you have permission to run it.

Note: Before you use this script, make sure that you can run it by using `other` on the media server. Run `chmod 755 script_name`, where *script_name* is the name of the script.

The `ndmp_start_notify` script runs each time a backup starts and after the tape has been positioned. This script must exit with a status of 0 for the calling program to continue and for the backup to proceed. A nonzero status causes the client backup to exit with a status of `ndmp_start_notify failed`.

If the `/usr/opensv/netbackup/bin/ndmp_start_notify` script exists, it runs in the foreground. The `bptm` process that is on the NetBackup for NDMP server waits for it to complete before continuing. Any commands in the script that do not end with an `&` character run serially.

The server expects the client to respond with a `continue` message within the period of time that the NetBackup `CLIENT_READ_TIMEOUT` option on the server specifies.

The default for `CLIENT_READ_TIMEOUT` is 300. If the script needs more time than 300 seconds, increase the value to allow more time.

NetBackup passes the following parameters to the script:

Table 11-2 Script parameters for `ndmp_start_notify` (UNIX)

Parameter	Description
\$1	Specifies the name of the NDMP host.
\$2	Specifies the policy name from the NetBackup catalog.
\$3	Specifies the schedule name from the NetBackup catalog.
\$4	Specifies one of the following: FULL INCR (differential incremental) CINC (cumulative incremental)
\$5	Specifies the NetBackup status code for the operation.

For example:

```
ndmp_start_notify freddie cd4000s fulls FULL 0
ndmp_start_notify danr cd4000s incrementals INCR 0
ndmp_start_notify hare cd4000s fulls FULL 0
```

To create an `ndmp_start_notify` script for a specific policy or policy and schedule combination, create script files with a `.polycname` or `.polycname.schedulename` suffix. In the following two examples of script names, the policy is named `production` and the schedule is named `fulls`:

```
/usr/opensv/netbackup/bin/ndmp_start_notify.production  
/usr/opensv/netbackup/bin/ndmp_start_notify.production.fulls
```

The first script affects all scheduled backups in the policy that is named `production`. The second script affects scheduled backups in the policy that is named `production` only when the schedule is named `fulls`.

Note: For a given backup, NetBackup uses only one `ndmp_start_notify` script and that is the one with the most specific name. For example, if there are both `ndmp_start_notify.production` and `ndmp_start_notify.production.fulls` scripts, NetBackup uses only `ndmp_start_notify.production.fulls`.

The `ndmp_start_notify` script can use the following environment variables:

```
BACKUPID  
UNIXBACKUPTIME  
BACKUPTIME
```

The NetBackup `bptm` process creates these variables. The following are examples of the strings that are available to the script for use in recording information about a backup:

```
BACKUPID=freddie_0857340526  
UNIXBACKUPTIME=0857340526  
BACKUPTIME=Sun Mar 2 16:08:46 1997
```

ndmp_start_notify.cmd script (Microsoft Windows)

When you use Windows NetBackup for NDMP media servers, you can create the batch scripts that provide notification whenever the client starts a backup. These scripts must reside on the media server in the following directory:

```
install_path\NetBackup\bin
```

where `install_path` is the directory where NetBackup is installed.

You can create `ndmp_start_notify` scripts that provide notification for all backups or only for backups of a specific policy or schedule. The `ndmp_start_notify` script runs each time a backup starts and after the tape is positioned.

To create a script that applies to all backups, name the script:

```
install_path\netbackup\bin\ndmp_start_notify.cmd
```

To create an `ndmp_start_notify` script that applies only to a specific policy or policy and schedule combination, add a `.polycname` or `.polycname.schedulename` suffix to the script name. The following are two examples:

- The following script applies only to a policy named `days`:

```
install_path\netbackup\bin\ndmp_start_notify.days.cmd
```

- The following script applies only to a schedule that is named `fulls`, which is in a policy named `days`:

```
install_path\netbackup\bin\ndmp_start_notify.days.fulls.cmd
```

The first script affects the scheduled backups in the policy named `days`. The second script affects the scheduled backups in the policy named `days` only when the schedule is named `fulls`.

