

VERITAS NetBackup™ 5.1

Media Manager System Administrator's Guide

for Windows

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Legal Notice

Copyright © 1998-2004 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS Software, the VERITAS logo, VERITAS NetBackup, VERITAS Backup Exec, and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo, VERITAS NetBackup Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

Portions of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright 1991-92, RSA Data Security, Inc. Created 1991. All rights reserved.

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650-527-8000 Fax 650-527-2901
www.veritas.com

Third-Party Copyrights

ACE 5.2A: ACE(TM) is copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine, Copyright (c) 1993-2002, all rights reserved.

IBM XML for C++ (XML4C) 3.5.1: Copyright (c) 1999,2000,2001 Compaq Computer Corporation; Copyright (c) 1999,2000,2001 Hewlett-Packard Company; Copyright (c) 1999,2000,2001 IBM Corporation; Copyright (c) 1999,2000,2001 Hummingbird Communications Ltd.; Copyright (c) 1999,2000,2001 Silicon Graphics, Inc.; Copyright (c) 1999,2000,2001 Sun Microsystems, Inc.; Copyright (c) 1999,2000,2001 The Open Group; All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

JacORB 1.4.1: The licensed software is covered by the GNU Library General Public License, Version 2, June 1991.

Open SSL 0.9.6: This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

TAO (ACE ORB) 1.2a: TAO(TM) is copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine, Copyright (c) 1993-2002, all rights reserved.



Contents

Preface	xxv
What Is In This Guide?	xxv
How To Use This Guide	xxvi
Getting Help	xxvi
NetBackup Manuals	xxviii
Related Resources	xxx
Glossary	xxx
Accessibility Features	xxxi
Conventions	xxxi
 Chapter 1. Introduction to Media Manager	1
Media Manager Terminology	1
Media Manager Features	5
Media Manager Hosts	7
Master Servers	8
Media Servers	8
SAN Media Servers	8
Volume Database Host	9
Global Device Database Host	9
Media Manager Storage Devices	10
Media Manager Volumes	10
Mounting and Using Volumes	11
Media Manager Administration Utilities	12
Starting the Media Manager Administration Utilities	12



Shortcut Menus	14
Device and Media Configuration Overview	14
Security Issues	15
Chapter 2. Configuring Storage Devices	17
Starting Device Management	18
Using the Device Management Window	18
Menus and Commands	19
Toolbars	21
Tree Pane	22
Global Topology Pane	23
Topology Icons	23
Topology Connections	24
Selecting Topology Objects	24
Devices Pane	25
Managing the Devices Pane	25
Using the Drives Tab	25
Using the Robots Tab	29
Using the Hosts Tab	31
Status Bar	31
Shortcut Menus and Commands	31
Customizing the Window	32
Viewing and Rearranging Columns	33
Changing the View of the Topology Pane	33
Allowable Media Manager Characters	34
Performing Initial Device Configuration	34
Managing the Device Manager Service (Windows) or the Device Daemon (UNIX) ..	36
The Device Mapping File	36
NetBackup Mixed Server Configurations	37
Administering Devices on Other Servers	38



Media Manager Security	39
vmd Considerations	40
Example SERVER Entries	40
The Global Device Database Host	41
A Single Host is Required	41
How This Host is Determined	42
Managing The Global Device Database Host	42
Why You Should Use the Media Manager Wizards	43
The Device Configuration Wizard	44
Operating System Changes	45
Possible Global Device Database Host Conflict	45
Configuring Devices not Supported by the Wizard	45
Managing Devices that are Partially-Configured	45
Learning More About the Device Configuration Wizard	46
Starting the Device Configuration Wizard	46
Adding Robots	46
Dialog Entries for Adding and Changing Robots	48
Device Host	48
Robot Type	48
Robot Number	49
Volume Database Host	50
Robot Control Section of the Dialog	50
Robot is controlled locally by this device host	53
Robot control is handled by a remote host	55
Robot control is attached to an NDMP host	57
Adding Shared Drives	57
Using the Device Configuration Wizard to Configure Shared Drives	58
Using The Shared Drive Wizard to Configure Shared Drives	59
Learning More About the Shared Drive Wizard	59
Starting the Shared Drive Wizard	59



Using Alternate Interfaces to Configure Shared Drives	59
tpconfig menus	60
tpconfig Command Line Interface	60
Adding Drives	60
Dialog Entries for Adding (or Changing Drives)	62
Device Host Section of the Dialog	62
Device Host	62
Drive Information Section of the Dialog	62
Drive Name	63
Drive Type	63
Device Name	63
No Rewind Device	63
Character Device	64
Volume Header Device	64
Cleaning Frequency	65
Drive Is In A Robotic Library	65
Robotic Drive Information Section of the Dialog	66
Robotic Library	66
Robot Drive Number	66
Managing Your Device Configuration	68
When to Perform Device Configuration Changes	69
Using the Device Configuration Wizard for Configuration Changes	69
Changing a Robot Configuration	69
Changing the Configuration of a Drive	70
Changing a Non-Shared Drive to a Shared Drive	70
Changing the Volume Database Host for Standalone Drives	71
Deleting Robots	72
Deleting Drives	72
Drive Cleaning Functions	73
Performing Drive Diagnostics	74



Executing Diagnostic Tests for a Drive	74
Exiting a Diagnostic Test When Testing is Complete	76
Stopping a Diagnostic Test and Changing the Drive to be Tested	76
Obtaining Detailed Information For a Particular Test Step	76
Managing a Test Step that Requires Operator Intervention	76
Using SANPoint Control to Investigate SAN Problems	77
Printing Your Device Configuration	78
Robot and Drive Configuration Examples	79
Example 1: Configuring a Robot on a Server	79
Example 2: Configuring Standalone Drives on a Server	81
Example 3: Configuring a Robot Distributed Among Multiple Servers	83
Configuration on the Windows Server eel	84
Configuration on the Windows Server shark	85
Configuration on the UNIX Server whale	86
Example 4: Configuring An ACS Robot on a Windows Server	87
Chapter 3. Managing Media	91
Starting Media Management	92
Using the Media Management Window	92
Menus and Commands	93
Toolbars	94
Tree Pane	95
Volumes Pane	96
Volume Pools List	97
Volume Groups List	98
Robots List	99
Volumes List	100
Status Bar	104
Shortcut Menus and Commands	104
Customizing the Window	105



Allowable Media Manager Characters	105
Administering Media on Other Servers	106
Volume Database Best Practices	106
Determining the Volume Database Host for a Device	106
Managing Media on Other Servers	107
Configuring Volume Pools	108
Adding a New Volume Pool or Scratch Volume Pool	109
Adding a Scratch Volume Pool	110
Changing the Attributes of a Volume Pool	111
Changing a Volume Pool To be a Scratch Volume Pool	112
Changing the Volume Pool Assignment for a Volume	112
Deleting a Volume Pool	113
Methods Available for Injecting and Ejecting Volumes	114
Methods for Injecting Volumes into a Robot	114
When Adding New Volumes	114
When Moving Volumes	114
When Performing a Volume Configuration Update Using Robot Inventory	115
Methods for Ejecting Volumes From a Robot	115
When Moving Volumes	116
Using the Eject Volumes From Robot Command	116
Inject and Eject Functions Available by Robot Type	117
Media Ejection Timeout Periods	118
Adding New Volumes	119
Methods Available for Adding Volumes	119
Robotic Volumes (Volumes Located in a Robot)	119
Standalone Volumes (Volumes To Be Used in Standalone Drives)	120
NetBackup Catalog Backup Volumes	120
Notes on Labeling NetBackup Volumes	120
Adding Volumes Using a Robot Inventory Update	121
Adding Volumes Using the Actions Menu	122



Dialog Entries for New Volumes	123
Media Type	124
Robot	124
Find Robots	125
Number of Volumes	125
Media ID Naming Style	125
Media ID or First Media ID	126
Media Description	126
First Slot Number	126
Maximum Mounts or Maximum Cleanings	127
Volume Group	127
Volume Pool	128
Inject Volume Into Robot via the Media Access Port	129
Using the Volume Configuration Wizard	129
Learning More About the Volume Configuration Wizard	129
Starting the Volume Configuration Wizard	130
Moving Volumes	130
Moving Volumes Using the Robot Inventory Update Option	130
Moving Volumes Using the Actions Menu	131
Dialog Entries for Move Volumes	133
Volumes to Move	133
Robot	133
Find Robots	133
Volume Group	134
First Slot Number	135
Eject Volume From Robot via the Media Access Port	135
Inject Volume Into Robot via the Media Access Port	135
When to Delete Volumes	136
Deleting Volumes	136
Deleting a Volume Group	137



Ejecting Volumes From Robots (Actions Menu Command)	137
Eject Volumes Dialog Type 1	138
Eject Volumes Dialog Type 2	139
Labeling Media	139
Erasing Media Functions	140
SCSI Quick Erase	140
SCSI Long Erase	141
Erasing Media	141
Deassigning Volumes	142
Determining Which Application is Using a Volume	142
Deassigning NetBackup Volumes	143
Deassigning NetBackup Regular Backup Volumes	143
Deassigning NetBackup Catalog Backup Volumes	143
Deassigning Storage Migrator Volumes	144
Changing the Attributes for a Volume	144
Dialog Entries for Change Volumes	145
Maximum Mounts	145
Expiration Date	146
Description	147
Volume Pool	147
Number of Cleanings Remaining	147
Changing the Volume Group of a Volume	148
Exchanging Volumes	149
Exchanging a Volume and Using a New Media ID	149
Exchanging a Volume and Using the Old Media ID	150
Recycling Volumes	150
Recycling Volumes Using the Existing Media ID	150
Recycling Volumes Using a New Media ID	151

Chapter 4. Managing Media in Robots 153



Overview of Robot Inventory Operations	153
Accessing the Robot Inventory Dialog	155
Showing the Contents of a Robot	157
How Contents Reports for API Robots are Generated	158
ACS Robots	158
LMF Robots	159
RSM Robots	159
TLH Robots	159
TLM Robots	160
Comparing Robot Contents with the Volume Configuration	160
Compare Volume Configuration Reports	161
Updating the Volume Configuration for a Robot	162
When to Use Update Volume Configuration	163
When Not to Use Update Volume Configuration	164
Updating the Volume Configuration for Non-Barcoded Media	165
Procedure To Update the Volume Configuration	165
Example Update Volume Configuration Reports	167
Media Settings Tab (Advanced Options)	168
Setting Media Options	169
Properties for the Media Settings Tab	169
Media Which Have Been Removed From the Robot	170
Media Which Have Been Moved Into or Within the Robot	171
Use the Following Media ID Prefix	172
Use Barcode Rules	173
Media Type	173
Volume Pool	178
Barcode Rules Tab (Advanced Options)	179
Adding a New Barcode Rule	179
Changing a Barcode Rule	180
Deleting a Barcode Rule	181



Dialog Properties for Adding or Changing Barcode Rules	181
Media ID Generation Tab (Advanced Options)	184
Adding a New Media ID Generation Rule	185
Changing a Media ID Generation Rule	186
Deleting a Media ID Generation Rule	186
Dialog Properties for Adding or Changing Media ID Generation Rules	186
Media Type Mappings Tab (Advanced Options)	188
How the Mapping Defaults Shown on the Tab are Determined	188
Using the Tab to Change Media Type Mappings	189
Adding Mapping Entries to vm.conf	190
Default and Allowable Media Types for API Robots	190
Examples of Updating a Volume Configuration	195
Example 1: Removing a Volume from a Robot	196
Example 2: Adding Existing Standalone Volumes to a Robot	197
Example 3: Moving Existing Volumes Within a Robot	200
Example 4: Adding New Volumes to a Robot	201
Example 5: Adding Cleaning Tapes to a Robot	203
Example 6: Moving Existing Volumes Between Robots	204
Example 7: Adding Existing Volumes when Barcodes are Not Used	205
Rescanning and Updating Barcodes for a Robot	207
When to Use Rescan/Update	208
When Not to Use Rescan/Update	208
Procedure To Rescan/Update Barcodes	208
Chapter 5. Monitoring Storage Devices	211
Starting the Device Monitor	212
Using the Device Monitor Window	212
Menus and Commands	213
Toolbars	216
Global Topology Pane	217



Topology Images	217
Topology Connections	219
Selecting Topology Objects	219
Drives Status Pane	220
Managing the Drives Status Pane	224
Pending Requests Pane	224
Managing the Pending Requests Pane	227
Status Bar	227
Shortcut Menus and Commands	227
Customizing the Window	228
Allowable Media Manager Characters	229
Controlling the NetBackup Device Manager Service	230
Monitoring Devices on Other Servers	230
Changing the Operating Mode of a Drive	232
Changing Mode Example	232
Resetting a Drive	233
Drive Cleaning Functions	234
Adding or Changing a Drive Comment	236
Handling Pending Requests and Pending Actions	237
Pending Requests	237
Pending Actions	238
Resolving Pending Requests	238
Resolving a Pending Request Example (Drive in AVR mode)	240
Resolving Pending Actions	241
Resubmitting Requests	242
Denying Requests	243
Chapter 6. Shared Storage Option (SSO) Topics	245
What is SSO?	245
An Extension of Media Manager	246



A SAN is not Required for SSO	246
Sample SSO Configuration with SAN Components	246
Configuring and Verifying Your SSO Hardware	247
Using the Media Manager Device Configuration Guide	248
Configuration Tasks	248
Verifying Your Hardware is Connected and Working	249
Installing the Shared Storage Option	250
System Requirements for SSO	250
Volume Database Host (Device Allocation Host) Requirements	251
Supported Robot Types for SSO	251
Supported Media Servers for SSO	251
SSO Restrictions and Limitations	252
SSO Installation	253
Configuring SSO in NetBackup	253
Configuring SSO Devices in Media Manager	254
Device Configuration Wizard Limitations	254
Shared Drive Wizard Limitations	254
Configuring NetBackup Storage Units and Backup Policies	255
Configuring Storage Units for Each Media Server	255
Configuring a Backup Policy for Each Media Server	255
Verifying Your SSO Configuration	255
Using Media Manager with SSO	258
Using the Device Monitor with SSO	259
The Drive Status Pane	259
Changing the Operating Mode for a Shared Drive	259
Adding or Changing a Comment for a Shared Drive	259
Performing Drive Cleaning Functions for a Shared Drive	259
Adding SSO Configuration Options	260
Troubleshooting SSO Issues	260
Hardware Configuration Guidelines	260



Media Manager Configuration Guidelines	261
Operating System Help	262
Common Configuration Issues with SSO	262
Frequently Asked Questions About SSO	263
SSO Reference Topics	264
SSO-Related Terms and Concepts	264
Shared Drive	264
Backup Exec Shared Storage Option	264
Library Sharing or Robot Sharing	265
Media Servers and NetBackup SAN Media Servers	265
SSO Components in Media Manager	265
vmd/DA	265
Example SSO Configuration Showing Media Manager Components	266
Scan Host	267
Device Allocation Host	268
Appendix A. Media Manager Reference Topics	269
NetBackup Media Manager Best Practices	270
General Practices	270
Media and Device Management Domain Management	271
Media Management	271
Device Management	272
Performance and Troubleshooting	273
Other Best Practices	274
NetBackup and Media Manager Databases	274
Media Manager Volume Database	275
Media Catalog	275
NetBackup Catalogs	275
Device Databases	276
Robot Overview	276



Media Manager Robot Types	276
Media Manager Media Types	277
Alternate Media Types	279
Robot Attributes	279
Table-Driven Robotics	291
Robotic Test Utilities	292
Robotic Processes	292
Process Example	293
Processes by Robot Type	294
Frequently Asked Questions About Device Discovery	295
How NetBackup Uses SCSI Reserve/Release	298
Background Topics	299
NetBackup Releases Prior to NetBackup 4.5	299
NetBackup 4.5 and Later Releases	299
SCSI Reserve/Release Commands	299
How NetBackup Uses SCSI Reserve/Release Commands	300
Issuing the Reserve	300
Checking for Data Loss	301
Checking for Tape/Driver Configuration Errors	302
Issuing the Release	303
SCSI Reserve/Release Logging and Conflict Notification	303
Issuing Reset Commands to Break a Reservation	304
Controlling SCSI Reserve/Release	305
SCSI Reserve/Release Requirements and Limitations	306
Correlating Device Files to Physical Drives When Adding Drives	306
On Windows Hosts	307
On UNIX Hosts	308
Drive Cleaning	309
Available Types of Cleaning	310
Reactive Cleaning (TapeAlert)	310



Requirements for Using TapeAlert with Media Manager	311
TapeAlert and Media Manager	311
TapeAlert and Frequency-Based Cleaning	311
Library-Based Cleaning	312
Frequency-Based Cleaning	312
Frequency-Based Cleaning Limitations	313
Managing Frequency-Based Cleaning	313
Operator-Initiated Cleaning	313
Using a Cleaning Tape	314
Volume Pools and Volume Groups	314
Volume Pools	315
Volume Groups	315
Rules for Assigning Volume Groups	316
Volume Pool and Volume Group Example	316
Scratch Volume Pools	318
Scratch Pool Example	318
Scratch Pool Usage	319
Moving Volumes	320
Move Operations	320
Physical and Logical Moves	320
Barcodes	321
Barcode Advantages	321
Barcode Best Practices	322
Barcode Rules	323
Media Manager Actions for Barcodes	323
Example Barcode Rules	324
Media ID Generation Rules	325
Using the Physical Inventory Utility for Non-Barcoded Media	325
Why Use vmphyinv?	326
Features	326



Requirements and Restrictions	327
When to Use vmphyinv	327
How vmphyinv Performs a Physical Inventory	328
Obtaining a List of Drives Used to Mount the Media	329
Obtaining a List of Media to be Mounted	329
Mounting Media and Reading the Tape Header	330
Updating the Media Manager Volume Database	332
Making Changes to Your Hardware Configuration	335
Replacing Devices in a SSO Configuration	335
Decommissioning a Media Server	336
Labeling Media	338
Pre-labeling of Media	338
Mounting and Unmounting of Media	338
Suspending Media Or Downing Devices	339
How Media Manager Selects a Drive for a Robotic Mount Request	339
Controlling Hardware Compression	340
How NetBackup Selects Media in Robots	340
Spanning Media	341
How NetBackup Selects Media in Standalone Drives	342
Media Selection Using Standalone Drive Extensions	342
Disabling Standalone Drive Extensions	343
Spanning Media	343
Keeping Standalone Drives in the Ready State	344
Media Formats	344
Non-QIC Tape Format	345
QIC Tape Format	345
Optical Media Format	345
Fragmented Backups	345
Multiplexing Format	346
Spanning Tapes	346



Media Manager Security	347
NetBackup Authentication/Authorization	347
Media Manager Authentication/Authorization	348
No vm.conf Entry Present	348
vm.conf Entry is Present	349
Media Manager Security (Using SERVER Configuration Entries)	349
Possible NetBackup and Media Manager Conflicts	350
Media Manager Enhanced Authorization	350
Supported Commands and Daemons	351
Allowing Enhanced Authorization	352
Enabling Robot Authorization	352
Administrators Quick Reference	352
Media Manager Commands	352
Media Manager Log Files	355
The Media Manager Configuration File (vm.conf)	355
ACS Media Mapping	357
Adjacent LSM Specification for ACS Robots	357
API Robot Barcode Rule Enable	358
Authorization Required	359
Automatically Empty Robot MAP	359
AVRD Scan Delay	359
AVRD Pending Status Delay	360
Backup Exec - Mapping Media Types	360
Backup Exec - Mapping Robots	361
Cleaning Drives Timeout	361
Client Port Range	362
Connect to Firewall Options	362
DAS Client Name	363
Days To Keep Debug Logs	363
Device Host Entries	364



Disable Automatic Path Remapping	364
Disallow Non-NDMP Request on NDMP Drive	364
Do Not Eject Standalone Tapes	365
Enable Robot Authorization	365
Inventory Robot Filter	365
Media Access Port Default for ACS Robots	366
Media ID Generation	367
Media ID Prefix	368
Not Allowing a Host To Manage Databases	368
Preferred Group	368
Prevent Media Removal (for TL8 Robots)	369
Random Port Numbers	369
Cluster Name, Media Manager Name, Required Network Interface	370
Return Media to the Scratch Pool	371
RSM Media Mapping	371
Scratch Pool Configuration	371
Server Entry	372
SSO DA Re-register Interval	372
SSO DA Retry Time	372
SSO Host Name	373
SSO Scan Ability Factor	373
TLH Media Mapping	374
TLM Media Mapping	374
Vault Media Description Reset	374
Verbose Message Logging	375
Example vm.conf File	375
Appendix B. STK Automated Cartridge System (ACS)	377
Sample ACS Configuration	378
Media Requests	380



Configuring ACS Robotic Control	380
Configuring ACS Drives	380
Configuring Shared ACS Drives	382
Using the STK SN6000	383
Should SN6000 Drives Be Configured as Shared Drives?	384
Hosts Connected To a Single Port	384
Hosts Connected To Different Ports	384
Adding Volumes	385
Removing Volumes	385
Removing Volumes Using the STK Utility	386
Removing Volumes Using Media Manager	386
Robot Inventory Operations	386
Advanced ACS Robot Topics	388
ACS Process (acsd)	388
ACS Robotic Test Utility (acstest)	388
Robotic Inventory Filtering	389
Inventory Filtering Example	389
Appendix C. Microsoft Removable Storage Manager (RSM)	391
Media Manager and Microsoft RSM	391
Considerations When Using Microsoft RSM	391
The Microsoft RSM Interface	392
Media Requests Involving an RSM Robot	392
Configuring RSM Robotic Control	393
Configuring RSM Drives in Media Manager	393
Verifying a Configuration	393
Activating a Configuration	394
Adding Volumes	394
Removing Volumes	396
Robot Inventory Operations	396



Appendix D. IBM Automated Tape Library (ATL)	399
Sample TLH Configurations	399
Media Requests for a TLH Robot	402
Configuring Robotic Control	403
Robotic Control on a Windows System	403
Determine the Library Name	403
Verify Library Communications	404
Configure the Robotic Library Name	405
Configuring Drives for TLH Robots	405
Cleaning Drives	406
Adding Volumes	407
Removing Volumes	407
Robot Inventory Operations	408
Robotic Inventory Filtering	409
 Appendix E. ADIC Distributed AML Server/Scalar Distributed Library Controller	 411
Sample TLM Configuration	411
Media Requests Involving a TLM Robot	413
Configuring TLM Robotic Control	413
Configuring TLM Drives on a DAS/SDLC Server	413
Installing ADIC Software for the Client Component	414
Configuring the DAS/SDLC Client Name	414
Allocating TLM Drives on a DAS Server	415
Configuring TLM Drives on a SDLC Server	416
Configuring TLM Drives in Media Manager	416
Configuring Shared TLM Drives	417
Configuring the ADIC DAS Server	417
Configuring the ADIC SDLC Server	418
Using the Device Configuration Wizard in Media Manager	419
Providing Common Access to Volumes	420

Adding Volumes	420
Removing Volumes	421
Robot Inventory Operations	422
Index	425





Preface

This guide describes using the NetBackup Administration Console to manage Media Manager software and its components on a Windows server. See the NetBackup release notes for information about the supported Windows server platforms for NetBackup.