For a given backup, NetBackup calls only one `ndmp_start_notify` script and checks for them in the following order:

```
ndmp_start_notify.policy.schedule.cmd
ndmp_start_notify.policy.cmd
ndmp_start_notify.cmd
```

For example, if there are both `ndmp_start_notify.policy.cmd` and `ndmp_start_notify.policy.schedule.cmd` scripts, NetBackup uses only the `ndmp_start_notify.policy.schedule.cmd` script.

Note: If you also use `ndmp_end_notify` scripts, they can provide a different level of notification than the `ndmp_start_notify` scripts. For example, if you had one of each, they could be `ndmp_start_notify.policy.cmd` and `ndmp_end_notify.policy.schedule.cmd`.

When the backup starts, NetBackup passes the following parameters to the script:

Table 11-3 Script parameters for `ndmp_start_notify.cmd` (Microsoft Windows)

Parameter	Description
%1	Specifies the name of the client from the NetBackup catalog.

Table 11-3 Script parameters for ndmp_start_notify.cmd (Microsoft Windows)
(continued)

Parameter	Description
%2	Specifies the policy name from the NetBackup catalog.
%3	Specifies the schedule name from the NetBackup catalog.
%4	Specifies one of the following: FULL INCR CINC
%5	Specifies the status of the operation is always 0 for bpstart_notify.
%6	Specifies the results file that NetBackup checks for a return code from the script. NetBackup uses %6 to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named <i>install_path\netbackup\bin\NDMP_START_NOTIFY_RES.policy.schedule</i> If the script applies to a specific policy, the results file must be named <i>install_path\NetBackup\bin\NDMP_START_NOTIFY_RES.policy</i> If the script applies to all backups, the results file must be named <i>install_path\NetBackup\bin\NDMP_START_NOTIFY_RES</i> An <code>echo 0> %6</code> statement is one way for the script to create the file. NetBackup deletes the existing results file before it calls the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.

The server expects the client to respond with a `continue` message within the period of time that the NetBackup `CLIENT_READ_TIMEOUT` option on the server specifies. The default is 300 seconds. If the script needs more than 300 seconds, increase the value to allow more time.

ndmp_end_notify script (UNIX)

The `ndmp_end_notify` script is run at the end of the backup. The backup does not wait for the script to complete.

Note: Before you use this script, make sure you can run it by using `other` on the media server. Run `chmod 755 script_name`, where *script_name* is the name of the script.

The UNIX scripts are provided as examples only. You must customize the scripts before using them. For example, the `-ne` value in the first if statement must be modified to reflect the number of passed parameters. For the `ndmp_end_notify` script, the `-ne` value must be set to 7.

For a UNIX media server, if you need notification whenever the NDMP host completes a backup, copy

```
/usr/opensv/netbackup/bin/goodies/bpend_notify
```

from the server, to

```
/usr/opensv/netbackup/bin/ndmp_end_notify
```

on the UNIX NetBackup for NDMP host. Then, modify the script and ensure that you have permission to run it.

The `ndmp_end_notify` script runs each time a backup completes.

NetBackup passes the following parameters to the `ndmp_end_notify` script:

Table 11-4 Script parameters for `ndmp_end_notify` (UNIX)

Parameter	Description
\$1	Specifies the name of the client from the NetBackup catalog.
\$2	Specifies the policy name from the NetBackup catalog.
\$3	Specifies the schedule name from the NetBackup catalog.
\$4	Specifies one of the following: FULL INCR (differential incremental) CINC (cumulative incremental)
\$5	Specifies the exit code from <code>bptm</code> .

For example:

```
ndmp_end_notify freddie cd4000s fulls FULL 0  
ndmp_end_notify danr cd4000s incrementals INCR 73
```

To create an `ndmp_end_notify` script for a specific policy or policy and schedule combination, create script files with a `.policyname` or `.policyname.schedulename` suffix. In the following two examples of script names, the policy is named `production` and the schedule is named `fulls`:

```
/usr/opensv/netbackup/bin/ndmp_end_notify.production  
/usr/opensv/netbackup/bin/ndmp_end_notify.production.fulls
```

The first script affects all scheduled backups in the policy that is named `production`. The second script affects scheduled backups in the policy that is named `production` only when the schedule is named `fulls`.