Media Manager is the component of VERITAS NetBackup™ that is used to configure and manage media, drives, and robots that are used to store and retrieve your backup data.

This guide assumes you are familiar with the operating system of the server on which NetBackup and Media Manager is installed and Windows systems in general.

What Is In This Guide?

This guide contains the following chapters:

- ◆ “Introduction to Media Manager” on page 1 provides an overview of Media Manager.
- ◆ “Configuring Storage Devices” on page 17 explains how to attach storage devices and configure Media Manager to use them.
- ◆ “Managing Media” on page 91 contains topics on configuring Media Manager to use the media (volumes and volume pools) that Media Manager requires to store backups.
- ◆ “Managing Media in Robots” on page 153 explains how to configure Media Manager to use and manage the media in robots (using robot inventory).
- ◆ “Monitoring Storage Devices” on page 211 explains tasks such as monitoring drives and media mount requests, and assigning a requested volume to a drive.
- ◆ “Shared Storage Option (SSO) Topics” on page 245 provides information on installing, configuring, and using the NetBackup Shared Storage Option on UNIX and Windows-based servers. SSO is an extension to tape drive allocation and configuration for NetBackup Media Manager.

In addition to these chapters, this guide contains the following appendixes and an index.

- ◆ “Media Manager Reference Topics” on page 269 provides background information on important Media Manager features and concepts.



- ◆ “STK Automated Cartridge System (ACS)” on page 377 explains how Media Manager works with StorageTek (STK) Automated Cartridge System robots.
- ◆ “Microsoft Removable Storage Manager (RSM)” on page 391 explains how Media Manager communicates with robots under the control of Microsoft Removable Storage Manager.
- ◆ “IBM Automated Tape Library (ATL)” on page 399 explains how Media Manager supports robots controlled by the IBM Automated Tape Library.
- ◆ “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 411 explains how Media Manager works with the EMASS Distributed AML Server to control Tape Library Multimedia (TLM) robots, including the Grau AML Library.

How To Use This Guide

Keep the following points in mind when using this guide.

- ◆ This guide is intended for use with NetBackup Server and NetBackup Enterprise Server. For readability in this guide, the term NetBackup refers to both NetBackup server types unless specifically noted.
- ◆ Portions of this guide apply only to specific robot types (for example, API, RSM, or optical robots), server platforms (UNIX or Windows), or NetBackup server type (for example, NetBackup Enterprise Server).

These topics are identified with the use of italics as in the following example:

This step is only applicable for NetBackup Enterprise Server.

- ◆ This guide is intended primarily for the system administrator, who will probably want to read every chapter.

An operator should read the chapter “Monitoring Storage Devices” on page 211 and may have an interest in reading the Media Manager overview in the chapter “Introduction to Media Manager” on page 1.

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Technical Support Web Site

The VERITAS Support Web site allows you to:

- ◆ obtain updated information about NetBackup, including system requirements, supported platforms, and supported peripherals



- ◆ contact the VERITAS Technical Support staff and post questions to them
- ◆ get the latest patches, upgrades, and utilities
- ◆ view the NetBackup Frequently Asked Questions (FAQ) page
- ◆ search the knowledge base for answers to technical support questions
- ◆ receive automatic notice of product updates
- ◆ find out about NetBackup training
- ◆ read current white papers related to NetBackup

The address for the VERITAS Technical Support Web site follows:

- ◆ <http://support.veritas.com>

Subscribing to VERITAS Email Notification Service

Subscribe to the VERITAS Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.

Go to <http://support.veritas.com>. Select a product and click “E-mail Notifications” on the right side of the page. Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.

Accessing VERITAS Telephone Support

Telephone support for NetBackup is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Technical Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

▼ To locate the telephone support directory on the VERITAS web site

1. Open <http://support.veritas.com> in your web browser.
2. Click the **Phone Support** icon. A page that contains VERITAS support numbers from around the world appears.



Accessing VERITAS E-mail Support

▼ To contact support using E-mail on the VERITAS web site

1. Open <http://support.veritas.com> in your web browser.
2. Click the **E-mail Support** icon. A brief electronic form will appear and prompt you to:
 - ◆ Select a language of your preference
 - ◆ Select a product and a platform
 - ◆ Associate your message to an existing technical support case
 - ◆ Provide additional contact and product information, and your message
3. Click **Send Message**.

Contacting VERITAS Licensing

For license information call 1-800-634-4747 option 3, fax 1-650-527-0952, or e-mail amercustomercare@veritas.com.

NetBackup Manuals

The following manuals, along with the online help, comprise the NetBackup documentation set:

For a complete list of related documents, see the NetBackup release notes. Depending on your configuration, other documents may also be required.

- ◆ *VERITAS NetBackup Commands for UNIX*

NetBackup_Commands_UNIX.pdf

Describes NetBackup commands and processes that can be executed from a UNIX command line.

- ◆ *VERITAS NetBackup Commands for Windows*

NetBackup_Commands_Windows.pdf

Describes NetBackup commands and processes that can be executed from a Windows command prompt.

- ◆ *VERITAS NetBackup Global Data Manager System Administrator's Guide for UNIX and Windows*

NetBackup_AdminGuide_GDM.pdf



Explains how to install, configure, and use Global Data Manager (GDM) for NetBackup products on UNIX and Windows-based operating systems.

- ◆ *VERITAS NetBackup Installation Guide for UNIX*

NetBackup_Install_UNIX.pdf

Explains how to install NetBackup software on UNIX-based platforms.

- ◆ *VERITAS NetBackup Installation Guide for Windows*

NetBackup_Install_Windows.pdf

Explains how to install NetBackup software on Windows-based platforms.

- ◆ *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX and Windows*

MediaMgr_DeviceConfig_Guide.pdf

Explains how to add device drivers and perform other system-level configurations for storage devices and media servers (or SAN media servers) that are supported by NetBackup Media Manager.

- ◆ *VERITAS NetBackup Media Manager System Administrator's Guide for UNIX*

MediaMgr_AdminGuide_Unix.pdf

Explains how to configure and manage the storage devices and media on UNIX servers running NetBackup. Media Manager is part of NetBackup.

- ◆ *VERITAS NetBackup for NDMP System Administrator's Guide*

NetBackup_AdminGuide_NDMP.pdf

Explains how to install, configure, and use NetBackup for NDMP to control backups on an NDMP host.

- ◆ *VERITAS NetBackup Release Notes for UNIX and Windows*

NetBackup_Release_Notes.pdf

Provides important information about NetBackup on UNIX- and Windows-based servers, such as the platforms and operating systems that are supported and operating notes that may not be in the NetBackup manuals or the online help.

- ◆ *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I*

NetBackup_AdminGuideI_UNIXServer.pdf

Explains how to configure and manage NetBackup on a UNIX server, including managing storage units, backup policies, catalogs and host properties.

- ◆ *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II*

NetBackup_AdminGuideII_UNIXServer.pdf



Explains additional NetBackup features such as access control and enhanced authorization and authentication. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

- ◆ *VERITAS NetBackup System Administrator's Guide for Windows, Volume I*

NetBackup_AdminGuideI_WinServer.pdf

Explains how to configure and manage NetBackup on a Windows server, including managing storage units, backup policies, catalogs and host properties.

- ◆ *VERITAS NetBackup System Administrator's Guide for Windows, Volume II*

NetBackup_AdminGuideII_WinServer.pdf

Explains additional NetBackup features such as access control and enhanced authorization and authentication. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

- ◆ *VERITAS NetBackup Troubleshooting Guide for UNIX and Windows*

NetBackup_Troubleshoot_Guide.pdf

Provides troubleshooting information for UNIX- and Windows-based NetBackup products, including Media Manager.

- ◆ *VERITAS NetBackup Vault System Administrator's Guide for UNIX and Windows*

NetBackup_AdminGuide_Vault.pdf

Describes how to configure and use logical vaults and profiles to duplicate backups, perform catalog backups, eject media, and generate reports.

- ◆ *VERITAS Security Services(tm) Version 4.0 Administrator's Guide*

VxSS_AdminGuide.pdf on the VERITAS Security Services CD-ROM.

Explains how to configure and manage core security mechanisms, including authentication, protected communications, and authorization.

Related Resources

Glossary

If you encounter unfamiliar terminology, consult the NetBackup online glossary. The glossary contains terms and definitions for NetBackup and all additional NetBackup options and agents.

The NetBackup online glossary is included in the NetBackup help file.



▼ **To access the NetBackup online glossary**

1. In the NetBackup Administration Console, click **Help** > **Help Topics**.
2. Click the **Contents** tab.
3. Click **Glossary of NetBackup Terms**.

Use the scroll function to navigate through the glossary.

Accessibility Features

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- ◆ Support for assistive technologies such as screen readers and voice input (Windows servers only)
- ◆ Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the *NetBackup System Administrator's Guide for Windows, Volume I* or the *NetBackup System Administrator's Guide for UNIX, Volume I*.

Conventions

The following conventions apply throughout the documentation set.

Product-Specific Conventions

The following term is used in the NetBackup 5.1 documentation to increase readability while maintaining technical accuracy.

- ◆ Microsoft Windows, Windows

Terms used to describe a specific product or operating system developed by Microsoft, Inc. Some examples you may encounter in NetBackup documentation are, Windows servers, Windows 2000, Windows Server 2003, Windows clients, Windows platforms, or Windows GUI.



When Windows or Windows servers is used in the documentation, it refers to all of the currently supported Windows operating systems. When a specific Windows product is identified in the documentation, only that particular product is valid in that instance.

For a complete list of Windows operating systems and platforms that NetBackup supports, refer to the *NetBackup Release Notes for UNIX and Windows* or go to the VERITAS support web site at <http://www.support.veritas.com>.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the Password field.
<i>Italics</i>	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace <i>filename</i> with the name of your file. Do <i>not</i> use file names that contain spaces. This font is also used to highlight NetBackup server-specific or operating system-specific differences. For example: <i>This step is only applicable for NetBackup Enterprise Server.</i>
Code	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip	Used for nice-to-know information, like a shortcut.
------------	---

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Ignore a caution at your own risk.

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets []

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

```
command arg1 | arg2
```

In this example, the user can use either the *arg1* or *arg2* variable.

Navigating Multiple Menu Levels

When navigating multiple menu levels, a greater-than sign (>) is used to indicate a continued action.

The following example shows how the > is used to condense a series of menu selections into one step:

❖ Select **Start > Programs > VERITAS NetBackup > NetBackup Administration Console**.

The corresponding actions could be described in more steps as follows:

1. Click **Start** in the task bar.
2. Move your cursor to **Programs**.
3. Move your cursor to the right and highlight **VERITAS NetBackup**.
4. Move your cursor to the right. First highlight and then click **NetBackup Administration Console**.





Introduction to Media Manager

Media Manager provides control of tape storage devices and tracks the location of the removable media that are used in these devices. Media Manager is an integral part of NetBackup and is installed with it on every server where NetBackup is running.

This chapter provides an overview of Media Manager and contains the following topics:

- ◆ Media Manager Terminology
- ◆ Media Manager Features
- ◆ Media Manager Hosts
- ◆ Media Manager Storage Devices
- ◆ Media Manager Volumes
- ◆ Media Manager Administration Utilities
- ◆ Device and Media Configuration Overview
- ◆ Security Issues

When you are familiar with the features and the administration of NetBackup and Media Manager described in this guide, you should review the list of recommended practices. See “NetBackup Media Manager Best Practices” on page 270.

Media Manager Terminology

The following table contains key terms that are used in Media Manager documentation and help.



For the complete NetBackup glossary of terms, refer to the glossary that is included in the NetBackup help file. This glossary contains terms and definitions for NetBackup, and all additional NetBackup options and agents.

Term	Description
<i>ADAMM database</i>	(Advanced Device and Media Management). The Backup Exec database that maintains device and media information.
<i>API robots</i>	<p>A group of Media Manager robot types where the robot-vendor software or the operating system (in the case of RSM robots) manage their own media.</p> <p>The following are the supported API robots for the NetBackup server types on UNIX servers and Microsoft Windows servers:</p> <ul style="list-style-type: none">♦ NetBackup Server for Windows: RSM.♦ NetBackup Enterprise Server for Windows: ACS, RSM, TLH, and TLM.♦ NetBackup Server for UNIX: None.♦ NetBackup Enterprise Server for UNIX: ACS, LMF, TLH, and TLM.
<i>avrd</i>	The Media Manager automatic volume recognition daemon on UNIX and process on Windows servers.
<i>barcode</i>	A label attached to the media that associates the media to its slot location in a robot. The alphanumeric barcode is also usually included on the magnetic label that is written on the media.
<i>barcode rule</i>	A rule that specifies criteria for assigning attributes to new robotic volumes.
<i>device host</i>	A host where a drive or robotic control is attached or is defined, that also has Media Manager installed.
<i>drive status</i>	A status indicating the condition or state of a drive.
<i>global device database</i>	<p>A database that is the repository for global device configuration information. This information is used by Media Manager to automate device configuration and is the basis for the device configuration presented in the GUIs.</p> <p>The <i>global device database host</i> is the host where this database is located.</p>
<i>insert</i>	A volume is physically placed in a robot without using an add or move option to update the volume database.



Term	Description
<i>labeled volume</i>	A volume with a recorded media ID (that is, the volume was labeled by NetBackup or Backup Exec).
<i>library sharing</i>	<i>Applies only to NetBackup Enterprise Server.</i> Allows different drives in a robot to be connected to different hosts. Also known as <i>robot sharing</i> or <i>remote robot control</i> .
<i>ltid</i>	The Media Manager device daemon on UNIX and the NetBackup Device Manager service on Windows.
<i>Media and Device Management (MDM) domain</i>	<i>Applies only to NetBackup Enterprise Server.</i> A domain that includes all of the servers listed in the global device database (this domain also includes the global device database host). The <i>Media and Device Management domain server</i> is the host where the Media Manager volume database, volume pool database, barcode rule database, and global device database for a domain are located.
<i>media ID</i>	An identifier used by Media Manager to track media.
<i>media server</i>	A server that can back up its own data or other clients on the network as well to devices.
<i>media type</i>	A Media Manager classification of tape or optical media with differing physical characteristics.
<i>mount request</i>	A request for a volume that is displayed in the Pending Requests pane. This means to make a volume available for reading or writing by placing it in an appropriate drive and then assigning the associated request to that drive.
<i>NetBackup authentication</i>	A NetBackup security level that verifies NetBackup client to server, or server to server access. Authentication also controls access to the services available on that host.
<i>NetBackup authorization</i>	A NetBackup security level that verifies if a NetBackup user (or groups of users) has permission to use the services available on that host. Authorization provides additional security over the security provided by authentication.
<i>NetBackup media database</i>	A database that contains media attributes (like media state and image expiration date) for media assigned to a particular NetBackup server. There is a media database located on each server that has (or had) drives connected to it and is also running NetBackup.



Term	Description
<i>no rewind on close</i>	A device name that applies to tape drives attached to (or controlled by) UNIX devices. This type of device remains at its current position on a close operation.
<i>operator</i>	A person responsible for performing manual intervention, for example mounting tapes.
<i>pending actions</i>	Special requests for operator assistance to complete a tape mount request, when the request causes an error.
<i>residence information or residence</i>	Attributes in the Media Manager volume database. This information shows the robotic location and includes the robot host, robot type, robot number, and slot location.
<i>robot control host</i>	<i>Applies only to NetBackup Enterprise Server.</i> The host that is providing the robotic control for a robot.
<i>robot number</i>	A unique, logical identification number of a robot.
<i>robot type</i>	Media Manager classification of robots, according to one of the following: the physical characteristics of the robot, the media type commonly used by that class of robots, or the communication methods used by the underlying robotics.
<i>robotic control path</i>	The control path to a robot through a SCSI connection.
<i>robotic library or robot</i>	A peripheral device that contains a mechanism for the automated mounting and dismounting of media in tape or optical disk drives. A robot may also be called a robotic library, media changer, automated library, jukebox, or tape stacker.
<i>SAN media server</i>	A server that can only back up its own data to devices. Backing up of data residing on other clients on a network is not allowed.
<i>shared drive</i>	<i>Applies only to NetBackup Enterprise Server.</i> A tape drive that is shared among hosts, when SSO is installed.
<i>Shared Storage Option (SSO)</i>	<i>Applies only to NetBackup Enterprise Server.</i> A NetBackup software option that allows individual tape drives (stand-alone or in a robotic library) to be dynamically shared between multiple NetBackup media servers (or SAN media servers).
<i>standalone drive</i>	A drive that is not in a robotic library.



Term	Description
<i>system administrator</i>	A person with typical UNIX or Windows administrator privileges and responsibilities.
<i>unlabeled volume</i>	A volume that does not have recorded media IDs.
<i>user</i>	A person or application (for example, NetBackup) that initiates Media Manager requests.
<i>vmd</i>	The Media Manager volume daemon on UNIX and the NetBackup Volume Manager service on Windows.
<i>volume database</i>	<p>The database that is the repository for Media Manager volume configuration information.</p> <p>The <i>volume database host</i> is a Media Manager host where this database is located.</p>
<i>volume group</i>	A logical grouping that identifies a set of volumes that reside at the same physical location.
<i>volume pool</i>	A logical grouping that identifies a set of volumes by their usage.

Media Manager Features

◆ Robotic and Standalone Drive Support

In Media Manager, a robot is a peripheral device for the automated mounting and dismounting of volumes in tape drives. A standalone drive is a drive that is not associated with a robot.

Media Manager supports a wide range of robots and automates the handling of volumes in these devices. Except for initial setup and loading of tapes or an equipment failure, manual intervention is not required.

Visit the VERITAS support web site for a list of the platforms and peripherals that Media Manager supports.

Media handling in standalone drives is also automated to the extent that Media Manager automatically uses the tape that is in a drive, if it is required by NetBackup.

Capability to perform automated drive cleaning, based on the TapeAlert feature or a frequency-based cleaning schedule. Cleaning tapes that are configured incorrectly are also recognized.



Media Manager running on NetBackup Windows servers does not support optical disk storage devices.

- ◆ **Media Location Tracking**

Media Manager maintains a volume database that shows the location of all media (for example, the robot and slot). This information permits Media Manager to find media when it is required to satisfy a request.

- ◆ **Media Statistics Tracking**

Media Manager keeps a record of statistics that are useful in tracking the useful life of media (for example, an expiration date and the number of times that media has been mounted).

- ◆ **Security**

Media Manager `vmmd` security works in conjunction with NetBackup authentication/authorization security to control user access to `vmmd` (the NetBackup Volume Manager service).

The topic, “Media Manager Security” on page 347 explains important security features, including the following topics:

- ◆ The relationship with NetBackup authentication/authorization security.
- ◆ Controlling user access to `vmmd` (the Media Manager volume daemon).
- ◆ Controlling user access to Media Manager robotic daemons and services.

- ◆ **Robot Inventory and Update**

Media Manager can inventory a robot, provide reports, and update the volume database to match the results of the inventory. This simplifies administration, by permitting you to quickly determine the contents of a robot. This also automates the configuration process.

Media Manager can also inventory a robotic library that does not support barcodes or that contains volumes that do not have readable barcodes. In these cases, you use the physical inventory utility (`vmphysinv`).

- ◆ **Automatic Volume Recognition**

Media Manager compares the media IDs on media with media IDs that are requested and then assigns the correct media to requests. This is an essential part of providing hands-off operation for both robots and standalone drives.

- ◆ **Automatic Scanning of Media Labels**

Media Manager scans the labels of media that are in drives and displays them in the Device Monitor. This is useful if you want to know whether a certain drive contains a particular volume.

- ◆ **Volume Pools**



During configuration, you can assign media to pools that are reserved for specific uses. For example, media can be reserved for backups of specific departments. It is also possible to create a scratch pool from which media can be allocated to other pools as they are needed.

A pool named NetBackup is created by default and, unless you specify otherwise in the class or schedule, all NetBackup backup images go to media in the NetBackup pool. You can create other volume pools as desired. Other volume pools that are created by default are named None and DataStore.

- ◆ **Volume Groups**

When media is added, it is assigned (or you can assign) a volume group name that corresponds to the physical location of the media (for example, the robot that has the media). This is useful for administering groups of volumes and for tracking location. For example, when media is taken to offsite storage, you can move the media to specific standalone groups.

- ◆ **Graphical User Interfaces for Media and Device Management**

The following interfaces (or tree nodes) are available from the NetBackup Administration Console.

- ◆ **Device Monitor** shows the current status of all drives and allows you to easily change the state of a drive. For example, it is possible to set a drive to DOWN to prevent its use by Media Manager or reset it to clear a hang condition. You can also assign requests to drives in those instances when assignment does not occur automatically.
- ◆ **Media** provides intuitive and easy-to-use methods for managing your media, volume pools, and volume groups.
- ◆ **Devices** provides intuitive and easy-to-use methods for managing your device hosts, robots, drives, and shared drives.

Media Manager Hosts

In the NetBackup Administration Console and in this guide, a Media Manager host (or server) is a UNIX or Microsoft Windows server that has NetBackup and Media Manager software installed. Media Manager software is automatically installed as part of the installation of NetBackup software.

Key Media Manager hosts are described in the following topics.



Master Servers

NetBackup and Media Manager support both master server and media servers. A master server manages the NetBackup backups, archives, and restores. Media servers typically provide additional storage by allowing NetBackup to use the storage devices that are attached.

A master server has Media Manager software installed.

The following point applies only to NetBackup Server.

NetBackup master and media server software are both installed on the same host. This is the host where NetBackup is installed. In this case, the host acts as both a master and a media server. All related databases are also located on that host.

The following point applies only to NetBackup Enterprise Server.

You can have multiple master and media servers in your configuration. Typically a master server controls multiple media servers. You should manage your media servers from the master server point of view.

Media Servers

A host with Media Manager software installed and devices attached is termed a media server. The use of Media servers can increase system performance by distributing network loads.

Media servers can also be referred to as device hosts. Regular media servers are licensed by VERITAS, and can back up their own data or data from other network clients. Also see “SAN Media Servers” on page 8.

The following points apply only to NetBackup Enterprise Server.

You can have multiple media servers in your configuration.

A media server can also just be a host that provides the robotic control for a robot (known as a robot control host).

SAN Media Servers

This is a NetBackup Enterprise Server topic.

VERITAS also licenses SAN media servers that can only back up their own data to shared drives—no backing up of data residing on other clients is allowed.

Volume Database Host

A volume database host is a Media Manager host where the volume database is located. This database is the repository for all Media Manager volume configuration information about the media in storage devices.

The following point applies only to NetBackup Server.

The Media Manager volume database is located on the host where NetBackup is installed.

The following points apply only to NetBackup Enterprise Server.

All servers where Media Manager is installed (even if the server does not have any drives or robots attached) can have volume databases and can contain volume information. VERITAS recommends that you centralize the information on one Media Manager host (this host is usually the NetBackup master server).

Caution Although it is possible to maintain separate volume databases on multiple hosts, administration of these databases is more difficult, as is merging the databases later. The `vmdb_merge` command can be used to merge volume, pool, and media databases. See the NetBackup commands guide for details.

Also, shared drive (SSO) configurations require that one volume database host is used for all servers where a shared drive is configured.

There should be only one volume database host per global device database host (see “Global Device Database Host” on page 9), and both of these key databases should be located on the same server. This server is known as the Media and Device Management Domain (MDM Domain) server.

Global Device Database Host

This is a NetBackup Enterprise Server topic.

The global device database host is a Media Manager host where the global device database is located. This database is the repository for Media Manager device configuration information.

The following methods are typically used to configure devices:

- ◆ Device discovery (Device Configuration wizard)
- ◆ Auto-configuration (Device Configuration wizard)
- ◆ Manual configuration (using the NetBackup Administration Console or `tpconfig`)

For device configuration to work properly (particularly where devices are connected to many servers) a single host must serve as the repository for this global device configuration information.



Also, there should be only one volume database host (see “Volume Database Host” on page 9) per global device database host and both of these key databases should be located on the same server. This server is known as the Media and Device Management Domain (MDM Domain) server.

When you install NetBackup, the default option is to have the master server configured to be the global device database host. If your environment contains multiple master servers, you can designate a different server to be your global device database host during the installation.

The `tpautoconf` command has options to preview and merge existing device databases. See the NetBackup commands guide for details.

Media Manager Storage Devices

Drives and robots must be added to the Media Manager configuration before NetBackup can use them. Devices can be added using either of the following methods with the NetBackup Administration Console:

- ◆ The Device Configuration Wizard (this is the recommended method). This wizard is available from the right pane of the NetBackup Administration Console, if you have selected **Media and Device Management** in the tree pane.
- ◆ Using **Devices** (use the new robot and new drive menu items).

You may also use the `tpconfig` command from the Windows command prompt to add devices (see the NetBackup commands for Windows reference guide).

Media Manager Volumes

The tapes that Media Manager uses are referred to as volumes in NetBackup. Volumes are assigned media IDs and other attributes that are required for tracking and management. You can do the assignment manually or let Media Manager do it automatically.

These methods are explained in the following chapters:

- ◆ “Managing Media” on page 91.
- ◆ “Managing Media in Robots” on page 153.

The following are examples of the events that occur when NetBackup requests a volume for a backup:

- ◆ If NetBackup requests an existing volume, Media Manager locates the volume and performs the steps necessary to have the volume mounted in a drive.

- ◆ If NetBackup requests a new volume, Media Manager looks for a volume of the requested density and assigns it to NetBackup before mounting it in a drive. Once a volume is assigned to NetBackup, other applications cannot use it until NetBackup no longer needs the backups on the volume.
- ◆ If Media Manager does not have a record of a volume suitable for the request, an error occurs and you must configure a volume to use before the operation can proceed.

Mounting and Using Volumes

Mounting a volume consists of the steps necessary to make it available for reading or writing data. After finding a volume, Media Manager mounts it as follows:

- ◆ If the volume is in a robot, Media Manager issues the commands that move the volume to a drive, position the heads to the beginning of the volume, and assign it to the request. No manual intervention is required.
- ◆ If the volume happens to be in a standalone drive and has been requested by NetBackup, Media Manager automatically mounts and assigns it. Again, no manual intervention is required.
- ◆ If the volume is not in a robot or a standalone drive, Media Manager displays a pending request in the Device Monitor. The operator must then find the volume and do one of the following:
 - ◆ Check the Device Monitor to find a suitable drive, and mount the requested volume in that drive.
 - ◆ Move the volume into the robot and update the volume configuration to reflect the correct location for the media, and resubmit the request.
- ◆ The administrator or operator can then find the required volume, insert it into the drive, and assign the drive to the request with the Device Monitor. This situation will exist, for example, if the requested volume happens to be off site.

In robots that have barcode readers, Media Manager verifies the barcode to ensure that the robot loads the correct volume. If the barcode on the volume does not match the barcode in the Media Manager volume database, it is considered an error and the operation is stopped.

Note Media Manager is involved only in backups that are stored on removable media. If the defined NetBackup storage unit is on magnetic disk, NetBackup sends the backup to the file path specified during configuration of the storage unit and records the location in the NetBackup media database. Media Manager, in this instance, does not have a record of the storage location.



Media Manager Administration Utilities

Utilities for managing media and devices are available in the NetBackup Administration Console.

There are also some operations that may require you to use a command from the Windows command prompt (see the NetBackup commands for Windows reference guide). These operations are not required in the normal use of NetBackup.

Starting the Media Manager Administration Utilities

▼ To Start the administration utilities

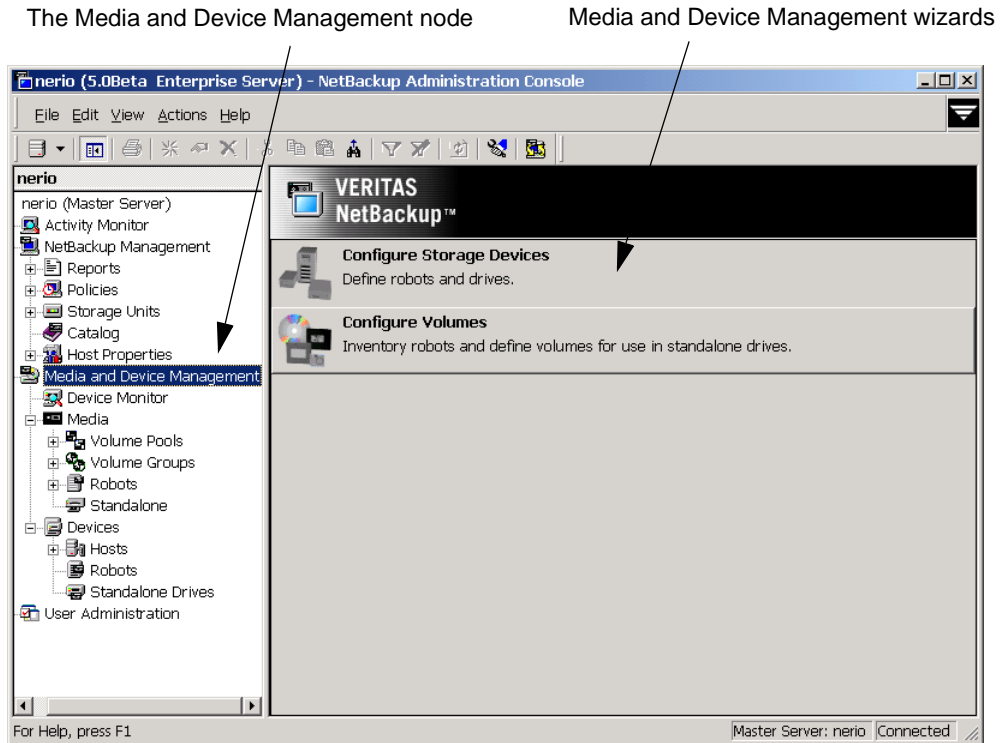
1. Log on to a Windows workstation as a member of the Administrators group.
2. From **Start > Programs**, select **VERITAS NetBackup > NetBackup Administration Console**. The NetBackup Administration Console appears on your workstation.

The NetBackup Administration Console is the starting point for administering NetBackup. The left pane of the console window has a node for each major area of NetBackup administration (including nodes for optional VERITAS software).

3. Click the **Media and Device Management** node. This node contains the Media Manager utilities.

The right pane initially contains the key NetBackup wizards that apply to this node. The following figure shows these Media Manager wizards. These wizards have the following links:

- ◆ **Configure Storage Devices**
- ◆ **Configure Volumes**



4. Expand **Media and Device Management** to view the additional Media Manager nodes. Clicking a node displays information related to that node in the right pane. The menus and buttons contain commands relevant to each selected node.

Note See the NetBackup system administrator's guide for Windows servers for details on the other NetBackup Administration Console nodes, other NetBackup administration utilities, and menu commands.

- ◆ Click **Device Monitor**. The device monitor has commands for monitoring the operation of storage devices.
"Monitoring Storage Devices" on page 211 explains how to use the Device Monitor.
- ◆ Click **Media**. This node has commands for managing media.
"Managing Media" on page 91 and "Managing Media in Robots" on page 153 explain how to manage your media.
- ◆ Click **Devices**. This node has commands for configuring and managing hosts, robots, drives, and shared drives.



“Configuring Storage Devices” on page 17 explains how to configure devices for Media Manager use.

Shortcut Menus

Pressing the right-mouse button while the pointer is over sections of the NetBackup Administration Console, displays shortcut menus. Different menus appear depending on where your pointer is positioned.

Device and Media Configuration Overview

The following summarizes the steps for configuring storage devices and media. Complete your NetBackup policy and storage unit configuration as explained in the NetBackup system administrator’s guide for Windows servers.

▼ To configure devices and media

1. Install NetBackup software by following the instructions in the installation program. Media Manager is installed as a part of NetBackup.
2. Use the Device Configuration Wizard (select **Configure Storage Devices** in the right pane of the NetBackup Administration Console) to configure your robots and non-shared drives. For more information, see “The Device Configuration Wizard” on page 44.

To manually configure devices not supported by this wizard, you must use the menus of the **Devices** node. See “Configuring Storage Devices” on page 17.

3. *This step applies only to NetBackup Enterprise Server.*

To configure shared drives (SSO), you can use the Device Configuration Wizard or the the Shared Drive wizard. For more information, see “Adding Shared Drives” on page 57 and “Shared Storage Option (SSO) Topics” on page 245.

4. Use the Volume Configuration Wizard (select **Configure Volumes** in the right pane of the NetBackup Console) to define the media that you will be using in the storage devices. This wizard configures volumes for all supported standalone drives and robots.

When you logically add a new volume (or move volumes) in a robot that supports barcodes, a scan occurs and the Media Manager volume database is updated to reflect the contents of the robotic library.

To manually configure volumes for devices, use the menus of the **Media** node. See “Managing Media” on page 91 and “Managing Media in Robots” on page 153 for advanced robot inventory operations.

Security Issues

See the topic, “Media Manager Security” on page 347 for important information about security.

Media Manager security topics include the following:

- ◆ The relationship with NetBackup authentication/authorization security.
- ◆ Controlling user access to vmd (the Volume Manager service).
- ◆ Controlling user access to Media Manager robotic functions.





The device management window allows you to add, configure, and manage the devices that Media Manager uses.

This chapter explains how to attach drives and robotic libraries and configure Media Manager to use them. The topics in this chapter are listed below. If this is the first time you have configured devices, read the topics in the order they are presented in this chapter.

- ◆ “Starting Device Management” on page 18
- ◆ “Using the Device Management Window” on page 18
- ◆ “Performing Initial Device Configuration” on page 34
- ◆ “Managing the Device Manager Service (Windows) or the Device Daemon (UNIX)” on page 36
- ◆ “The Device Mapping File” on page 36
- ◆ “NetBackup Mixed Server Configurations” on page 37
- ◆ “Administering Devices on Other Servers” on page 38
- ◆ “The Global Device Database Host” on page 41
- ◆ “The Device Configuration Wizard” on page 44
- ◆ “Adding Robots” on page 46
- ◆ “Adding Drives” on page 60
- ◆ “Managing Your Device Configuration” on page 68
- ◆ “Printing Your Device Configuration” on page 78
- ◆ “Robot and Drive Configuration Examples” on page 79

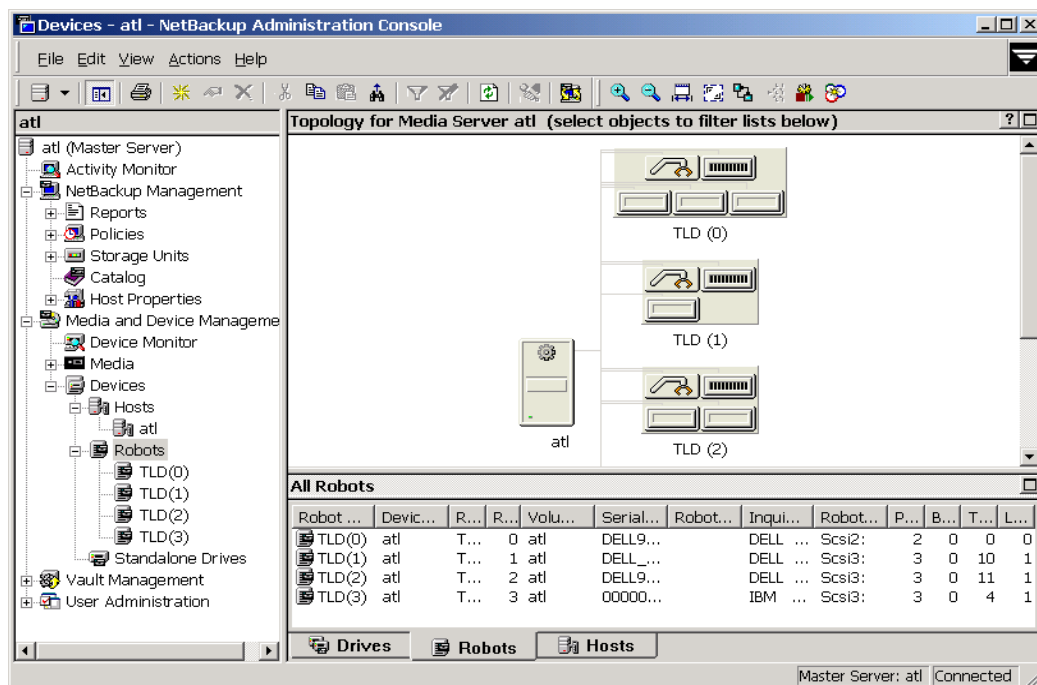
The following topics apply only to NetBackup Enterprise Server.

- ◆ “Administering Devices on Other Servers” on page 38
- ◆ “Adding Shared Drives” on page 57



Starting Device Management

In the NetBackup Administration Console, click **Media and Device Management > Devices**. The device management window similar to the following appears:



In addition to the tree pane on the left, the following two panes are displayed on the right when you start device management:

- ◆ A pane showing global topology.
- ◆ A pane showing devices.

Using the Device Management Window

The following topics provide an overview of the window's contents:

- ◆ “Menus and Commands” on page 19
- ◆ “Toolbars” on page 21
- ◆ “Tree Pane” on page 22
- ◆ “Global Topology Pane” on page 23
- ◆ “Devices Pane” on page 25

- ◆ “Status Bar” on page 31
- ◆ “Shortcut Menus and Commands” on page 31
- ◆ “Customizing the Window” on page 32
- ◆ “Allowable Media Manager Characters” on page 34

Menus and Commands

The device management window has available the menus and commands shown in the following table. Review the Note column for any restrictions.

The items on the menus are enabled based on the objects that are currently selected in the tree pane or topology pane, or which tab is selected in the devices pane. For example, if the robot tab is selected in the devices pane and a robotic library is selected in the list, **Inventory Robot** is enabled on the **Actions** menu.

Device Management Menus and Commands

Menu	Commands	Note
File	<p>Change Server - Displays a dialog that allows you to change to a different server that is running NetBackup. See “Administering Devices on Other Servers” on page 38 for details.</p> <p>New Console - Starts another instance of NetBackup Administration Console.</p> <p>New Window from Here - Starts another instance of the NetBackup Administration Console node that was active.</p> <p>Login as New User - Log into NetBackup as a different user without exiting NetBackup. This is useful if a NetBackup Administrator wants to log in again as the Security Administrator to administer Access Management. Controlling access to NetBackup is discussed in the NetBackup system administrator’s guide.</p> <p>Backup, Archive, and Restore - Starts the NetBackup backup, archive, and restore interface.</p> <p>MS SQL Client - Shortcut to access the SQL server NetBackup client, if it is installed on the selected server.</p> <p>Print Setup - Displays a setup dialog for printing.</p> <p>Print Preview - Previews the print image.</p> <p>Print - Prints the topology pane or devices pane (when one of these panes is selected).</p> <p>Close - Closes the current window.</p> <p>Exit - Closes all open windows.</p>	



Device Management Menus and Commands (continued)

Menu	Commands	Note
Edit	Undo - Allows you to cancel the last action. Cut, Copy, Paste - Commands for managing items in the display lists. New - Displays a dialog to add an item of the type that is currently selected. Change - Displays a dialog for changing the configuration of the selected items. Delete - Deletes selected items from the configuration. Find, Find Next, Find Prev, Find All - Commands for finding items in the display lists.	
View	Contains commands for specifying your viewing preferences for the device management window, including showing and hiding the toolbar or tree, showing and hiding robots, sorting, filtering, column layout, using the topology window, and refreshing the display. See “Customizing the Window” on page 32.	
Actions	New - Displays choices for adding robots or drives to a configuration. You can also add shared drives to a configuration.	Applies only to NetBackup Enterprise Server.
	Global Device Database - Displays a sub-menu that allows you to synchronize the entries in the global device database with the device configuration database. Synchronizing databases is normally not necessary, but can be done if you are experiencing problems and have made recent configuration changes that may not have been recognized. Also displays choices for adding or removing device hosts from the global device database. See “The Global Device Database Host” on page 41.	Applies only to NetBackup Enterprise Server.
	Change Standalone Volume Database Host - Displays a dialog to change the volume database host for standalone drives.	Applies only to NetBackup Enterprise Server.
	Inventory Robot - Displays a dialog with choices for performing an inventory of the selected robot or updating the volume configuration to match the contents of the robot.	