Note: For a given backup, NetBackup uses only one `ndmp_end_notify` script and that is the one with the most specific name. For example, if there are both `ndmp_end_notify.production` and `ndmp_end_notify.production.fulls` scripts, NetBackup uses only `ndmp_end_notify.production.fulls`.

The `ndmp_end_notify` script can use the following environment variables:

```
BACKUPID  
UNIXBACKUPTIME  
BACKUPTIME
```

The NetBackup `bptm` process creates these variables. The following are examples of the strings that are available to the script for use in recording information about a backup:

```
BACKUPID=freddie_0857340526  
UNIXBACKUPTIME=0857340526  
BACKUPTIME=Sun Mar 2 16:08:46 1997
```

ndmp_end_notify.cmd script (Microsoft Windows)

For Windows media servers, you can create the batch scripts that provide notification whenever the client completes a backup. These scripts must reside on the media server in the same directory as the NetBackup binaries:

```
install_path\NetBackup\bin
```

where *install_path* is the directory where NetBackup is installed.

You can create `ndmp_end_notify` scripts that provide notification for all backups or only for backups of a specific policy or schedule.

To create an `ndmp_end_notify` script that applies to all backups, name the script:

```
install_path\netbackup\bin\ndmp_end_notify.cmd
```

To create a script that applies only to a specific policy or policy and schedule combination, add a `.policyname` or `.policyname.schedulename` suffix to the script name. The following are two examples:

- The following script applies only to a policy named `days`:

```
install_path\netbackup\bin\ndmp_end_notify.days.cmd
```

- The following script applies only to a schedule that is named `fulls`, which is in a policy named `days`:

```
install_path\netbackup\bin\ndmp_end_notify.days.fulls.cmd
```

The first script affects all scheduled backups in the policy named `days`. The second script affects scheduled backups in the policy named `days` only when the schedule is named `fulls`.

For a given backup, NetBackup calls only one `ndmp_end_notify` script and checks for them in the following order:

```
ndmp_end_notify.policy.schedule.cmd  
ndmp_end_notify.policy.cmd  
ndmp_end_notify.cmd
```

For example, if there are both `ndmp_end_notify.policy.cmd` and `ndmp_end_notify.policy.schedule.cmd` scripts, NetBackup uses only `ndmp_end_notify.policy.schedule.cmd`.

Note: If you also use `ndmp_start_notify` scripts, they can provide a different level of notification than the `ndmp_end_notify` scripts. For example, if you had one of each, they could be `ndmp_start_notify.policy.cmd` and `ndmp_end_notify.policy.schedule.cmd`.

When the backup completes, NetBackup passes the following parameters to the script:

Table 11-5 Script parameters for `ndmp_end_notify.cmd` (Microsoft Windows)

Parameter	Description
%1	Specifies the name of the client from the NetBackup catalog.
%2	Specifies the policy name from the NetBackup catalog.

Table 11-5 Script parameters for ndmp_end_notify.cmd (Microsoft Windows)
(continued)

Parameter	Description
%3	Specifies the schedule name from the NetBackup catalog.
%4	Specifies one of the following: FULL INCR CINC
%5	Specifies the status of the operation. It is the same as the status sent to the NetBackup server. This status is 0 for successful backups and 1 for partially successful backups. If an error occurs, the status is the value associated with that error.
%6	Note: The following file is not checked at the end of a backup. Specifies the results file that NetBackup checks for a return code from the script. NetBackup uses %6 to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named <i>install_path\NetBackup\bin\NDMP_END_NOTIFY_RES.policy.schedule</i> If the script applies to a specific policy, the results file must be named <i>install_path\netbackup\bin\NDMP_END_NOTIFY_RES.policy</i> If the script applies to all backups, the results file must be named <i>install_path\NetBackup\bin\NDMP_END_NOTIFY_RES</i> An <code>echo 0> %6</code> statement is one way for the script to create the file. NetBackup deletes the existing results file before it calls the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.

ndmp_start_path_notify script (UNIX)

The UNIX scripts are provided as examples only. You must customize the scripts before using them. For example, the `-ne` value in the first `if` statement must be modified to reflect the number of passed parameters. For the `ndmp_start_path_notify` script, the `-ne` value must be set to 7.

To use this script, create a script similar to

```
/usr/opensv/netbackup/bin/goodies/bpstart_notify
```

on the server, and copy it to

```
/usr/opensv/netbackup/bin/ndmp_start_path_notify
```

on the UNIX NetBackup for NDMP server. Then, modify the script and ensure that you have permission to run it.

On the UNIX media server, the `ndmp_start_path_notify` script runs before the backup process is issued to the NAS machine. This script must exit with a status of 0 for the calling program to continue and for the backup to proceed. A nonzero status causes the client backup to exit with a status of 99 (NDMP backup failure).

Note: Before you use this script, make sure you can run it by using `other` on the media server. Run `chmod 755 script_name`, where *script_name* is the name of the script.

If the `/usr/opensv/netbackup/bin/ndmp_start_path_notify` script exists, it runs in the foreground. The `bptm` process on the NetBackup for NDMP server waits for it to complete before continuing. Any commands in the script that do not end with an `&` character run serially.

The server expects the client to respond with a `continue` message within the period of time that the NetBackup `CLIENT_READ_TIMEOUT` option on the server specifies.

The default for `CLIENT_READ_TIMEOUT` is 300. If the script needs more time than 300 seconds, increase the value to allow more time.

NetBackup passes the following parameters to the script:

Table 11-6 Script parameters for `ndmp_start_path_notify` (UNIX)

Parameter	Description
\$1	Specifies the name of the NDMP host.
\$2	Specifies the policy name from the NetBackup catalog.
\$3	Specifies the schedule name from the NetBackup catalog.
\$4	Specifies one of the following: FULL INCR (differential incremental) CINC (cumulative incremental)
\$5	Specifies the NetBackup status code for the operation.

Table 11-6 Script parameters for ndmp_start_path_notify (UNIX) (*continued*)

Parameter	Description
\$6	Not used.
\$7	Specifies the path being backed up.

For example:

```
ndmp_start_path_notify freddie cd4000s fulls FULL
ndmp_start_path_notify danr cd4000s incrementals INCR
ndmp_start_path_notify hare cd4000s fulls FULL
```

To create an `ndmp_start_path_notify` script for a specific policy or policy and schedule combination, create script files with a `.polycyname` or `.polycyname.schedulename` suffix. In the following two examples of script names, the policy is named `production` and the schedule is named `fulls`:

```
/usr/opensv/netbackup/bin/ndmp_start_path_notify.production
/usr/opensv/netbackup/bin/ndmp_start_path_notify.production.fulls
```

The first script affects all scheduled backups in the policy that is named `production`. The second script affects scheduled backups in the policy that is named `production` only when the schedule is named `fulls`.

Note: For a given backup, NetBackup uses only one `ndmp_start_path_notify` script and that is the one with the most specific name. For example, if there are both `ndmp_start_path_notify.production` and `ndmp_start_path_notify.production.fulls` scripts, NetBackup uses only `ndmp_start_path_notify.production.fulls`.

The `ndmp_start_path_notify` script can use the following environment variables:

```
BACKUPID
UNIXBACKUPTIME
BACKUPTIME
```

The NetBackup `bptm` process creates these variables. The following are examples of the strings that are available to the script for use in recording information about a backup:

```
BACKUPID=freddie_0857340526
UNIXBACKUPTIME=0857340526
BACKUPTIME=Sun Mar 2 16:08:46 1997
```

ndmp_start_path_notify.cmd script (Microsoft Windows)

For Windows media servers, you can create the batch scripts that provide notification before the backup process is issued to the NAS machine. These scripts must reside on the media server in the same directory as the NetBackup binaries:

```
install_path\NetBackup\bin
```

where *install_path* is the directory where NetBackup is installed.