Device Management Menus and Commands (continued)

Menu	Commands	Note
	<p>Configure Shared Drive - Starts a wizard that guides you through the steps involved in adding a shared drive, changing a shared drive, or changing a non-shared drive to a shared drive (SSO option).</p> <p>Using this wizard is not the preferred method for adding shared drives. See “Adding Shared Drives” on page 57 first, if you are configuring shared drives.</p> <p>Drive Cleaning - Displays a sub-menu with choices for performing drive cleaning functions.</p> <p>Diagnose - Displays a dialog with choices for running diagnostic tests on a drive.</p> <p>Stop/Restart Device Manager Service - Stops and restarts the NetBackup Device Manager service.</p> <p>View SANPoint Control - Launches VERITAS SANPoint Control™. This web-based application helps you locate the cause of problems on your SAN or direct fibre-channel attached storage. See “Using SANPoint Control to Investigate SAN Problems” on page 77.</p>	Applies only to NetBackup Enterprise Server.
Help	<p>Help Topics - Provides online help information for the NetBackup Console.</p> <p>Troubleshooter - Helps you to debug errors.</p> <p>VERITAS Web Page - Displays the VERITAS web page, if the host has a browser configured.</p> <p>License Keys - Provides information about your active and registered license keys.</p> <p>About Administration Console - Displays program information, version number, and copyright information. You can click More for detailed information.</p> <p>Current NBAC User - Provides NetBackup Access Control information for the current user. Gives the permissions for the user that you are currently logged in as.</p>	

Toolbars

The toolbar buttons of the device management window provide shortcuts for commands that are on the menus. Also see “Customizing the Window” on page 32.



▼ **To show or hide the toolbar buttons**

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click **View > Toolbar**.

▼ **To customize the toolbar buttons**

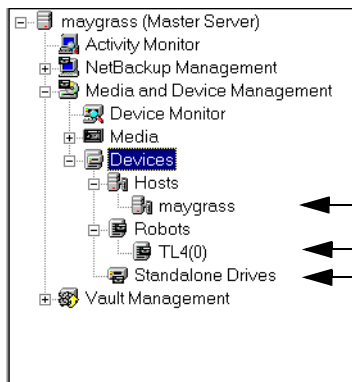
1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click **View > Customize....**

In the **Customize Toolbar** dialog you can reorder the buttons on the current toolbar, add buttons, or remove toolbar buttons. Use **Default** to reset the buttons on the toolbar.

Tree Pane

The tree pane for **Devices** contains nodes for **Hosts**, **Robots**, and **Standalone Drives**. You can select items in the tree pane or the Topology pane in conjunction with the tabs of the Devices pane to filter the lists that are shown in the Devices pane.

The following figure shows just the tree pane and contains an expanded view of the **Devices** node:



If you select a device host, robot, or Standalone Drives, the Topology pane shows the pertinent connections highlighted and the Devices pane shows information filtered for that specific selection.

Note Selecting an item in the Tree pane (for example, a specific robot) *does not* enable the **Robots** tab in the Devices pane.

The following point applies only to NetBackup Enterprise Server.

You can view or configure devices on another master or media server. See “Administering Devices on Other Servers” on page 38 for more information.

Global Topology Pane

A description bar is displayed at the top of the topology pane. Tool tips are also provided for all of the objects displayed in the topology pane.

Your view and use of the topology pane can be customized. See “Customizing the Window” on page 32. These commands are also available using the right mouse button in the topology pane.




The topology view shows how devices are configured to the server being administrated, by showing images of servers and devices. The topology information is taken from the Media Manager global device database and is displayed in this pane.

See the following related topics:

- ◆ “Topology Icons”
- ◆ “Topology Connections”
- ◆ “Selecting Topology Objects”

Topology Icons

The following are some of the images that can appear in the topology pane.

Description	Topology Image
NetBackup media server (or SAN media server)	
Robot	
Robot that is partially configured	



Volume database (robot media)



Drive



Drive that is partially configured



Drive that is shared (*NetBackup Enterprise Server*)



Topology Connections

Connections in the topology indicate physical and logical connections of the devices, as follows:

- ◆ Media server (or SAN media server) to robotic library and drive relationships are indicated. A line attaches a robot arm to the media server that has robot control.
- ◆ Drives that are physically located in a robotic library are shown directly below the robotic library. Standalone drives are represented as individual drive objects.
- ◆ A line attaches a drive to the servers that are configured to use it. Robot to server connections and robot to volume database connections are always shown.
- ◆ Media is represented as in a robotic library. A line attaches the media to the server doing media management.
- ◆ The topology also indicates robotic library to volume database host connections.

Selecting Topology Objects

Selecting objects in the topology pane is also one of the methods to filter the contents of the lists shown in the Devices pane.

Multiple objects of the same type can be selected by pressing the Ctrl key and selecting another object. If the Ctrl key is used and an object of a different type is selected, the selection is allowed and the other objects will not be selected. If the Ctrl key is not used and an object is selected, the previous selection will be unselected.

Selecting an object will highlight the connecting lines from the object to all other objects to which it is connected, as follows:

- ◆ Clicking on a drive will highlight the connection to the server where it is attached.
- ◆ Clicking on a server will highlight connections to all robots, media, and drives that are connected or configured to the server.

The following point applies to NetBackup Enterprise Server.

- ◆ Clicking on a shared drive will highlight connections to all servers that are configured to use the drive.

Devices Pane

The lower right pane contains tabs for **Drives**, **Robots**, and **Hosts**. These tabs allow you to select different views of your configuration. Information in the devices pane is taken from the Media Manager global device database and the local device databases.

You can use the tree pane or the topology pane in conjunction with the tabs to filter the lists shown in this pane. Selecting an item in the tree (for example, a specific robot) *does not* enable the **Robots** tab in the devices pane.

See the following topics:

- ◆ “Managing the Devices Pane” on page 25
- ◆ “Using the Drives Tab” on page 25
- ◆ “Using the Robots Tab” on page 29
- ◆ “Using the Hosts Tab” on page 31

Managing the Devices Pane

The **Edit** and **View** menus have commands for finding or showing items. These commands are useful if you are managing many devices. Some of the columns are initially hidden by default.

▼ To rearrange or hide columns

- ❖ Click **View > Columns > Layout**

Using the Drives Tab

The drives list allows you to view detailed information about drives configured with NetBackup.



To update the drives list with more detailed information, a drive must be selected in the topology pane. You can select a drive in the topology explicitly or implicitly by selecting a robotic library. The drives list will then be updated with the objects that are selected in the topology.

The following table describes the columns in the drives list. Check the Note column for any restrictions.

Drives List

Column	Description	Note
Drive Name	Contains the configured name of the drive. If the drive is configured as a shared drive (SSO), the icon for the drive appears as a shared item. If the icon shown for a drive contains a red arrow, the current server is <i>not</i> the volume database host for the drive. In this case, it is recommended to change to the correct server before adding volumes for this drive.	Applies only to NetBackup Enterprise Server.
Device Host	Contains the name of the device host (media server) where this drive is attached.	
Drive Type	Contains the type of drive. For example, 4MM. If the drive is partially configured, PCD is shown in this column. See “Managing Devices that are Partially-Configured” on page 45 for details.	
Robot Type	Specifies the type of robot that contains this drive. For example, TL4. NONE in this column means that the drive is a standalone drive. If the robot is partially configured, PCR is shown in this column. See “Managing Devices that are Partially-Configured” on page 45 for details.	
Robot Number	Contains the number of the robot. If the robot type is NONE, this column is blank.	
Robot Drive Number	Specifies the number of the drive in the robot. For ACS, TLH, and TLM robot types, the robot drive number is not displayed.	Applies only to NetBackup Enterprise Server.



Drives List (continued)

Column	Description	Note
Vendor Drive Identifier	For TLM robots, this column contains the DAS/SDLC drive name. For TLH robots, this column contains the IBM device number.	Applies only to NetBackup Enterprise Server.
ACS	Contains the ACS library software index that identifies the robot where this drive is located.	Applies only to NetBackup Enterprise Server.
LSM	Contains the ACS Library Storage Module where this drive is located.	Applies only to NetBackup Enterprise Server.
Panel	Contains the ACS robot panel where this drive is located.	Applies only to NetBackup Enterprise Server.
Drive	Contains the ACS library software physical number of the drive.	Applies only to NetBackup Enterprise Server.
Drive Path	Contains the path for the drive. For example, Tape5.	
Serial Number	Contains the drive serial number, if the drive reports a serial number.	
World Wide ID	Contains a unique identifier that is assigned to each device. Some drives may not report this identifier.	
Shared	Yes, means this drive is configured as a shared drive. No, means the drive is not a shared drive.	Applies only to shared drives (SSO) on NetBackup Enterprise Server.
Drive Status	Contains the current status of the drive. Status can be UP or DOWN.	
Port	This column contains the SCSI port number of the drive.	Applies only to NetBackup Windows servers.



Drives List (continued)

Column	Description	Note
Bus	This column contains the SCSI bus number of the drive.	Applies only to NetBackup Windows servers.
Target	This column contains the SCSI target number (or SCSI ID) of the drive.	Applies only to NetBackup Windows servers.
Lun	This column contains the SCSI logical unit number of the drive.	Applies only to NetBackup Windows servers.
Last Mount	Contains the last time a volume was mounted in the drive.	
Mount Time	Contains the total accumulated mount time (in hours).	
Cleaning Frequency	Contains the cleaning frequency for the drive (in hours). Contains a dash (-) for shared drives or robots that do not support frequency-based cleaning.	Applies only to NetBackup Enterprise Server.
Last Cleaning Time	Contains the date that the drive was last cleaned.	
Cleaning Comment	Contains the message, NEEDS CLEANING, if a cleaning frequency was defined for the drive and the value for Mount Time is greater than the frequency; or the TapeAlert CLEAN_NOW flag is set.	
TapeAlert Enabled	Contains Yes, if TapeAlert is enabled.	
Volume Header Device	This column specifies the volume header device path for the drive.	Applies only to optical disk drives on some NetBackup UNIX servers.



Drives List (continued)

Column	Description	Note
Drive Comments	Contains any user comments added for the drive.	
Inquiry Information	Contains device information returned from the device. This information is used to identify the device. For example, vendor ID, product ID, and product revision.	
NDMP Host	Contains the name of the NDMP control host.	
Drive Index	Drive index assigned to the drive during configuration.	

Using the Robots Tab

The robots list allows you to view detailed information about robots configured with NetBackup. Initially, all robots in the global device database are listed in the robot list. However, only information found in the global device database will be displayed in the list.

To update the robot list with more detailed information, a robot must be selected in the topology pane or in the tree pane. You can select a robot in the topology explicitly or implicitly by selecting a drive in the robot or the media server that the robot is connected to. The list will then be updated with the objects that are selected in the topology.

The following table describes the columns in the robots list. Check the Note column for any restrictions.

Robots List

Column	Description	Note
Robot Name	Contains the type and number of the robot, for example TLD(3). If the robot is partially configured, PCR is shown in this column. For example, PCR(3). See “Managing Devices that are Partially-Configured” on page 45 for details.	
	If the icon shown for a robot contains a red arrow, the current server is <i>not</i> the volume database host for the robot. In this case, it is recommended to change to the correct server before adding volumes for this device.	Applies only to NetBackup Enterprise Server.



Robots List (continued)

Column	Description	Note
Device Host	Contains the name of the device host where this robot is attached.	
Robot Type	Contains the type of robot. See “Media Manager Robot Types” on page 276 for a list of supported robot types. If the robot is partially-configured, PCR is shown in this column.	
Robot Number	Number of the robot.	
Volume Database Host	Contains the name of the volume database host that is used to track the volumes in this robot	
Serial Number	Contains the robot serial number, if the robot reports this information.	
Robotic Path	Contains the path for the robot if one exists. For example, changer0.	
Robot Control Host	Contains the name of the host that is providing the robotic control.	Applies only to NetBackup Enterprise Server.
Port	This column contains the SCSI port number of the robot.	Applies only to NetBackup Windows servers.
Bus	This column contains the SCSI bus number of the robot.	Applies only to NetBackup Windows servers.
Target	This column contains the SCSI target number (or SCSI ID) of the robot.	Applies only to NetBackup Windows servers.
Lun	This column contains the SCSI logical unit number of the robot.	Applies only to NetBackup Windows servers.
Inquiry Information	Contains device information returned from the device that is used to identify the device. For example, vendor ID, product ID, and product revision.	



Using the Hosts Tab

The hosts list allows you to view detailed information about the servers that are referenced in your Media Manager configuration.

To update the hosts list with more detailed information, a host must be selected in the topology pane or in the tree pane. You can select a host in the topology explicitly or implicitly by selecting a robot. The hosts list will then be updated with the objects that are selected in the topology.

The following table describes the columns in the hosts list:

Hosts List

Column	Description
Host Name	Contains the name of the device host.
Connection Status	Contains the current NetBackup connection status for this server. This status field can contain Connected, Not Connected, or the text of a connection error message.
Standalone Volume Database Host	Contains the name of the volume database host for all of the standalone drives controlled by this device host.
Version	Contains the NetBackup software version.

Status Bar

The status bar appears at the bottom of the NetBackup Console window. The status bar

- ◆ Shows tool tips (when the mouse is over a toolbar icon or an object)
- ◆ Indicates the name of the master server.
- ◆ Indicates if you are connected to the master server.

▼ To show or hide the status bar

- ❖ Click **View > Status Bar**.

Shortcut Menus and Commands

Shortcut menus work in the context of what device is currently selected in the tree pane or topology pane, or which tab is selected in the devices pane. Shortcut commands are also available on the menus or toolbars.

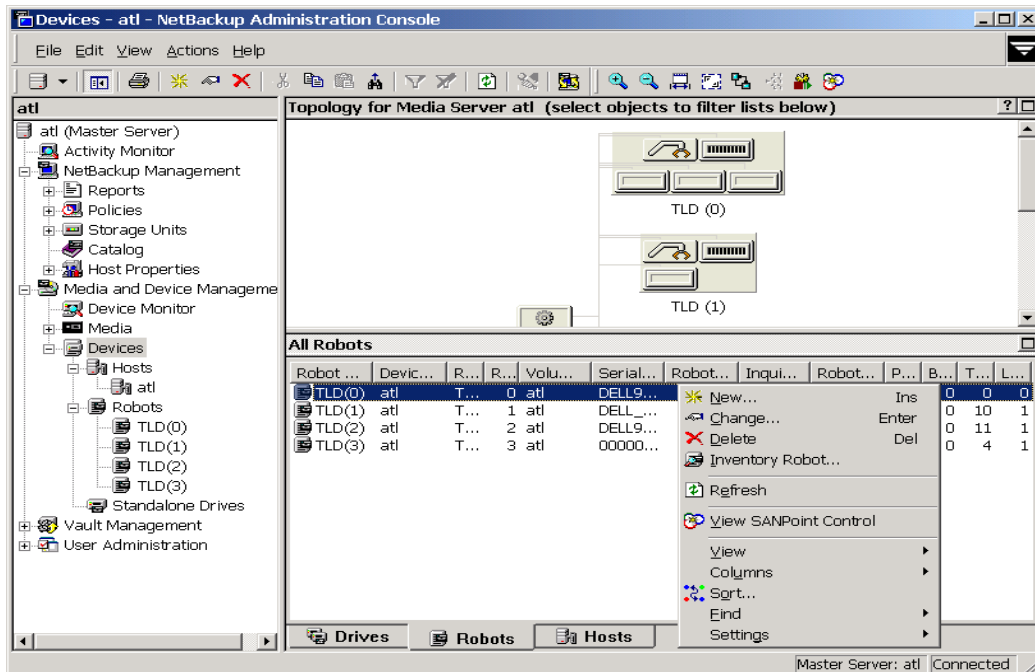


▼ To display a shortcut menu

- ❖ Click the right mouse button while the pointer is over a pane or a selection of a pane.

Help for the topology pane is available using the right mouse button in the topology pane (select **Topology Info**).

Short Cut Menu



Customizing the Window

The **View** menu has options for sorting, filtering, and changing the layout and appearance of the panes.

See the following topics:

- ◆ “Viewing and Rearranging Columns” on page 33
- ◆ “Changing the View of the Topology Pane” on page 33

See the NetBackup administrator’s guide for UNIX or the NetBackup administrator’s guide for Windows for more details.

Viewing and Rearranging Columns

▼ To show or hide columns, or rearrange the order of columns

- ❖ Click **View > Columns > Layout**.

Changing the View of the Topology Pane

These commands are also available using the right mouse button in the topology pane.

▼ To fit the topology diagram to the pane

This procedure will fit the diagram to the pane, and not use the default size on start up.

1. Click **View > Options > Devices**.
2. Select **Fit topology to window on startup**.

▼ To enlarge the topology diagrams

This command can be done multiple times.

- ❖ Click **View > Zoom > Zoom In**.

▼ To decrease the size of the topology diagrams

This command can be done multiple times.

- ❖ Click **View > Zoom > Zoom Out**.

▼ To size the topology diagram to the size of the current pane

- ❖ Click **View > Zoom > Fit to Window**.

▼ To select objects and focus on a portion of the topology diagram

1. Click **View > Zoom > Overview Window**.

A copy of the topology diagram appears in a secondary window.

2. Use the mouse to select desired objects or portions of objects in the configuration. The selected objects will be the focus of the main topology pane, allowing you to focus on areas of the topology diagram.



▼ **To show only the connection for a selected device**

Use this option to show the connection for a selected device, rather than showing all connections in the topology.

❖ Click **View > HighLighted Connections Only**.

▼ **To show all of the connections in the topology**

❖ Click **View > All Connections**.

Allowable Media Manager Characters

The following set of characters can be used in user-defined names, such as drive comments, host names, and drive names that you enter when creating these Media Manager entities. These characters must be used even when specifying these items in foreign languages.

Do not use a minus as the first character. Spaces are only allowed in a comment for a drive.

- ◆ Alphabetic (A-Z and a-z)
- ◆ Numeric (0-9)
- ◆ Period (.)
- ◆ Plus (+)
- ◆ Minus (-)
- ◆ Underscore (_)

Performing Initial Device Configuration

For NetBackup to recognize and communicate with the connected devices, and for device discovery to discover devices, NetBackup issues SCSI pass-thru commands to the devices in a configuration.

The server platforms supported by NetBackup may require special operating system configuration changes. This may include changes needed for device discovery and other configuration requirements for devices to be recognized.

See the appropriate chapter of the NetBackup Media Manager device configuration guide for your particular server platform.

When performing initial device configuration, a prompt at the end of the procedure asks if you want to stop and restart `ltid`. This action also stops and restarts any robotic processes. See “Managing the Device Manager Service (Windows) or the Device Daemon (UNIX)” on page 36 for information on manually controlling `ltid`.

▼ **To attach devices to a Windows master or media server**

The following steps describe a general method for attaching devices to a Windows media server. The Microsoft Windows device applications available on the server that you use in these steps may differ depending on your Windows operating system.

1. Use the appropriate Windows application to obtain information on any currently attached SCSI devices.
2. If you are attaching a new robotic library or drive to a Media Manager media server, follow the vendor’s instructions for attaching the device.

Shut down the server and physically attach the supported device, ensuring that SCSI targets and termination settings are consistent with adapter card and peripheral vendor recommendations.

3. Reboot the server and answer the prompts for adapter card peripheral configuration options. Watch the display to ensure that the adapter card recognizes the attached peripherals.
4. If you are adding drives, install the tape drivers and use the appropriate Windows application to verify that the drive was recognized.

You can download the latest 32-bit tape drivers and tape installer from <http://support.veritas.com>. Drivers are also available on the NetBackup installation CD.

Search on the keywords *tape device installer*. These drivers support the tape devices listed in the compatibility lists on this web site.

`NetBackupTapeDeviceDriverInstall.exe` will run only if NetBackup has been installed.

5. Configure the storage devices using Media Manager. Depending on the type of device you are installing, proceed to the following topics:
 - ◆ “The Device Configuration Wizard” on page 44.
 - ◆ “Adding Robots” on page 46.
 - ◆ “Adding Drives” on page 60.

The following points apply only to NetBackup Enterprise Server.



- ◆ If you are adding the device to a remote host, see “Administering Devices on Other Servers” on page 38.
- ◆ “Adding Shared Drives” on page 57.

Managing the Device Manager Service (Windows) or the Device Daemon (UNIX)

Stopping and restarting `ltid` also stops and restarts any robotic processes. `ltid` is the Media Manager device daemon on UNIX servers and the NetBackup Device Manager service on Windows servers.

Caution Stopping and restarting `ltid` may abort any backups, archives, or restores that are in progress.

▼ To manage this service

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click **Actions > Stop/Restart Device Manager Service**.
3. *The following step applies only to NetBackup Enterprise Server.*
Select a device host. The dialog also shows the current status of this service.
4. The dialog allows you to start, stop, or stop/restart the service on the host. Select the action you want to perform.
5. Click **OK** or **Apply**.
You may find it useful to select **Stop** and click **Apply**, and then select **Start** and click **Apply**.

The Device Mapping File

This mapping file is used by the Device Configuration wizard to discover and configure new robots and drives. This file is also used by NetBackup processes to communicate with various vendor devices.

In some cases, device discovery support for new or upgraded devices may be accomplished without waiting for a patch from VERITAS. Support for some new devices only requires that you download an updated device mapping file when any device changes are made to your configuration.

Note The contents of this file does not indicate support for any of the devices, only the ability to recognize and automatically configure them.

▼ **To obtain the current device mapping file**

1. Visit the VERITAS support web site (<http://www.support.veritas.com>) to download the latest device mapping file for your devices.
2. Refer to the supplied README file for instructions. The files that you download are named similar to the following files: `Mappings_5_nnnnnn.TAR` and `Mappings_5_nnnnnn.ZIP`.

NetBackup Mixed Server Configurations

This is a NetBackup Enterprise Server topic.

Mixed levels of NetBackup servers are supported. This enables NetBackup master and media servers to run a mixture of NetBackup major releases and patch releases in the same environment.

The basic rules for a NetBackup mixed server environment are as follows:

- ◆ The master server must be running the highest release level of NetBackup that is installed in the environment. All of the media servers in the environment must be running equal or lower levels of NetBackup.
- ◆ Starting with the NetBackup 5.0 release, a master server can inter-operate with a media server that is running a level of NetBackup that is one major release lower. (NetBackup 4.5 release levels cannot inter-operate with lower release levels.)

For example, a NetBackup master server running NetBackup 5.1 can inter-operate with media servers running NetBackup 4.5, 5.0, 4.5 MP2, 5.1, and 5.0 MP1.

Ensure that all of the servers in the environment have the appropriate and latest NetBackup patches installed.

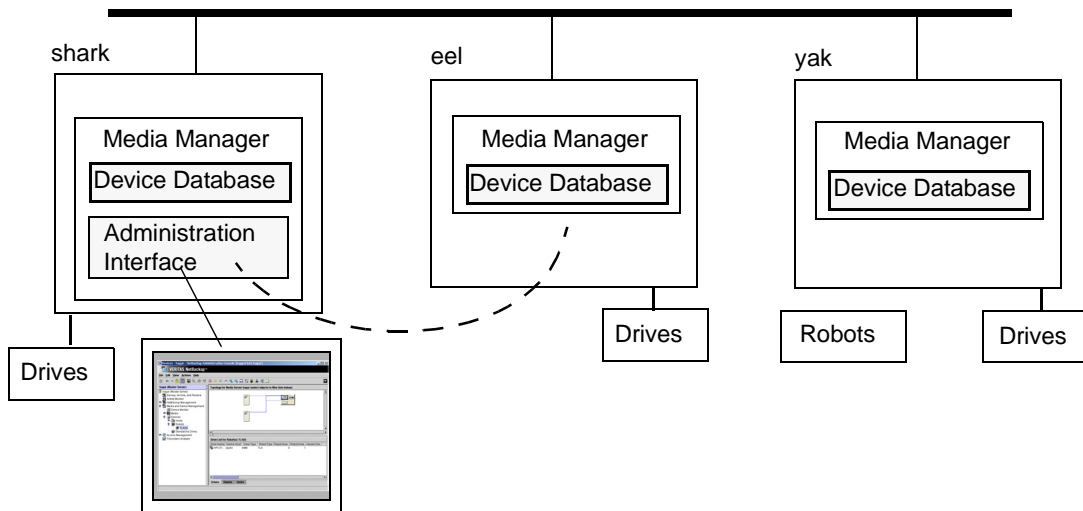
If you are using SSO, be sure to review the “Volume Database Host (Device Allocation Host) Requirements” on page 251.



Administering Devices on Other Servers

This is a NetBackup Enterprise Server topic.

Initially, you can manage the storage devices that are configured on the server where you are running the NetBackup Media Manager interface. In the following figure, the administrator is running the NetBackup Administration Console on server shark and managing devices on host eel.



You can administer devices that are attached to other servers, if these servers are in the same hardware configuration and are using the same global device database host. Select the device or host that you want to administer in the tree pane of the NetBackup Administration Console.

You can also change from the current server to a different master or media server. If you change from a NetBackup Enterprise Server to a NetBackup Server, the functionality available on the new server is limited to the functionality supported by NetBackup Server.

If you change from a NetBackup Server to a NetBackup Enterprise Server, complete functionality is available on the new server.

▼ To change to a different master or media server

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click **File > Change Server**.

(You can also click the **arrow** to the right of the **Change Server** icon on the toolbar and select one of the servers shown in the list).

3. In the dialog that appears, do *one* of the following to specify the server that you want to monitor.
 - ◆ Enter the name of the server.
 - ◆ Select a server from the servers shown in the list.
 - ◆ Click **Browse** and select a server.
 - ◆ Login to the current server using a different user name.
 - ◆ Login to a different server using a different user name.

You can also click **Remove** to delete a server from the list.

4. Click **OK**.

The name of the new server appears, and the topology and devices panes show device information for the new server.

In addition to using **File > Change Server** to manage devices on other servers, you can use **File > Login as New User**. See “Menus and Commands” on page 19.

Media Manager Security

For Media Manager to access media and device management functionality on another host, you may need to add a `SERVER` entry to the `vm.conf` file on the remote host.

`SERVER` entries are used for Media Manager security. If there are no `SERVER` entries and authentication is not enabled, *any* host can perform media and device management on the host. You can add entries allowing only specific hosts to remotely access those capabilities.

If the <code>vm.conf</code> File on a Remote Host Contains	Then
No <code>SERVER</code> entries and authentication is not enabled	Any host can perform media and device management on this host. It is not necessary to make any additions to <code>vm.conf</code> .
<code>SERVER</code> entries	You must add a <code>SERVER</code> entry for the host where you are running (the server you logged into) the NetBackup Administration Console (if an entry is not present).



vmd Considerations

`vmd` is the Media Manager volume daemon on UNIX servers and the NetBackup Volume Manager service on Windows servers. Device configuration changes, even those made local to a server, may require `vmd` to be running. It is recommended that `vmd` be running at all times, including when changes are being made to the Media Manager device configuration.

Media Manager authentication/authorization may affect systems where NetBackup authentication/authorization has been enabled.

Connections to `vmd` will fail if authentication/authorization are enabled, an `AUTHORIZATION_REQUIRED` entry is present in `vm.conf`, and the caller of `vmd` does not have the required permission to use `vmd` functions.

▼ To enable authentication/authorization in NetBackup (but not in Media Manager)

You can do either of the following:

- ❖ Add `SERVER` entries in `vm.conf`.
- ❖ Have no `SERVER` and no `AUTHORIZATION_REQUIRED` entries in `vm.conf`.

See “Media Manager Security” on page 347 for more information on the following topics:

- ◆ The relationship with NetBackup authentication/authorization security.
- ◆ Controlling user access to `vmd` (the Media Manager volume daemon).
- ◆ Controlling user access to Media Manager robotic daemons and services.

Example SERVER Entries

Assume that you have three hosts, named `eel`, `yak`, and `shark`; and that NetBackup authentication is not enabled.

You want to centralize device management on host `shark` and also permit each host to manage its own devices.

- ◆ The `vm.conf` file on `shark` contains the following:

```
SERVER = shark
```

The `vm.conf` file on `shark` does not require any additional `SERVER` entries, because all device management for `shark` will be performed from `shark`.

- ◆ The `vm.conf` file on `eel` contains the following:

```
SERVER = eel
```

```
SERVER = shark
```

This allows eel to manage its own devices and also permits shark to access them.

- ◆ The `vm.conf` file on yak contains the following;

```
SERVER = yak
```

```
SERVER = shark
```

This allows yak to manage its own devices and also permits shark to access them.

The Global Device Database Host

The global device database is the repository for all Media Manager device configuration information. See the following topics for more information about this host:

- ◆ “A Single Host is Required” on page 41
- ◆ “How This Host is Determined” on page 42
- ◆ “Managing The Global Device Database Host” on page 42

A Single Host is Required

This is a NetBackup Enterprise Server topic.

Device discovery, auto-configuration, and manual configuration (for example, `tpconfig`) are all methods used by NetBackup and Media Manager to configure devices. For device configuration to work properly (particularly where devices are connected to many servers) a single host must serve as the repository for global device configuration information.

See “Media and Device Management Domain Management” on page 271 and “Frequently Asked Questions About Device Discovery” on page 295.

Note When using the Device Configuration wizard, a global device database host conflict may be detected during device scanning. This indicates that the hosts you selected to scan do not agree on which host to store the global device information.

Also, the **Devices** node of the NetBackup Administration Console requires that all hosts that the node references need to be using the same global device database host. The **Devices** node verifies global device database consistency between any hosts that are included for device management.

The `tpautoconf` command has options to preview and merge existing global databases. See the NetBackup commands guide for details.



How This Host is Determined

This is a NetBackup Enterprise Server topic.

When you install NetBackup, the default option is to have the master server configured to be the global device database host. If your environment contains multiple master servers, you can designate a different server to be your global device database host during the installation.

If you have multiple master servers in your configuration or did not install or upgrade your master servers before the media servers, then more than one host may have been designated as the global device database host. Refer to synchronizing the database in “Managing The Global Device Database Host” on page 42 to correct this problem.

You should manage your media servers from the master server point of view.

Managing The Global Device Database Host

The following topics explain the commands that are used to manage the global device database host.

▼ To add a device host to the database

This is a NetBackup Enterprise Server topic.

Unless you add a drive or add a robotic library, entries for each device host are not entered in the database (no host entries are present in the database).

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select **Actions > Global Device Database > Add Device Host**.
3. Enter a device host name or click **Browse** to find a host.

▼ To remove a device host from the database

This is a NetBackup Enterprise Server topic.

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select **Actions > Global Device Database > Remove Device Host**.

▼ To synchronize the database

This procedure updates host settings in the global device database to be consistent with the device configurations of all of the device hosts in your configuration.

Synchronizing the global device database is normally not necessary, but can be done if you are experiencing problems and have made recent configuration changes to your local device hosts that may not have been recognized.

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select **Actions > Global Device Database > Synchronize Global Device Database**.

▼ To specify a different host as the global device database host

This is a NetBackup Enterprise Server topic.

- ❖ Use the `tpautoconf` command to determine the current global device database host and to specify a different host as the global device database host.

See the NetBackup commands for UNIX or NetBackup commands for Windows reference guide for information about using the `get_gdbhost` and `set_gdbhost` options of the `tpautoconf` command.

`tpautoconf` is also used by the Device Configuration wizard to automatically discover and configure devices.

Why You Should Use the Media Manager Wizards

NetBackup provides two wizards for configuring devices (the Device Configuration wizard and the Shared Drive wizard), a wizard for configuring volumes, and also a device configuration analyzer.

Using the wizards is recommended and is the easiest method for configuring devices and media. The wizards guide you through the configuration steps. In addition to making the configuration process faster, these wizards eliminate many common mistakes made when configuration is done using alternate methods.

The wizards are available from the Media and Device Management interface of the NetBackup Administration GUI. Some of the wizard screens differ slightly on the Windows and UNIX versions of NetBackup.

Caution Use these wizards with care in a production environment, since these wizards stop the Media Manager daemons/services. You should *not* be running production backups when using these wizards.



▼ **To use the Media Manager wizards**

1. From your server use one of the device configuration wizards to configure robots and drives.

See “The Device Configuration Wizard” on page 44.

The following point applies only to NetBackup Enterprise Server.

If you are using the shared drive option, see “Adding Shared Drives” on page 57.

2. Use the Volume Configuration wizard to configure media for robots and standalone drives.

See “Using the Volume Configuration Wizard” on page 129.

The Device Configuration Wizard

Using the Device Configuration wizard is the recommended method of configuring most devices. You should use this wizard to configure the following types of devices:

- ◆ Robots
- ◆ Drives
- ◆ Robots and drives attached to NDMP hosts
- ◆ Shared drives (*for NetBackup Enterprise Server SSO configurations only*)

This wizard uses device discovery to auto-configure devices and add robotic libraries and drives to your Media Manager configuration. To perform these tasks, this wizard uses device serialization.

This wizard also uses the device mapping file when discovering and configuring devices. See “The Device Mapping File” on page 36.

In some cases, the wizard may leave some devices partially configured. See “Managing Devices that are Partially-Configured” on page 45 for more information.

For important background information on device discovery, device serialization, and the Device Configuration wizard, see “Frequently Asked Questions About Device Discovery” on page 295.

See the following related topics:

- ◆ “Operating System Changes” on page 45
- ◆ “Possible Global Device Database Host Conflict” on page 45
- ◆ “Configuring Devices not Supported by the Wizard” on page 45
- ◆ “Managing Devices that are Partially-Configured” on page 45

- ◆ “Learning More About the Device Configuration Wizard” on page 46
- ◆ “Starting the Device Configuration Wizard” on page 46

Operating System Changes

For device discovery to discover devices, NetBackup issues SCSI pass-thru commands to the devices in a configuration. The server platforms supported by NetBackup may require special operating system configuration changes. This may include changes needed for device discovery and other configuration requirements for devices to be recognized.

See the appropriate chapter of the NetBackup Media Manager device configuration guide for your particular server platform.

Possible Global Device Database Host Conflict

The following topic applies only to NetBackup Enterprise Server.

When using this wizard a global device database host conflict may be detected during device scanning. This conflict occurs when the hosts you selected to scan in the wizard do not agree on which host stores global device information. See “The Global Device Database Host” on page 41 for more information.

Configuring Devices not Supported by the Wizard

To configure devices that are not supported or fully-supported by the Device Configuration wizard, see the following topics:

- ◆ “Adding Robots” on page 46.
- ◆ “Using the Device Configuration Wizard to Configure Shared Drives” on page 58.
- ◆ “Adding Drives” on page 60.

Managing Devices that are Partially-Configured

Under certain conditions, for example in the case of an unsupported robotic library or drive, the Device Configuration wizard may leave some devices as partially configured. Also if you deselect a discovered device from the tree view in the wizard, the device will be configured as partially configured.

Partially-configured drives are shown as **PCD** and partially-configured robots as **PCR** in the Drives list of the Devices window pane. See “Using the Drives Tab” on page 25 and “Using the Robots Tab” on page 29.



If you have partially-configured drives, ensure that you have downloaded the most recent device mapping file from the VERITAS support web site (see “The Device Mapping File” on page 36).

Learning More About the Device Configuration Wizard

You can obtain detailed information about this wizard before you start using the wizard, including what to expect in the wizard, a wizard overview, and limitations of the wizard.

▼ To learn about this wizard

1. Start the wizard (see “Starting the Device Configuration Wizard” on page 46).
2. From the welcome screen of the wizard, click **Help**.
3. When finished reviewing the help information for the wizard, exit the help and click **Cancel** to exit the wizard.

Starting the Device Configuration Wizard

This wizard is available from the list of wizards displayed in the right pane of the **Media and Device Management** window of the NetBackup Administration Console or from the Getting Started wizard.

Be sure to review the limitations of this wizard before starting.

▼ To start the device configuration wizard

- ❖ In the NetBackup Administration Console, click **Media and Device Management > Configure Storage Devices**.

Adding Robots

Note Using the Device Configuration wizard is the recommended method of configuring robots. See “The Device Configuration Wizard” on page 44 for more information and wizard restrictions.

When adding a robotic library and drives, the best method is to add the robot first, as explained in the following procedure and then add the drives (see “Adding Drives” on page 60).

▼ To add a robot

1. Perform the steps explained in “Performing Initial Device Configuration” on page 34.
2. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
3. Select **Actions > New > New Robot**.

A dialog for adding a robotic library appears. The properties that appear in this dialog vary depending on the server platform type and robot type.

The screenshot shows the 'Add Robot' dialog box. It has a title bar with 'Add Robot' and a close button. The dialog is divided into several sections. At the top, there are four fields: 'Device host' (a dropdown menu showing 'nerio'), 'Robot type' (a dropdown menu showing 'TLD - Tape Library DLT'), 'Volume database host' (a dropdown menu showing 'nerio'), and 'Robot number' (a numeric input field showing '3'). To the right of these fields are three buttons: 'New...', 'OK', 'Cancel', and 'Help'. Below these fields, there is a 'Robot name' field showing 'TLD(3)'. In the center, there is a 'Robot control' section with two radio buttons. The first radio button is selected and is labeled 'Robot is controlled locally by this device host.' The second radio button is labeled 'Robot control is handled by a remote host.' Below the radio buttons, there is a 'Robot device' field with the text '(click Browse to select):' and a 'Browse...' button. At the bottom, there is a 'Robot control host' field showing 'test66'.

4. Specify the properties for the robotic library as explained in “Dialog Entries for Adding and Changing Robots” on page 48.
5. Click **OK**.

A prompt appears asking whether you want to stop and restart the NetBackup Device Manager service (this also stops and restarts any robotic processes). If your changes are complete, answer yes to this prompt.

Note It is possible that stopping and restarting this service will stop any backups, archives, or restores that are in progress.



Dialog Entries for Adding and Changing Robots

The following topics describe the properties that you specify when you add a robotic library or change a robot configuration. Some of these properties apply only to specific types of robots, types of server platforms, or NetBackup server types.

- ◆ “Device Host” on page 48
- ◆ “Robot Type” on page 48
- ◆ “Robot Number” on page 49
- ◆ “Volume Database Host” on page 50
- ◆ “Robot Control Section of the Dialog” on page 50
- ◆ “Robot is controlled locally by this device host” on page 53
- ◆ “Robot control is handled by a remote host” on page 55
- ◆ “Robot control is attached to an NDMP host” on page 57

Device Host

Device Host applies only to NetBackup Enterprise Server.

Specifies the host to which you are adding the robotic library.

▼ To specify a device host

- ❖ Click the **arrow** and select a host from the list.

▼ To specify a device host that is not in the list

1. Click **New ...**
2. In the dialog that appears, enter the name of the host that you want.

Robot Type

Specifies the type of robot that you are adding.

▼ To specify a robot type

1. Visit the VERITAS support web site (<http://www.support.veritas.com>) to locate the robot type to use for specific vendors and models.
2. Click the **arrow** and select from the list of types that Media Manager supports. (Specify **RSM** if you are adding a RSM robot.)

▼ To specify an RSM robot type

- ❖ Review the following important points about using the Microsoft Windows Removable Storage Manager (RSM):
 - ◆ Your device host must be running a Windows operating system that supports RSM.
 - ◆ The Microsoft Removable Storage Manager will be in control of the robot rather than Media Manager.
 - ◆ A robotic library configured as an RSM robot, cannot also be used as a Media Manager direct-controlled (SCSI) robot (for example, TLD).
 - ◆ For more information on configuring and using RSM robots, see the appendix, “Microsoft Removable Storage Manager (RSM)” on page 391.
 - ◆ *The following point applies only to NetBackup Enterprise Server.*
Shared drives cannot be configured in an RSM robot, and RSM robots cannot be shared.

Robot Number

Specifies a unique, logical identification number for the robotic library. This number identifies the robotic library in displays (for example, TLD (21)) and is also used when adding media for the robot to the Media Manager configuration.

▼ To specify a robot number

- ❖ Click an **arrow** and select a robot number.

The following points apply only to NetBackup Enterprise Server.

- ◆ Robot numbers must be unique for all physically-distinct robots on all hosts in the configuration. This applies regardless of the robot type or the host that controls them. For example, if you have two robots, use different robot numbers even if they are controlled by and configured on different hosts.



- ◆ If you are adding a robot definition for a robot where the robot control is handled by a remote device host, be sure to use the same robot number as used for that robot on all other device hosts.
- ◆ If the robot has its robotic control and drives on different hosts (for example, as permitted by a Tape Library DLT robot), be certain to specify the same robot number in all references to that library. That is, use the same robot number on the hosts with the drives, as you do on the host that has the robotic control.

See “Example 3: Configuring a Robot Distributed Among Multiple Servers” on page 83.