You can create `ndmp_start_path_notify` scripts that provide notification for all backups or only for backups of a specific policy or schedule.

To create an `ndmp_start_path_notify` script that applies to all backups, name the script:

```
install_path\netbackup\bin\ndmp_start_path_notify.cmd
```

To create a script that applies only to a specific policy or policy and schedule combination, add a `.polycname` or `.polycname.schedulename` suffix to the script name. The following are two examples:

- The following script applies only to a policy named `days`:

```
install_path\netbackup\bin\ndmp_start_path_notify.days.cmd
```

- The following script applies only to a schedule that is named `fulls`, which in a policy named `days`:

```
install_path\netbackup\bin\ndmp_start_path_notify.days.fulls.cmd
```

The first script affects all scheduled backups in the policy named `days`. The second script affects scheduled backups in the policy named `days` only when the schedule is named `fulls`.

For a given backup, NetBackup calls only one `ndmp_start_path_notify` script and checks for them in the following order:

```
ndmp_start_path_notify.policy.schedule.cmd  
ndmp_start_path_notify.policy.cmd  
ndmp_start_path_notify.cmd
```

For example, if there are both `ndmp_start_path_notify.policy.cmd` and `ndmp_start_path_notify.policy.schedule.cmd` scripts, NetBackup uses only `ndmp_start_path_notify.policy.schedule.cmd`.

Note: If you also use `ndmp_start_notify` scripts, they can provide a different level of notification than the `ndmp_start_path_notify` scripts. For example, if you had one of each, they could be `ndmp_start_notify.policy.cmd` and `ndmp_start_path_notify.policy.schedule.cmd`.

When the backup starts, NetBackup passes the following parameters to the script:

Table 11-7 Script parameters for `ndmp_start_path_notify.cmd` (Microsoft Windows)

Parameter	Description
%1	Specifies the name of the client from the NetBackup catalog.
%2	Specifies the policy name from the NetBackup catalog.
%3	Specifies the schedule name from the NetBackup catalog.
%4	Specifies one of the following: FULL INCR CINC
%5	Specifies the status of the operation. It is the same as the status sent to the NetBackup server. This status is 0 for successful backups and 1 for partially successful backups. If an error occurs, the status is the value associated with that error.
%6	Specifies the results file that NetBackup checks for a return code from the script. NetBackup uses %6 to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named <code>install_path\netbackup\bin\NDMP_START_PATH_NOTIFY_RES.policy.schedule</code> If the script applies to a specific policy, the results file must be named <code>install_path\NetBackup\bin\NDMP_START_PATH_NOTIFY_RES.policy</code> If the script applies to all backups, the results file must be named <code>install_path\NetBackup\bin\NDMP_START_PATH_NOTIFY_RES</code> An <code>echo 0> %6</code> statement is one way for the script to create the file. NetBackup deletes the existing results file before it calls the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.
%7	Pathname being backed up.

ndmp_end_path_notify script (UNIX)

The UNIX scripts are provided as examples only. You must customize the scripts before using them. For example, the `-ne` value in the first `if` statement must be modified to reflect the number of passed parameters. For the `ndmp_end_path_notify` script, the `-ne` value must be set to 7.

Note: Before you use this script, make sure you can run it by using `other` on the media server. Run `chmod 755 script_name`, where *script_name* is the name of the script.

For a UNIX media server, if you need notification whenever the NDMP host completes a backup, copy

```
/usr/opensv/netbackup/bin/goodies/bpend_notify
```

from the server, to

```
/usr/opensv/netbackup/bin/ndmp_end_path_notify
```

on the UNIX NetBackup for NDMP host. Then, modify the script and ensure that you have permission to run it.

The `ndmp_end_path_notify` script runs after the NAS machine has informed NetBackup that it has completed sending data.