Volume Database Host

Volume Database Host applies only to NetBackup Enterprise Server.

Specifies the name of the host where Media Manager keeps the volume configuration information about the media in the robotic library. You can specify any host that has Media Manager installed as the volume database host, even if the host does not have any drives or robots attached.

VERITAS recommends that you use one volume database host for all your volumes (robotic and standalone). Although it is possible to maintain separate volume databases on multiple hosts, administration is more difficult.

See “Media and Device Management Domain Management” on page 271 for more information.

“Example 3: Configuring a Robot Distributed Among Multiple Servers” on page 83, shows a configuration where the volume database is on a central host.

You will have to know the name of the volume database host when adding volumes to the robotic library.

Adding volumes is explained in “Managing Media” on page 91.

▼ To specify the volume database host

- ❖ Click the **arrow** and select from the list of hosts.

Robot Control Section of the Dialog

In the Robot control section you specify the type of control for the robot. Depending on the robot type you are adding and the type of media server, various combinations of the robot control buttons are available in the dialog.

Be sure to read your NetBackup release notes or visit the VERITAS support web site for more detailed information on supported robot types, media server platforms, and other NetBackup server limitations.

See the following topics:

- ◆ “Robot is controlled locally by this device host” on page 53.
- ◆ “Robot control is handled by a remote host” on page 55.
- ◆ “Robot control is attached to an NDMP host” on page 57.

Also see “Robot Attributes” on page 279 for more information.

Robot Control Configuration Overview

The following table provides an overview of robot control configuration, based on robot type and the media server platform type. The third column in the table indicates the robot control button that is valid for that particular robot type and server platform:

Media Manager Robot Type	Supported Media Server Platform	Type of Robot Control	Information Required for Configuration
ACS	All	Remote	ACSLS host
LMF	Solaris	Local	Library name
LMF	Solaris	Remote	Robot control host
ODL	AIX, Solaris, HP-UX, and IRIX	Local	Robotic device file
RSM	Windows (needs RSM support)	Local	Robot device
TL4	UNIX (except Linux)	Local	Robotic device file
TL8, TS8, and TSD	UNIX	Local	Robotic device file
TLD	UNIX	Local	Robotic device file
TSH	AIX, Solaris, and IRIX	Local	Robotic device file
TL4, TL8, TLD, TS8, and TSD	Windows	Local	Robot device
TL8	All	Remote	Robot control host



Media Manager Robot Type	Supported Media Server Platform	Type of Robot Control	Information Required for Configuration
TLD	All	Remote	Robot control host
TL8, TLD, TSD, and TLH	Windows, AIX, Solaris, and HP-UX	NDMP	NDMP host name and Robot device
TLH	AIX	Local	LMCP device file
TLH	UNIX (except AIX and Linux) and Windows	Local	Library name
TLH	All (except Linux)	Remote	Robot control host
TLM	All (except Linux)	Remote	DAS/SDLC server

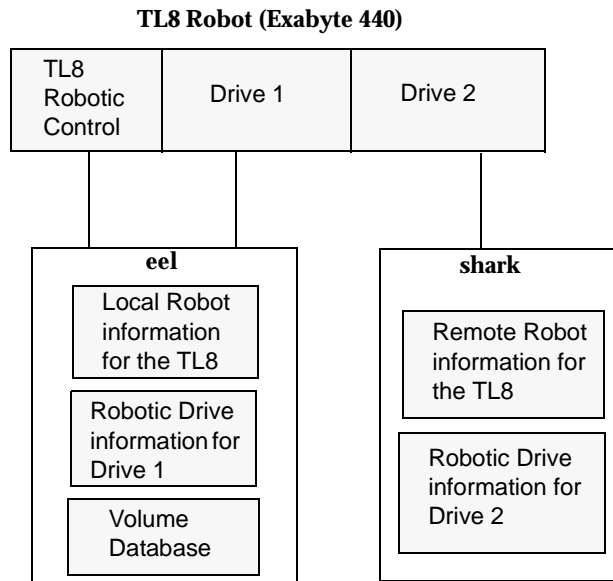
Library Sharing Example

The following example applies only to NetBackup Enterprise Server.

The following figure shows two servers using two drives in a TL8 robot. This is an example of library sharing. The robotic control for the robot is on the host named eel. One drive in the robot is connected to eel and the other is connected to the host shark.

When you add this robot to the device configuration on eel, you select **Robot is controlled locally by this device host**. When you add the robot to the device configuration on shark, you select **Robot control is handled by a remote host**.

Robot Control Host Example

**Robot is controlled locally by this device host**

For this type of robot control, you have the following possibilities based on the robot type that you selected and type of media server platform where you are adding the robot.

- ◆ “Robotic Device File” on page 53
- ◆ “Robot Device” on page 54
- ◆ “LMCP Device File” on page 54
- ◆ “Library Name” on page 55

Robotic Device File

Robotic Device File applies only when adding a robot to a UNIX device host.

This file is used for SCSI connections and is located in the `/dev` directory tree on the device host.

▼ **To specify the robotic device file path**

1. Click **Browse**.
2. Select a robotic device file from the list that appears in the **Devices** dialog. When you click **OK**, your selection will be placed in **Robotic device file**.



3. If the browse operation fails to find and display all of the attached robots, click **Other Device** to display a dialog that allows you to enter the path of the device file. Your entry will be placed in **Robotic device file**.

If the browse operation does not find any attached robots you will see an error dialog.

If the device file entry does not exist, create the entry as explained in the NetBackup Media Manager device configuration guide.

Robot Device

Robot Device applies only when adding a robot to a Windows device host.

For information on adding RSM robots to a Windows server, see the appendix, “Microsoft Removable Storage Manager (RSM)” on page 391.

▼ To specify the robot device

1. Click **Browse**.

If the browse operation does not find any attached robots you will see an error dialog.

2. Select a robot from the list that appears in the **Devices** dialog.

3. Click **OK**.

The resulting value that is set in **Robot device** depends on the type of Windows device host where the robot is being added. For RSM robot types, a device name is always set in **Robot device**.

The following table shows the resulting settings in **Robot device** for different types of Windows device hosts:

Robot Device Setting	For this Type of Windows Device Host
SCSI Port, Bus, Target, and LUN numbers	Windows NT servers.
SCSI Port, Bus, Target, and LUN numbers	Windows servers where a changer driver <i>is not</i> in control of the robot.
Device name (for example, Changer1)	Windows servers where a changer driver <i>is</i> in control of the robot.

LMCP Device File

LMCP Device File applies only to NetBackup Enterprise Server, and when adding a robot to a UNIX AIX device host.

▼ **To specify the LMCP file for TLH robot types controlled from an AIX device host**

- ❖ Specify the LMCP (Library Manager Control Point) device file name as it is configured on the AIX device host.

Library Name

Library Name applies only when adding a LMF or TLH robot on NetBackup Enterprise Server.

For more information on LMF robots, see the appendices of the NetBackup Media Manager system administrator's guide for UNIX.

For more information on TLH robots, see the appendix, "IBM Automated Tape Library (ATL)" on page 399.

▼ **To specify the library name for LMF robots controlled from a UNIX host**

1. Use the Fujitsu `lmadmin` command to determine the library name.
2. Specify the library name.

▼ **To specify the library name for TLH robots controlled from a UNIX host (the host is not AIX or Linux)**

- ❖ Specify the library name that is configured on the UNIX host.

▼ **To specify the library name for TLH robots on a Windows host**

1. Determine the library name by viewing the `C:\winnt\ibmatl.conf` file.

The following is an example entry in that file, where 3494AH is the library name:

```
3494AH 176.123.154.141 ibmpc1.
```

2. Specify the library name.

Robot control is handled by a remote host

This is a NetBackup Enterprise Server topic.

For this type of robot control, you have the following possibilities for the robot control host (based on the robot type and device host platform that you selected).

- ◆ "Robot Control Host" on page 56
- ◆ "DAS Server" on page 56
- ◆ "ACSLs Host" on page 56



Robot Control Host

Robot Control Host applies only to NetBackup Enterprise Server.

For more information on TLH robots, see the appendix, “IBM Automated Tape Library (ATL)” on page 399.

For more information on LMF robots, see the appendices of the NetBackup Media Manager system administrator’s guide for UNIX.

▼ To specify the robot control host for LMF (UNIX hosts only), TL8, TLD, or TLH robots

- ❖ Specify the device host that controls the robot. Enter the name of the device host where you have defined or will define the robot information for this robot.

Referring to the figure, “Robot Control Host Example” on page 53, you would specify eel as the Robot Control Host when adding a robot to host shark.

DAS Server

DAS Server applies only to NetBackup Enterprise Server.

For more information on TLM robots, see the appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 411.

▼ To specify the DAS server for TLM robots controlled by an ADIC DAS/SDLC server

- ❖ Specify the server name of the DAS/SDLC server. This server is an OS/2 workstation near or within the robot cabinet, or a Windows server near the ADIC Scalar library.

ACSLS Host

ACSLS Host applies only to NetBackup Enterprise Server.

The ACS library software component can be any of the following:

- ◆ Automated Cartridge System Library Software (ACSLS)
See “Example 4: Configuring An ACS Robot on a Windows Server” on page 87.
- ◆ STK Library Station
- ◆ Storagenet 6000 Storage Domain Manager (SN6000).

This STK hardware serves as a proxy to another ACS library software component (such as, ACSLS).

Note STK LibAttach software must also be installed, if the device host that has drives under ACS robotic control is a Windows server. LibAttach for Windows is not available for servers running Windows 2003.

For an overview of ACS robots, see the appendix, “STK Automated Cartridge System (ACS)” on page 377.

▼ **To specify the ACSLS host for ACS robot types**

- ❖ Specify the name of the host where the ACS library software resides. On some UNIX server platforms, this host can also be a Media Manager device host or volume database host.

Robot control is attached to an NDMP host

This is a NetBackup Enterprise Server topic.

For this type of robot control, you specify the following two items.

- ◆ “Robot Device” on page 57
- ◆ “NDMP Host Name” on page 57

Robot Device

▼ **To specify the robot device**

1. Enter the name of the robotic device that is attached to the NDMP host.
2. Click **Browse** to select a robot device from the list in the Devices dialog.

NDMP Host Name

▼ **To specify the host**

- ❖ Enter the name of the NDMP host where the robot is attached.

Adding Shared Drives

This is a NetBackup Enterprise Server topic.



Using the Device Configuration or the Shared Drive Media Manager wizards is recommended and is the easiest method for configuring drives in an SSO configuration. Each of these wizards guides you through the steps involved in configuring drives that will be shared among device hosts.

Determining which of the two wizards to use depends on the type of robot that controls the drives. VERITAS recommends the following:

- ◆ Use the Device Configuration wizard to configure shared drives when possible, rather than the Shared Drive wizard.
- ◆ Use the Shared Drive wizard with caution after initial device configuration.

There are also alternate ways that are available. In addition to configuring SSO faster, using these wizards eliminates many common mistakes made when SSO configuration is done using alternate methods.

See the following related topics:

- ◆ “Using the Device Configuration Wizard to Configure Shared Drives” on page 58
- ◆ “Using The Shared Drive Wizard to Configure Shared Drives” on page 59
- ◆ “Using Alternate Interfaces to Configure Shared Drives” on page 59
- ◆ “Shared Storage Option (SSO) Topics” on page 245

Using the Device Configuration Wizard to Configure Shared Drives

This is a NetBackup Enterprise Server topic.

Note When using the Device Configuration wizard in an SSO configuration, the limitations, supported devices, and device hosts are different than in a configuration without shared drives.

For TL8, TLD, or TLH robot types, VERITAS recommends using the Device Configuration wizard to add shared drives.

For ACS or TLM robot types you can use this wizard to configure shared drives, but some manual configuration is also involved. See “Configuring Shared ACS Drives” on page 382 and “Configuring Shared TLM Drives” on page 417.

See “The Device Configuration Wizard” on page 44 for more information and instructions on starting the wizard.

Using The Shared Drive Wizard to Configure Shared Drives

This is a NetBackup Enterprise Server topic.

The Shared Drive wizard can be used to configure shared drives in ACS, TL8, TLD, TLH, or TLM robots; to configure shared standalone drives, or to change an existing shared drive. This wizard has limited usage and does not configure robots.

Since this wizard does not use device serialization, it requires prior configuration details from you about your configuration before starting.

Learning More About the Shared Drive Wizard

You can obtain detailed information about this wizard before you start using the wizard, including what to expect in the wizard, a wizard overview, and limitations of the wizard.

▼ To learn about this wizard

1. Start the wizard (see “Starting the Shared Drive Wizard” on page 59).
2. From the welcome screen of the wizard, click **Help**.
3. When finished reviewing the help information in the wizard, exit the help and click **Cancel** to exit the wizard.

Starting the Shared Drive Wizard

Be sure to review the limitations of this wizard before starting. There are other possible ways to start this wizard (see “Changing the Configuration of a Drive” on page 70 and “Changing a Non-Shared Drive to a Shared Drive” on page 70).

▼ To start the shared drive wizard

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click **Actions > New > Shared Drive**.

Using Alternate Interfaces to Configure Shared Drives

There are alternatives available for configuring shared drives. These alternatives require manual configuration instead of using automated methods like device serialization and have an increased chance for configuration errors. Using one of the Media Manager device configuration wizards is recommended.



tpconfig menus

This topic applies only to NetBackup UNIX servers.

If you use `tpconfig`, make sure that

- ◆ All hosts that are sharing the drive use the same case-sensitive name for the drive (descriptive names are recommended).
- ◆ You define a common volume database host.

For more information about using this utility, see the `tpconfig` appendix of the UNIX NetBackup Media Manager system administrator's guide.

tpconfig Command Line Interface

If you use the `tpconfig` command interface, use the `-shared yes` option with the `-add -drive` or `-update -drive` commands when you are defining shared drives. See the NetBackup commands guide for details.

Adding Drives

Note Using the Device Configuration wizard is the recommended method of configuring drives. See “The Device Configuration Wizard” on page 44 for wizard restrictions and more information.

▼ To add drives

1. Complete the steps necessary for the server to recognize the attached drives (see “Performing Initial Device Configuration” on page 34).
2. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
3. Select **Actions > New > New Drive**.

The properties that appear in this dialog vary slightly, depending on the type of host platform and the robot type.

4. Specify the properties of the drive as explained in “Dialog Entries for Adding (or Changing Drives)” on page 62.
5. Click **OK**.

The display now shows the new drive information.

Note The initial drive status is up, so the drive is available as soon as you add it and restart `ltid`. To change the status of the drive, select **Device Monitor**.

A prompt appears asking whether you want to stop and restart the NetBackup Device Manager service (this also stops and restarts any robotic processes). If your changes are complete, answer yes to this prompt.

Note It is possible that stopping and restarting this service will abort any backups, archives, or restores that are in progress.

6. *This step applies only to NetBackup Enterprise Server.*

If the new drive was standalone, verify the volume database host setting and change it if necessary. See “Changing the Volume Database Host for Standalone Drives” on page 71.



Dialog Entries for Adding (or Changing Drives)

You specify properties when adding a drive or changing the properties of a drive. Note that some of these properties apply only to specific types of drives, server platforms, or NetBackup servers.

- ◆ “Device Host Section of the Dialog” on page 62
- ◆ “Drive Information Section of the Dialog” on page 62
- ◆ “Robotic Drive Information Section of the Dialog” on page 66

Device Host Section of the Dialog

“Device Host” on page 62 specifies the media server to which you are adding the drive.

Device Host

Device Host applies only to NetBackup Enterprise Server.

The host that is shown initially in the dialog box is the device host you selected earlier in the tree pane.

▼ To specify a different device host

- ❖ Click the **arrow** and select a host from the list.

▼ To specify a device host that is not in the list

1. Click New ...
2. In the dialog that appears, enter the name of the host.

Drive Information Section of the Dialog

Specifies specific information about the drive.

- ◆ “Drive Name” on page 63
- ◆ “Drive Type” on page 63
- ◆ “Device Name” on page 63
- ◆ “No Rewind Device” on page 63
- ◆ “Character Device” on page 64
- ◆ “Volume Header Device” on page 64

- ◆ “Cleaning Frequency” on page 65
- ◆ “Drive Is In A Robotic Library” on page 65

Drive Name

This name is used to identify the drive. It is important to note that each drive name *must be* unique. Descriptive names are recommended.

▼ To specify the drive name

- ❖ Enter a name for the drive.

Drive Type

Specifies the type of drive that you are adding.

See “Media Manager Media Types” on page 277 for more information.

▼ To specify the drive type

- ❖ Click the **arrow** and select from the list of the drive types that Media Manager supports.

Device Name

Device Name applies only to drives on NetBackup Windows servers.

▼ To specify the device name

1. Find the device name for the drive from the appropriate Windows application.
2. Enter the name of the drive in the box as it is recognized by the Windows server.

▼ To select from the drives that are currently attached to the Windows server

1. Click **Browse ...**
2. Select a drive.

No Rewind Device

No Rewind Device applies only to drives on NetBackup UNIX servers.



Although both no rewind and rewind device files are usually available, Media Manager requires only the no rewind on close device file.

Device files are located in the `/dev` directory on the UNIX host. If the device files do not exist, create them as explained in the NetBackup Media Manager device configuration guide.

A no rewind device remains at its current position on a close operation. Usually the device file name is preceded or followed by the letter `n`.

If you are using NDMP drives, see the NetBackup for NDMP system administrator's guide for configuration information.

▼ To specify the no rewind device file

- ❖ Enter the no rewind device file path for the drive.

▼ To select a no rewind device file

- ❖ Click the button on the right to display a dialog from which you can select a device file.

Character Device

Character Device applies only to optical disk drives on NetBackup UNIX servers.

Character device files are in the `/dev` directory on the UNIX host. If the entries do not exist, you can create them as explained in the NetBackup Media Manager device configuration guide. Media Manager uses character mode device files.

▼ To specify the character device

- ❖ Enter the character device file path for the drive.

Volume Header Device

Volume Header Device applies only to optical disk drives on NetBackup UNIX servers.

Volume header device files are in the `/dev` directory on the UNIX host. If the entry does not exist, you need to create it as explained in the NetBackup Media Manager device configuration guide.

▼ To specify the volume header device

- ❖ Enter the volume header device path for the drive.

Cleaning Frequency

Cleaning Frequency does not apply to shared drives or to any robots that do not support frequency-based cleaning.

If you want to set up a frequency-based cleaning schedule for the drive, set the number of mount hours between each drive cleaning. When you add a drive or reset the mount time to zero, Media Manager starts recording the amount of time that volumes have been mounted in that drive.

If you do not specify a cleaning frequency (the default frequency is zero), you can still utilize automated drive cleaning with the TapeAlert feature, provided all of the following conditions have been met:

- ◆ The robot supports TapeAlert.
- ◆ A cleaning volume has been defined in Media Manager.
- ◆ The host platform, robot type, and drive support drive cleaning.

If the drive is in a robotic library that supports drive cleaning and a cleaning cartridge is defined in that robotic library, cleaning occurs when the accumulated mount time exceeds the time you specify for cleaning frequency. The mount time is reset when the drive is cleaned.

See “Drive Cleaning Functions” on page 73 for information on resetting the mount time and initiating an operator-initiated cleaning of a drive. You can also perform these drive cleaning functions from the Device Monitor, in addition to setting or changing the cleaning frequency.

▼ To specify a cleaning frequency

- ❖ Click an **arrow** and select the number of hours.

Drive Is In A Robotic Library

▼ To specify that a drive is under robotic control

1. Select **Drive is in a robotic library**.
2. Enter additional information about the drive in the **Robotic drive information** section (see “Robotic Drive Information Section of the Dialog” on page 66).

▼ To specify that a drive is a standalone (non-robotic) drive

- ❖ Clear **Drive is in a robotic library**.



Robotic Drive Information Section of the Dialog

Specifies information about a drive in a robotic library.

- ◆ See “Robotic Library” on page 66
- ◆ See “Robot Drive Number” on page 66

Robotic Library

This dialog box allows you to select any currently configured robotic library that can control the drive.

▼ To specify the library

- ❖ Click the **arrow** and select a robotic library from the list.

Robot Drive Number

Robot drive number specifies the physical location in the robot of the drive that you are adding. When adding more than one drive to a robot, you can add the physical drives in any order. For example, in a TS8 robot you can add drive 2 before drive 1.

If you assign the wrong number Media Manager does not detect it, but an error will occur when the robotic control attempts to mount media on the wrong drive.

Note **Robot drive number** does not apply when adding drives to API robots. See “Robot drive number for API Robots” on page 66.

▼ To specify the robot drive number

1. Determine the correct robot drive number. You must determine which physical drive in the robot is identified by the logical device name (on Windows servers) or the device file (on UNIX servers).

See “Correlating Device Files to Physical Drives When Adding Drives” on page 306 for more information.