NetBackup passes the following parameters to the `ndmp_end_notify` script:

Table 11-8 Script parameters for `ndmp_end_path_notify` (UNIX)

Parameter	Description
\$1	Specifies the name of the client from the NetBackup catalog.
\$2	Specifies the policy name from the NetBackup catalog.
\$3	Specifies the schedule name from the NetBackup catalog.
\$4	Specifies one of the following: FULL INCR (differential incremental) CINC (cumulative incremental)
\$5	Specifies the exit code from <code>bptm</code> .
\$6	Not used.

Table 11-8 Script parameters for ndmp_end_path_notify (UNIX) (*continued*)

Parameter	Description
\$7	Specifies the path being backed up.

For example:

```
ndmp_end_path_notify freddie cd4000s fulls FULL 0
ndmp_end_path_notify danr cd4000s incrementals INCR 73
```

To create an `ndmp_end_path_notify` script for a specific policy or policy and schedule combination, create script files with a `.polycname` or `.polycname.schedulename` suffix. In the following two examples of script names, the policy is named `production` and the schedule is named `fulls`:

```
/usr/opensv/netbackup/bin/ndmp_end_path_notify.production
/usr/opensv/netbackup/bin/ndmp_end_path_notify.production.fulls
```

The first script affects all scheduled backups in the policy that is named `production`. The second script affects scheduled backups in the policy that is named `production` only when the schedule is named `fulls`.

Note: For a given backup, NetBackup uses only one `ndmp_end_path_notify` script and that is the one with the most specific name. For example, if there are both `ndmp_end_path_notify.production` and `ndmp_end_path_notify.production.fulls` scripts, NetBackup uses only `ndmp_end_path_notify.production.fulls`.

The `ndmp_end_path_notify` script can use the following environment variables:

```
BACKUPID
UNIXBACKUPTIME
BACKUPTIME
```

The NetBackup `bptm` process creates these variables. The following are examples of the strings that are available to the script for use in recording information about a backup:

```
BACKUPID=freddie_0857340526
UNIXBACKUPTIME=0857340526
BACKUPTIME=Sun Mar 2 16:08:46 1997
```

ndmp_end_path_notify.cmd script (Microsoft Windows)

For Windows media servers, you can create the batch scripts that provide notification whenever the client is finished writing to tape. These scripts must reside on the media server in the same directory as the NetBackup binaries:

```
install_path\NetBackup\bin
```

where *install_path* is the directory where NetBackup is installed.

You can create `ndmp_end_path_notify` scripts that provide notification for all backups or only for backups of a specific policy or schedule.

To create an `ndmp_end_path_notify` script that applies to all backups, name the script:

```
install_path\netbackup\bin\ndmp_end_path_notify.cmd
```

To create a script that applies only to a specific policy or policy and schedule combination, add a `.policyname` or `.policyname.schedulename` suffix to the script name. The following are two examples:

- The following script applies only to a policy named `days`:

```
install_path\netbackup\bin\ndmp_end_path_notify.days.cmd
```

- The following script applies only to a schedule that is named `fulls`, which is in a policy named `days`:

```
install_path\netbackup\bin\ndmp_end_path_notify.days.fulls.  
cmd
```

The first script affects all scheduled backups in the policy named `days`. The second script affects scheduled backups in the policy named `days` only when the schedule is named `fulls`.

For a given backup, NetBackup calls only one `ndmp_end_path_notify` script and checks for them in the following order:

```
ndmp_end_path_notify.policy.schedule.cmd  
ndmp_end_path_notify.policy.cmd  
ndmp_end_path_notify.cmd
```

For example, if there are both `ndmp_end_path_notify.policy.cmd` and `ndmp_end_path_notify.policy.schedule.cmd` scripts, NetBackup uses only `ndmp_end_path_notify.policy.schedule.cmd`.

Note: If you also use `ndmp_end_notify` scripts, they can provide a different level of notification than the `ndmp_end_path_notify` scripts. For example, if you had one of each, they could be `ndmp_end_notify.policy.cmd` and `ndmp_end_path_notify.policy.schedule.cmd`.

When the backup completes, NetBackup passes the following parameters to the script:

Table 11-9 Script parameters for `ndmp_end_path_notify.cmd` (Microsoft Windows)

Parameter	Description
%1	Specifies the name of the client from the NetBackup catalog.
%2	Specifies the policy name from the NetBackup catalog.
%3	Specifies the schedule name from the NetBackup catalog.
%4	Specifies one of the following: FULL INCR CINC
%5	Specifies the status of the operation. It is the same as the status sent to the NetBackup server. This status is 0 for successful backups and 1 for partially successful backups. If an error occurs, the status is the value associated with that error.

Table 11-9 Script parameters for ndmp_end_path_notify.cmd (Microsoft Windows) (*continued*)

Parameter	Description
%6	Note: The following file is not checked when using <code>ndmp_end_path_notify</code>. Specifies the results file that NetBackup checks for a return code from the script. NetBackup uses %6 to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named <i>install_path\NetBackup\bin\NDMP_END_PATH_NOTIFY_RES.policy.schedule</i> If the script applies to a specific policy, the results file must be named <i>install_path\netbackup\bin\NDMP_END_PATH_NOTIFY_RES.policy</i> If the script applies to all backups, the results file must be named <i>install_path\NetBackup\bin\NDMP_END_PATH_NOTIFY_RES</i> An <code>echo 0 > %6</code> statement is one way for the script to create the file. NetBackup deletes the existing results file before it calls the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.
%7	Specifies the pathname being backed up.

ndmp_moving_path_notify script (UNIX)

The UNIX scripts are provided as examples only. You must customize the scripts before using them. For example, the `-ne` value in the first if statement must be modified to reflect the number of passed parameters. For the `ndmp_moving_path_notify` script, the `-ne` value must be set to 7.

To use this script, create a script similar to

```
/usr/opensv/netbackup/bin/goodies/bpstart_notify
```

on the server, and copy it to

```
/usr/opensv/netbackup/bin/ndmp_moving_path_notify
```

on the UNIX NetBackup for NDMP server. Then, modify the script and ensure that you have permission to run it.

On UNIX media servers, the `ndmp_moving_path_notify` script runs after the backup process sends data to NetBackup.

Note: Before you use this script, make sure you can run it using other on the media server. Run `chmod 755 script_name`, where *script_name* is the name of the script.

If the `/usr/opensv/netbackup/bin/ndmp_moving_path_notify` script exists, it runs in the foreground. The `bptm` process that is on the NetBackup for NDMP server waits for it to complete before continuing. Any commands in the script that do not end with an `&` character run serially.

The server expects the client to respond with a `continue` message within the period of time that the NetBackup `CLIENT_READ_TIMEOUT` option on the server specifies.

The default for `CLIENT_READ_TIMEOUT` is 300 seconds. If the script needs more than 300 seconds, increase the value to allow more time.

NetBackup passes the following parameters to the script:

Table 11-10 Script parameters for `ndmp_moving_path_notify` (UNIX)

Parameter	Description
\$1	Specifies the name of the NDMP host.
\$2	Specifies the policy name from the NetBackup catalog.
\$3	Specifies the schedule name from the NetBackup catalog.
\$4	Specifies one of the following: FULL INCR (differential incremental) CINC (cumulative incremental)
\$5	Specifies the NetBackup status code for the operation.
\$6	Not used.
\$7	Specifies the path being backed up.

For example:

```
ndmp_moving_path_notify freddie cd4000s fulls FULL
ndmp_moving_path_notify danr cd4000s incrementals INCR
ndmp_moving_path_notify hare cd4000s fulls FULL
```

To create an `ndmp_moving_path_notify` script for a specific policy or policy and schedule combination, create script files with a `.polycname` or `.polycname.schedulename` suffix. In the following two examples of script names, the policy is named `production` and the schedule is named `fulls`:

```
/usr/opensv/netbackup/bin/ndmp_moving_path_notify.production
/usr/opensv/netbackup/bin/ndmp_moving_path_notify.production.fulls
```

The first script affects all scheduled backups in the policy that is named `production`. The second script affects scheduled backups in the policy that is named `production` only when the schedule is named `fulls`.