2. Click an **arrow** and select a number for the drive.

Robot drive number for API Robots

The following topic applies to NetBackup Enterprise Server.

Robot drive number does not apply when adding drives to the following types of API robots:

- ◆ ACS robots (Automated Cartridge System). See “ACS” on page 67 for more information.
- ◆ TLH robots (Tape Library Half-inch). See “TLH” on page 67 for more information.
- ◆ TLM robots (Tape Library Multimedia). See “TLM” on page 68 for more information.

ACS

▼ To specify a drive in an ACS robot

1. Determine the physical location of the drive within the robot. You must know which physical drive in the robot is identified by the device files that you specified earlier. You establish this correlation during installation.

The appendix, “STK Automated Cartridge System (ACS)” on page 377, has further information.

2. Select **ACS**.
3. In the dialog enter the following information:

For	Enter
ACS Number	The index (in ACS library software terms) that identifies the robot that has this drive.
LSM Number	The Library Storage Module that has this drive.
Panel Number	The robot panel where this drive is located.
Drive Number	The physical number of the drive (in ACS library software terms).

If you assign the wrong parameters for the drive, Media Manager does not detect it, but an error will occur when the robot mounts media on the wrong drive.

TLH

▼ To specify a drive in a TLH (Tape Library Half-inch) robot

1. Select **TLH**.
2. In the dialog, enter the IBM device number of the drive within the robot.



If you assign the wrong device number Media Manager does not detect it, but an error will occur when the robot mounts media on the wrong drive.

The appendix, “IBM Automated Tape Library (ATL)” on page 399, has further information.

TLM

▼ To specify a drive in a TLM (Tape Library Multimedia) robot

1. Select **TLM**.
2. In the dialog, enter the DAS/SDLC drive name of the drive within the robot.

If you assign the wrong drive name Media Manager does not detect it, but an error will occur when the robot mounts media on the wrong drive.

The appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 411, has further information.

Managing Your Device Configuration

The following topics explain how to manage the robots and drives in your configuration:

- ◆ “When to Perform Device Configuration Changes” on page 69
- ◆ “Using the Device Configuration Wizard for Configuration Changes” on page 69
- ◆ “Changing a Robot Configuration” on page 69
- ◆ “Changing the Configuration of a Drive” on page 70
- ◆ “Deleting Robots” on page 72
- ◆ “Deleting Drives” on page 72
- ◆ “Drive Cleaning Functions” on page 73
- ◆ “Performing Drive Diagnostics” on page 74
- ◆ “Using SANPoint Control to Investigate SAN Problems” on page 77
- ◆ “Printing Your Device Configuration” on page 78

The following topics apply only to NetBackup Enterprise Server.

- ◆ “Changing a Non-Shared Drive to a Shared Drive” on page 70
- ◆ “Changing the Volume Database Host for Standalone Drives” on page 71

Also see “Making Changes to Your Hardware Configuration” on page 335 for advanced configuration topics.

When to Perform Device Configuration Changes

Device configuration tasks should not be attempted when any backups or restores are running. When performing many of the following device configuration tasks, a prompt at the end of the procedure asks if you want to stop and restart `ltid`.

This action also stops and restarts any robotic processes. `ltid` is the Media Manager device daemon on UNIX and the NetBackup Device Manager service on Windows servers.

If your configuration changes are complete and you are not in a production environment, answer yes to this prompt.

Caution Stopping and restarting `ltid` may abort any backups, archives, or restores that are in progress.

Using the Device Configuration Wizard for Configuration Changes

Using or rerunning the Device Configuration wizard updates your Media Manager configuration to match any configuration changes. See “The Device Configuration Wizard” on page 44. For example, adding a new SCSI adapter may change the path to a robotic library. A similar change to the configuration may occur if you add a new drive or robotic library.

Changing a Robot Configuration

▼ To change configuration information for a robot

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Robots** tab in the Devices pane.
3. Select the robotic library you want to change.
4. Select **Edit > Change**.

A dialog appears, showing the current information for the selected robotic library.



5. Make your changes (see “Dialog Entries for Adding and Changing Robots” on page 48).
6. Click **OK**.

Changing the Configuration of a Drive

▼ To change configuration information for a drive

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Drives** tab in the Devices pane.
3. Select the drive you want to change.
4. Select **Edit > Change**.
 - a. A dialog appears showing the current information for the selected drive. Make your changes (refer to “Dialog Entries for Adding (or Changing Drives)” on page 62).
 - b. *This step applies only to NetBackup Enterprise Server.*

If the drive you selected is a shared drive, the Shared Drive wizard is started to guide you through the steps involved in changing the configuration of the drive. Follow the wizard prompts.
 - c. Click **OK**.

Changing a Non-Shared Drive to a Shared Drive

This is a NetBackup Enterprise Server topic.

An SSO license is required on each master and media server (or SAN media server) to configure and use a shared drive.

▼ To change a drive to a shared drive

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Drives** tab in the Devices pane.

3. Select the non-shared drive that you want to change.
4. Right-click and select **Configure Shared Drive** on the shortcut menu.

The Shared Drive wizard is started to guide you through the steps involved in changing the drive to be a shared drive.

If the drive you selected is currently a shared drive, the Shared Drive wizard guides you through the steps involved in changing the configuration properties of the drive.

Follow the wizard prompts.

Changing the Volume Database Host for Standalone Drives

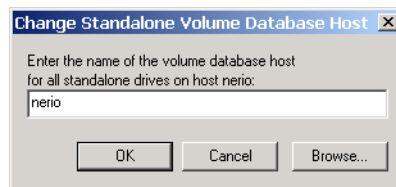
This is a NetBackup Enterprise Server topic.

All standalone drives on a specific host always use the same volume database.

▼ To change the volume database host

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Hosts** tab in the Devices pane.
3. Select the host you want to change.
4. Select **Actions > Change Standalone Volume Database Host**.

A dialog appears showing the current volume database host.



5. To change the host enter the new host name in the text box (or select a new host by clicking **Browse**).

You can enter the name of any server that has Media Manager installed, even if it does not have any attached drives. However, VERITAS recommends that you use a single volume database host for all your volumes (robotic and standalone). It is possible to maintain separate volume databases on multiple servers, but administration is more difficult.



See “Media and Device Management Domain Management” on page 271 for more information.

6. Click **OK**.

Deleting Robots

Note Any drives that are configured as residing in a robot that you delete will be changed to standalone drives.

▼ To delete a robot

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Robots** tab in the Devices pane.
3. Select the robotic library you want to delete.
4. Select **Edit > Delete**.
5. Answer the delete confirmation dialog.

Deleting Drives

▼ To delete a drive

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Drives** tab in the Devices pane.
3. Select the drive you want to delete.
4. Select **Edit > Delete**.
5. Answer the delete confirmation dialog.

Drive Cleaning Functions

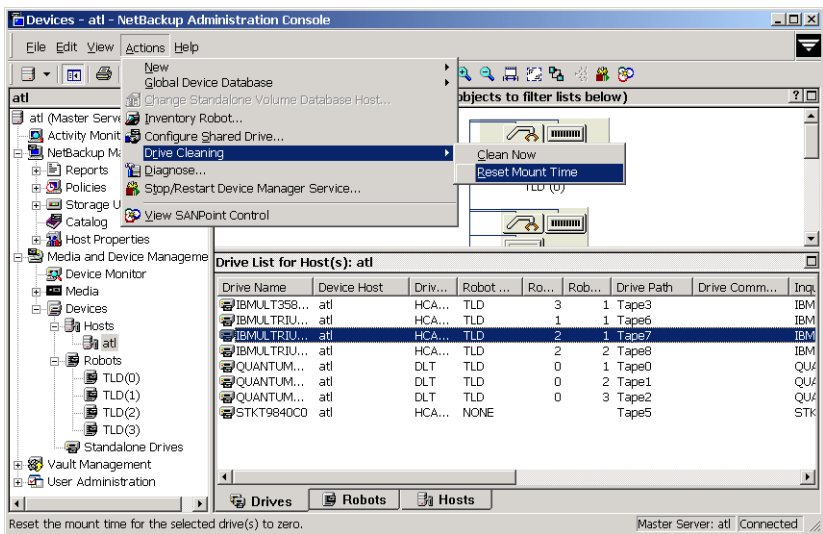
See “Drive Cleaning” on page 309 for background information on types of drive cleaning and cleaning tapes.

To add a cleaning tape, perform “Adding New Volumes” on page 119 and specify a cleaning tape as the media type.

Note You can also perform these drive cleaning functions from the Device Monitor. In addition, you can set or change the cleaning frequency from the Device Monitor. See “Drive Cleaning Functions” on page 234.

▼ To perform drive cleaning functions

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select the **Drives** tab in the Devices pane.
3. Select the drive that you want to clean.
4. Select **Actions > Drive Cleaning**.



The sub-menu choices allow you to perform the following functions:

Select	To
Clean Now	Start an operator-initiated cleaning of the selected drive, regardless of the cleaning frequency or accumulated mount time. If the drive is a standalone drive, it must contain a cleaning tape and a mount request will be issued. Clean Now resets the mount time to zero, but the cleaning frequency value remains the same.
Reset Mount Time	Reset the mount time for the selected drive to zero. Use Reset Mount Time to reset the mount time after doing a manual cleaning of a drive.

To change the cleaning frequency, see Cleaning Frequency in “Dialog Entries for Adding (or Changing Drives)” on page 62 or use the drive cleaning functions in the Device Monitor.

5. Updated drive cleaning information is presented in the Drives List. See “Devices Pane” on page 25 for information about the contents of the Drives List.

Note The **Clean Now** function may take several minutes to complete, so the cleaning information in the Drives List may not be updated immediately. You may also need to refresh the Drives List display.

Performing Drive Diagnostics

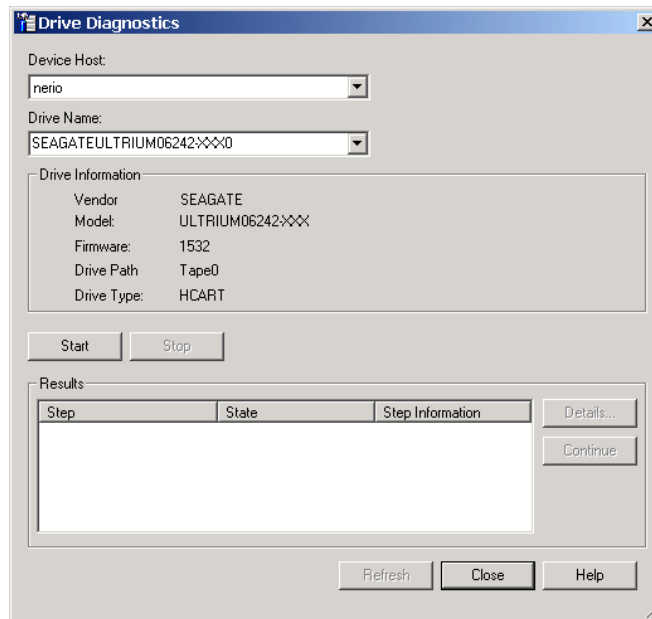
Media Manager drive diagnostic functions allow you to execute and manage drive diagnostic tests. The diagnostic test steps are executed in an ordered sequence to verify the functionality of hardware devices configured for use with NetBackup. These tests should help you to troubleshoot tape drive problems.

Executing Diagnostic Tests for a Drive

▼ To execute tests

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Select **Actions > Diagnose...**

A dialog appears that contains Drive Information and Results sections. This dialog allows you to execute and manage the drive diagnostics tests.



3. Select the media server that has the drives that you want to test in the Device Host box.
4. For the drive that you want to test, do the following:
 - a. Manually set the drive state to DOWN.
 - b. Manually insert a pre-labeled test tape with a NetBackup recorded label into the drive.
 - c. In the Drive Name box, select the drive.

Information for the drive you selected is displayed in the Drive Information section.

5. Click **Start** to start the diagnostic tests.

The results of each step in the test are shown in the Results display. Click **Refresh** to update the Results display



Exiting a Diagnostic Test When Testing is Complete

▼ To exit tests

- ❖ Click **Close**.

If a test is still executing, an exit confirmation dialog appears.

Stopping a Diagnostic Test and Changing the Drive to be Tested

▼ To stop tests

1. Click **Stop**.

The test will terminate after performing any necessary clean-up work and updating the test records to reflect that the test run has been stopped.

2. In the Device Host and the Drive Name boxes, select the host and the drive that you want to test.
3. Click **Start** to restart the diagnostic test.

Obtaining Detailed Information For a Particular Test Step

You can get information for a test step at any time during the test.

▼ To obtain information

1. Select a test step in the Results section.
2. Click **Details...** A dialog appears that displays detail information for the step.

The information includes a brief explanation of the checks performed by a specific step and the instructions associated with any step that requires manual intervention. For example, a step may prompt for a new tape to be loaded into a tape drive before allowing the diagnostic session to continue with further qualification tests.

3. Click **Close** to return to the Drive Diagnostics dialog.

Managing a Test Step that Requires Operator Intervention

Operator intervention is required if the Status column of the Results display contains *Waiting*. For example, a test step may prompt for a new tape to be loaded into a drive before allowing the test to continue.

▼ To manage a test that needs intervention

- 1. Complete the requested operations task.
- 2. Click **Continue** to resume the test.

If you click **Details** for a test step that requires operator intervention, you can also click **Continue** from the Test Details dialog to resume the test.

Using SANPoint Control to Investigate SAN Problems

SANPoint Control allows you to check for intermittent drive failures, and to see what types of SAN errors may be happening to help you diagnose problems that cause NetBackup to fail. The following table shows some typical problems and the benefits of using SANPoint Control:

Apparent NetBackup Problem	SANPoint Control Advantage
NetBackup shows that a device is up, but the backups to that device continually fail.	Select the device and launch SANPoint Control. This allows you to see if the device is still connected to the SAN, or if there are other SAN problems that have made the device unavailable, yet technically still up.
A NetBackup backup job fails intermittently and the drive is also downed intermittently. There are no errors in the NetBackup error log other than the job failed.	Select the drive and launch SANPoint Control to determine if the drive is attached. Check the alerts to see if there was a SAN problem that could have affected the drive during the time the job failed.
The NetBackup configuration was working fine and no configuration changes were made. Later NetBackup does not recognize the robots and drives that were previously recognized.	Launch SANPoint Control to check for any differences in the SAN since the time the installation was running correctly and the present. SANPoint Control can provide a snapshot of changes made in a SAN (you supply a start and finish time). The snapshot may show a switch failure, or show that the SAN was re-zoned and the desired device is no longer in a zone that NetBackup can reach.
The NetBackup administrator installs a new device and runs the Device Configuration wizard to configure it. The wizard does not recognize the newly installed device.	Launch SANPoint Control from the Drag and Drop Configuration screen of the wizard. The device does not appear in the SPC topology. If SANPoint Control cannot see the device as connected to the SAN, you should verify the connection.



▼ **To launch SANPoint Control**

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.

Note You can also launch SANPoint Control from the Device Monitor (click **Media and Device Management > Device Monitor**).

If there is a device selected in the Devices pane, SANPoint Control will be launched with the device as context. If there is no device selected, then SANPoint Control will be launched with the host as the context.

2. Select **Actions > View SANPoint Control**.
3. The SANPoint Control browser is launched. See your SANPoint Control documentation for information on usage.

If SANPoint Control is not installed, a message appears explaining how to enable it.

▼ **To access SANPoint Control reports**

The SANPoint Control reports allow you to check for intermittent failures of drives, and to see what types of SAN errors may be happening to help you diagnose problems.

1. In the NetBackup Administration Console, click **NetBackup Management > Reports**.
2. Select **Actions > View SANPoint Control Reports**.

This will launch a browser with the main reports screen. See your SANPoint Control documentation for more information.

Printing Your Device Configuration

▼ **To print your current device configuration**

1. In the Devices pane, click on **Drives, Robots, or Hosts**.
2. Select **File > Print**.

▼ **To print the device configuration topology diagram**

1. Click in the Topology pane.
2. Select **File > Print**.

▼ To print your current device configuration using tpconfig

The tpconfig command is located in *install_path*\Volmgr\bin\.

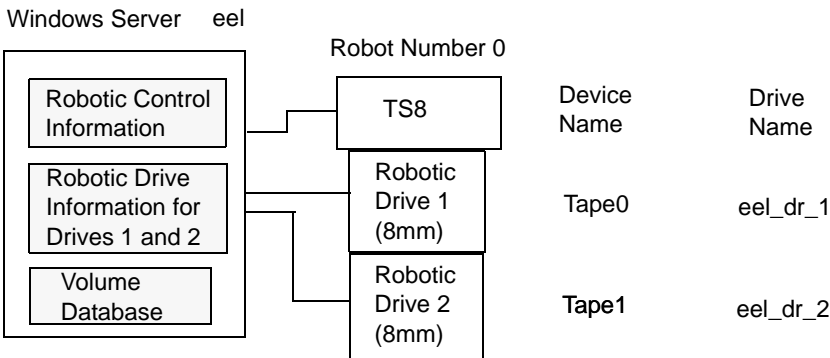
The following example uses tpconfig to list the device configuration and redirect the output to the file named devconf.txt, which can then be printed:

```
tpconfig -dl > devconf.txt
```

Note tpconfig -d and tpconfig -l may truncate drive names. Use tpconfig -dl to obtain the full drive name.

Robot and Drive Configuration Examples

Example 1: Configuring a Robot on a Server



This configuration has a tape stacker containing two 8mm tape drives. The robot and drives are connected to a server running Microsoft Windows.



After installing Media Manager software and attaching the drives, run the Device Configuration wizard or complete the Add Robot and Add Drive dialog entries as shown in the following tables.

Add Robot Dialog Entries

Device Host	eel
Robot Type	TS8 (Tape Stacker 8MM)
Volume Database Host	eel
Robot Number	0
Robot is controlled locally by this device host	Set (cannot be changed for this robot type)
Robot Device	Selecting a robot device sets the SCSI Port, Bus, Target, and LUN numbers in the dialog for Windows NT servers and for other Windows servers where a changer driver <i>is not</i> in control of the robot. On Windows 2000 servers (and later supported operating system levels) where a changer driver <i>is</i> in control of the robot, selecting a robot device sets the changer name in the dialog.

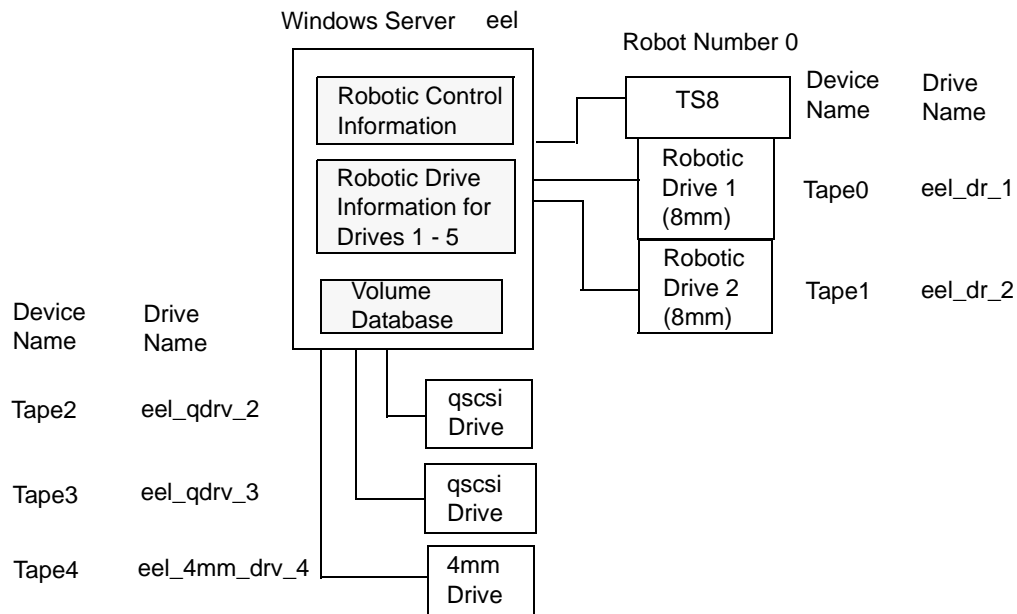
Add Drive Dialog Entries (Tape0)

Device Host	eel
Drive Name	eel_dr_1
Drive Type	8mm Cartridge (8mm)
Device Name	Tape0
Cleaning Frequency	0 (hours)
Drive is in a Robotic Library	Yes
Robotic Library	TS8(0) - eel
Robot Drive Number	1

Add Drive Dialog Entries (Tape1)

Device Host	eel
Drive Name	eel_dr_2
Drive Type	8mm Cartridge (8mm)
Device Name	Tape1
Cleaning Frequency	0 (hours)
Drive is in a Robotic Library	Yes
Robotic Library	TS8(0) - eel
Robot Drive Number	2

Example 2: Configuring Standalone Drives on a Server



This example adds three standalone drives to the device configuration for the host eel that was shown in Example 1. As in that example, the volume database and all devices are on the same server. The following tables show the Add Drive dialog entries for the standalone drives. Configuration information for the robot and its two drives is the same as in “Example 1: Configuring a Robot on a Server” on page 79 and is not repeated here.