Note: For a given backup, NetBackup uses only one `ndmp_moving_path_notify` script and that is the one with the most specific name. For example, if there are both `ndmp_moving_path_notify.production` and `ndmp_moving_path_notify.production.fulls` scripts, NetBackup uses only `ndmp_moving_path_notify.production.fulls`.

The `ndmp_moving_path_notify` script can use the following environment variables:

```
BACKUPID
UNIXBACKUPTIME
BACKUPTIME
```

The NetBackup `bptm` process creates these variables. The following are examples of the strings that are available to the script for use in recording information about a backup:

```
BACKUPID=freddie_0857340526
UNIXBACKUPTIME=0857340526
BACKUPTIME=Sun Mar 2 16:08:46 1997
```

ndmp_moving_path_notify.cmd script (Microsoft Windows)

For Windows media servers, you can create the batch scripts that provide notification whenever the NAS machine starts sending data. These scripts must reside on the media server in the same directory as the NetBackup binaries:

```
install_path\NetBackup\bin
```

where *install_path* is the directory where NetBackup is installed.

You can create `ndmp_moving_path_notify` scripts that provide notification for all backups or only for backups of a specific policy or schedule.

To create an `ndmp_moving_path_notify` script that applies to all backups, name the script:

```
install_path\netbackup\bin\ndmp_moving_path_notify.cmd
```

To create a script that applies only to a specific policy or policy and schedule combination, add a `.polycname` or `.polycname.schedulename` suffix to the script name. The following are two examples:

- The following script applies only to a policy named `days`:

```
install_path\netbackup\bin\ndmp_moving_path_notify.days.cmd
```

- The following script applies only to a schedule that is named `fulls`, which is in a policy named `days`:

```
install_path\netbackup\bin\ndmp_moving_path_notify.days.fulls.cmd
```

The first script affects all scheduled backups in the policy named `days`. The second script affects scheduled backups in the policy named `days` only when the schedule is named `fulls`.

For a given backup, NetBackup calls only one `ndmp_moving_path_notify` script and checks for them in the following order:

```
ndmp_moving_path_notify.policy.schedule.cmd  
ndmp_moving_path_notify.policy.cmd  
ndmp_moving_path_notify.cmd
```

For example, if there are both `ndmp_moving_path_notify.policy.cmd` and `ndmp_moving_path_notify.policy.schedule.cmd` scripts, NetBackup uses only `ndmp_moving_path_notify.policy.schedule.cmd`.

Note: If you also use `ndmp_start_notify` scripts, they can provide a different level of notification than the `ndmp_moving_path_notify` scripts. For example, if you had one of each, they could be `ndmp_start_notify.policy.cmd` and `ndmp_moving_path_notify.policy.schedule.cmd`.

When the backup starts, NetBackup passes the following parameters to the script.

Table 11-11 Script parameters for ndmp_moving_path_notify.cmd (Microsoft Windows)

Parameter	Description
%1	Specifies the name of the client from the NetBackup catalog.
%2	Specifies the policy name from the NetBackup catalog.
%3	Specifies the schedule name from the NetBackup catalog.
%4	Specifies one of the following: FULL INCR CINC
%5	Specifies the status of the operation. It is the same as the status sent to the NetBackup server. This status is 0 for successful backups and 1 for partially successful backups. If an error occurs, the status is the value associated with that error.
%6	Note: The following is not checked when using <code>ndmp_moving_path_notify</code>. Specifies the results file that NetBackup checks for a return code from the script. NetBackup uses %6 to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named <code>install_path\netbackup\bin\NDMP_END_NOTIFY_RES.policy.schedule</code> If the script applies to a specific policy, the results file must be named <code>install_path\NetBackup\bin\NDMP_END_NOTIFY_RES.policy</code> If the script applies to all backups, the results file must be named <code>install_path\NetBackup\bin\NDMP_END_NOTIFY_RES</code> An <code>echo 0> %6</code> statement is one way for the script to create the file. NetBackup deletes the existing results file before it calls the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.
%7	Specifies the pathname being backed up.