Add Drive Dialog Entries (Tape2)

Device Host	eel
Drive Name	eel_qdrv_2
Drive Type	1/4" Cartridge (qscsi)
Device Name	Tape2
Drive is in a Robotic Library	No

Add Drive Dialog Entries (Tape3)

Device Host	eel
Drive Name	eel_qdrv_3
Drive Type	1/4" Cartridge (qscsi)
Device Name	Tape3
Drive is in a Robotic Library	No

Add Drive Dialog Entries (Tape4)

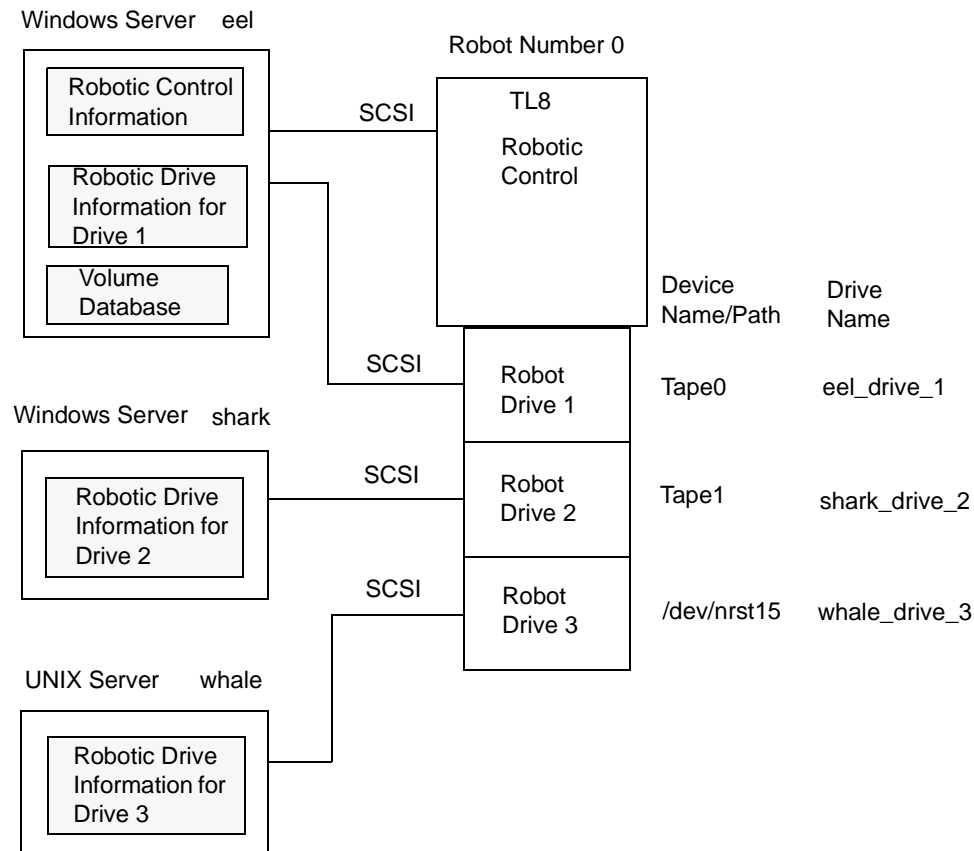
Device Host	eel
Drive Name	eel_4mm_drv_4
Drive Type	4mm Cartridge (4mm)
Device Name	Tape4
Cleaning Frequency	0 (hours)

Add Drive Dialog Entries (Tape4) (continued)

Drive is in a Robotic Library	No
-------------------------------	----

Example 3: Configuring a Robot Distributed Among Multiple Servers

The following example applies only to NetBackup Enterprise Server.



This is a more complex configuration than the previous examples because it involves a robot that has its robotic control on one server and its drives used by two other servers.

After installing Media Manager software and attaching the devices to the servers, run the Device Configuration wizard or complete the Add Robot and Add Drive dialog entries as shown in the following tables. Some things to note when examining these tables follow:



- ◆ Media for all devices is configured in a common volume database, which is located on server eel.
- ◆ The Robot Number is 0 in all three cases. This is required because the three servers refer to the same physical robot. In this case, robotic control is on host eel.
- ◆ Robot Drive Numbers correlate to the physical drive assignment within the robot.
- ◆ When you add volumes, add them to host eel because the volume database is on that server.

Configuration on the Windows Server eel

Use the following entries in the Add Robot and Add Drive dialogs:

Add Robot Dialog Entries

Device Host	eel
Robot Type	TL8 (Tape Library 8MM)
Volume Database Host	eel
Robot Number	0
Robot is controlled locally by this device host	Set
Robot Device	Selecting a robot device sets the SCSI Port, Bus, Target, and LUN numbers in the dialog for Windows NT hosts and for other Windows servers where a changer driver <i>is not</i> in control of the robot. On Windows 2000 servers (and later supported operating system levels) where a changer driver <i>is</i> in control of the robot, selecting a robot device sets the changer name in the dialog.

Add Drive Dialog Entries (Drive 1)

Device Host	eel
Drive Name	eel_drive_1
Drive Type	8mm Cartridge (8mm)

Add Drive Dialog Entries (Drive 1) (continued)

Device Name	Tape0
Cleaning Frequency	0 (hours)
Drive is in a Robotic Library	Yes
Robotic Library	TL8(0) - eel
Robot Drive Number	1

Configuration on the Windows Server shark

Use the following entries in the Add Robot and Add Drive dialogs:

Add Robot Dialog Entries

Device Host	shark
Robot Type	TL8 (Tape Library 8MM)
Volume Database Host	eel
Robot Number	0
Robot control is handled by a remote host	Set
Robot Control Host	eel

Add Drive Dialog Entries (Drive 2)

Device Host	shark
Drive Name	shark_drive_2
Drive Type	8mm Cartridge (8mm)
Device Name	Tape1
Cleaning Frequency	0 (hours)



Add Drive Dialog Entries (Drive 2) (continued)

Drive is in a Robotic Library	Yes
Robotic Library	TL8(0) - eel
Robot Drive Number	2

Configuration on the UNIX Server whale

Use the following entries in the Add Robot and Add Drive dialogs:

Add Robot Dialog Entries

Device Host	whale
Robot Type	TL8 (Tape Library 8MM)
Volume Database Host	eel
Robot Number	0
Robot control is handled by a remote host	Set
Robot Control Host	eel

Add Drive Dialog Entries (Drive 3)

Device Host	whale
Drive Name	whale_drive_3
Drive Type	8mm Cartridge (8mm)
No Rewind Device	/dev/nrst15
Cleaning Frequency	20 (hours)
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TL8(0) - eel

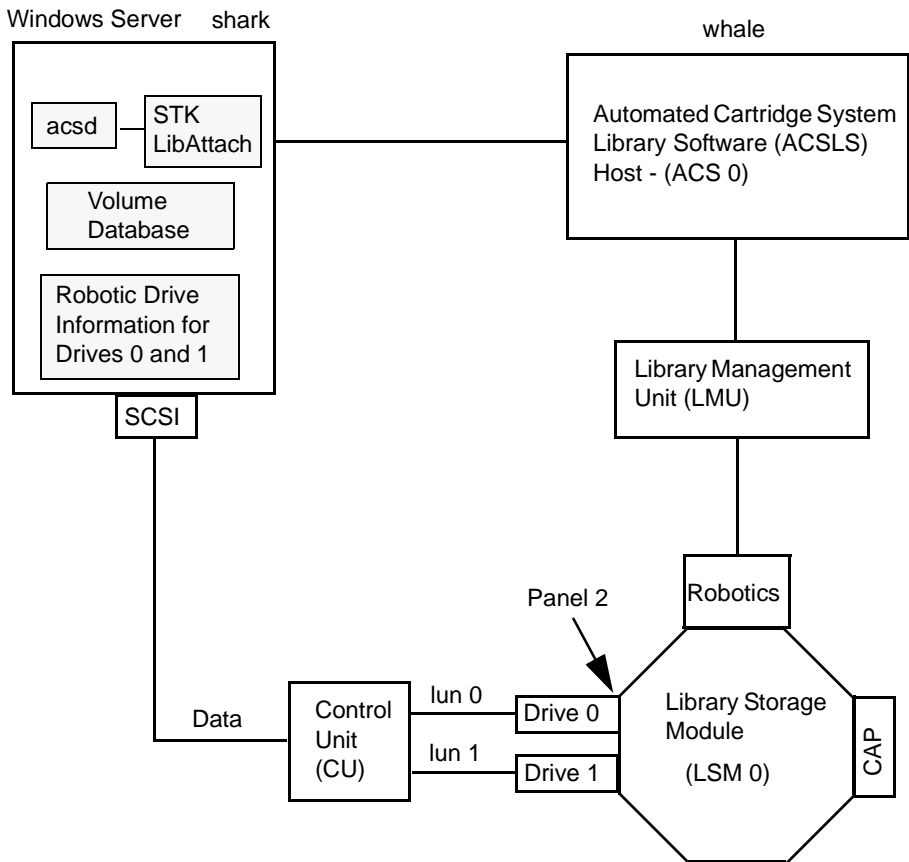


Add Drive Dialog Entries (Drive 3) (continued)

Robot Drive Number	3
--------------------	---

Example 4: Configuring An ACS Robot on a Windows Server

The following example applies only to NetBackup Enterprise Server.



This configuration uses an Automated Cartridge System (ACS) robot for storage. Server shark can be a Windows NetBackup master server or media server. The following tables show the Add Drive and Add Robot dialog entries for server shark. Items to note when reviewing these tables follow:

- ◆ The ACSLS host (in the Add Robot dialog) is host whale, where the ACS library software resides. In this example, Automated Cartridge System Library Software (ACSL) is installed as the ACS library software.



On some server platforms it may be possible to run Media Manager software and ACS library software on the same server, eliminating the need for two servers.

- ◆ The ACS, LSM, PANEL, and DRIVE numbers are part of the ACS library software configuration and must be obtained from the administrator of that host.
- ◆ Robot number and ACS number are different terms. Robot number is the robot identifier used in Media Manager. ACS number is the robot identifier in ACS library software. These numbers can be different, although they both default to zero.
- ◆ It is possible for the drives to connect through an independent control unit. If so, the correct Logical Unit Numbers (lun) are needed in order to find the correct tape name to use.
- ◆ The Add Robot dialog entries include an ACSLS Host entry, since communication with the ACS library software host is over the network using STK LibAttach software. This software must be installed on each Windows server that has ACS drives attached.

See the appendix, “STK Automated Cartridge System (ACS)” on page 377 for more information.

Add Robot Dialog Entries

Device Host	shark
Robot Type	ACS (Automated Cartridge System)
Volume Database Host	shark
Robot Number	0
Robot control is handled by a remote host	Set (cannot be changed for this robot type)
ACSLS Host	whale

Add Drive Dialog Entries (Drive 0)

Device Host	shark
Drive Type	1/2" Cartridge (hcart)
Drive Name	shark_drive_0
Device Name	Tape0



Add Drive Dialog Entries (Drive 0) (continued)

Drive is in a Robotic Library	Yes
Robotic Library	ACS(0) - whale
ACS	ACS: 0
	LSM: 0
	PANEL: 2
	DRIVE: 0

Add Drive Dialog Entries (Drive 1)

Device Host	shark
Drive Type	1/2" Cartridge (hcart)
Drive Name	shark_drive_1
Device Name	Tape1
Drive is in a Robotic Library	Yes
Robotic Library	ACS(0) - whale
ACS	ACS: 0
	LSM: 0
	PANEL: 2
	DRIVE: 1





This chapter explains how to use the media management window to add and manage the removable media that Media Manager controls. These media are referred to as volumes, and are assigned media IDs and other attributes that are used to track and manage them.

The chapter, “Managing Media in Robots” on page 153 explains how to manage media in robots.

If you have Backup Exec volumes to manage, see the Backup Exec tape reader topics in the NetBackup system administrator’s guides for Windows servers.

If you have volumes without barcodes to manage, see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 325.

See the following topics:

- ◆ “Starting Media Management” on page 92
- ◆ “Using the Media Management Window” on page 92
- ◆ “Configuring Volume Pools” on page 108
- ◆ “Methods Available for Injecting and Ejecting Volumes” on page 114
- ◆ “Adding New Volumes” on page 119
- ◆ “Using the Volume Configuration Wizard” on page 129
- ◆ “Moving Volumes” on page 130
- ◆ “When to Delete Volumes” on page 136
- ◆ “Ejecting Volumes From Robots (Actions Menu Command)” on page 137
- ◆ “Labeling Media” on page 139
- ◆ “Erasing Media Functions” on page 140
- ◆ “Deassigning Volumes” on page 142
- ◆ “Changing the Attributes for a Volume” on page 144
- ◆ “Changing the Volume Group of a Volume” on page 148
- ◆ “Exchanging Volumes” on page 149



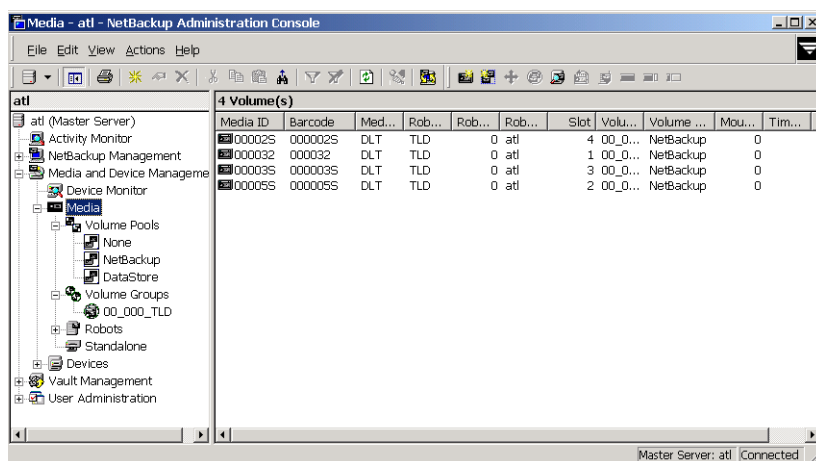
- ◆ “Recycling Volumes” on page 150

The following topics apply only to NetBackup Enterprise Server.

- ◆ “Administering Media on Other Servers” on page 106

Starting Media Management

In the NetBackup Administration Console, click **Media and Device Management** > **Media**. The media management window similar to the following appears:



In addition to the tree pane displayed on the left, a volume pane is displayed on the right when you start media management.

Using the Media Management Window

The following topics describe the media management window:

- ◆ “Menus and Commands” on page 93
- ◆ “Toolbars” on page 94
- ◆ “Tree Pane” on page 95
- ◆ “Volumes Pane” on page 96
- ◆ “Status Bar” on page 104
- ◆ “Shortcut Menus and Commands” on page 104
- ◆ “Customizing the Window” on page 105



- ◆ “Allowable Media Manager Characters” on page 105

Menus and Commands

The media management window contains the menus and commands shown in the following table.

The menu items are enabled and available based on the items that are currently selected in the tree pane or volumes pane. For example, if a volume group is selected in the tree pane, the **Delete** command is enabled on the **Edit** menu.

Media Management Menus and Commands

Menu	Commands
File	<p>Change Server - Displays a dialog that allows you to change to a different host that is running NetBackup. See “Managing Media on Other Servers” on page 107 for details.</p> <p>New Console - Starts another instance of NetBackup Administration Console.</p> <p>New Window from Here - Starts another instance of the NetBackup Administration Console node that was active.</p> <p>Login as New User - Log into NetBackup as a different user without exiting NetBackup. This is useful if a NetBackup Administrator wants to log in again as the Security Administrator to administer Access Management. Controlling access to NetBackup is discussed in the NetBackup system administrator’s guides.</p> <p>Backup, Archive, and Restore - Starts the NetBackup backup, archive, and restore GUI.</p> <p>MS SQL Client - Shortcut to access the SQL server NetBackup client, if it is installed on the selected host.</p> <p>Print Setup - Displays a setup dialog for printing.</p> <p>Print Preview - Previews the print image.</p> <p>Print - Prints the contents of the volumes pane.</p> <p>Close - Closes the current window.</p> <p>Exit - Closes all open windows.</p>
Edit	<p>Undo - Allows you to cancel the last action.</p> <p>Cut, Copy, Paste - Commands for managing items in the display lists.</p> <p>New - Displays a dialog to add a new item of the type that is currently selected.</p> <p>Change - Displays a dialog for changing the configuration of the selected items.</p> <p>Delete - Deletes selected items from the configuration.</p> <p>Find, Find Next, Find Prev, Find All - Commands for locating items in the display lists.</p>



Media Management Menus and Commands (continued)

Menu	Commands
View	Contains commands for specifying your viewing preferences for the media management window, including showing and hiding the toolbar or tree, sorting, filtering, column layout, and refreshing the display. See “Customizing the Window” on page 105.
Actions	New - Displays a dialog for adding volumes or volume pools to a configuration. Change Volume Group - Displays a dialog for changing the volume group for selected volumes. Move - Displays a dialog for moving volumes. Rescan/Update Barcodes - Rescans the barcodes in the selected robotic library and updates the barcodes for the selected volumes, as necessary. Eject Volume(s) From Robot - Ejects selected single or multiple volumes to the robot’s media access port. Label - Displays a dialog for labeling unassigned media. Long Erase - Displays a dialog to perform a full erase of unassigned media. Quick Erase - Displays a dialog to perform a short erase of unassigned media. Inventory Robot - Displays a dialog with choices for performing an inventory of the selected robot or updating the volume configuration to match the contents of the robot.
Help	Help Topics - Provides online help information for the NetBackup Console. Troubleshooter - Helps you to debug errors. VERITAS Web Page - Displays the VERITAS web page, if the host has a browser configured. License Keys - Provides information about your active and registered license keys. About Administration Console - Displays program information, version number, and copyright information. You can click More for detailed information. Current NBAC User - Provides NetBackup Access Control information for the current user. Gives the permissions for the user that you are currently logged in as.

Toolbars

The toolbar buttons of the Media window provide shortcuts for commands that are on the menus. Also see “Customizing the Window” on page 105.



▼ To show or hide the toolbar buttons

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. Click **View > Toolbar**.

▼ To customize the toolbar buttons

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. Click **View > Customize....**

In the **Customize Toolbar** dialog you can reorder the buttons on the current toolbar, add buttons, or remove toolbar buttons. Use **Default** to reset the buttons on the toolbar.

Tree Pane

The tree pane for **Media** contains nodes for **Volume Pools**, **Volume Groups**, **Robots**, and **Standalone**.

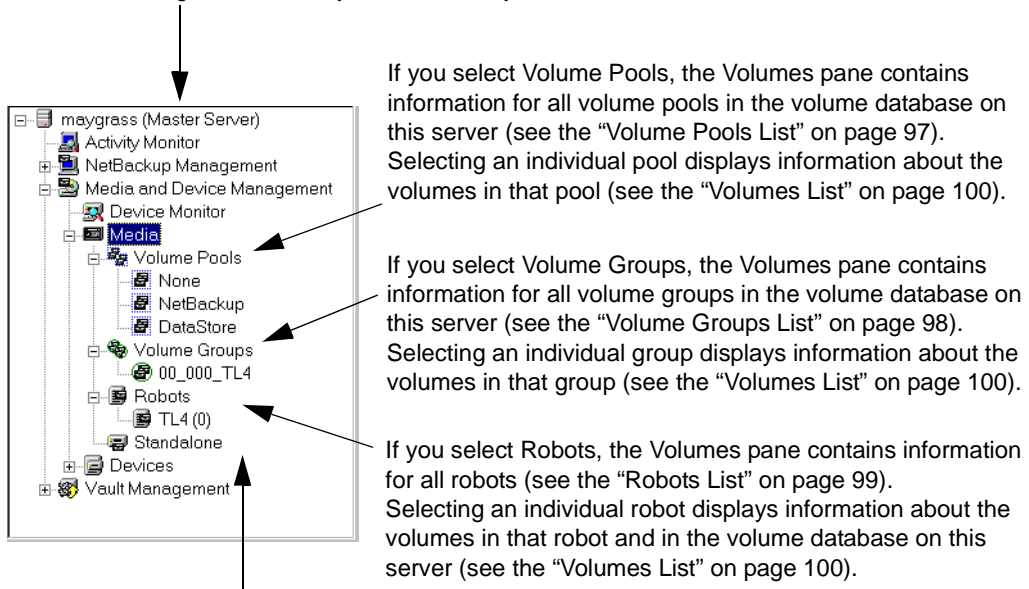
The display in the Volumes pane (the pane on the right) shows the volumes that are in the volume database on this server. If you add any volumes, they are added to this volume database.

If there are no volumes configured in the volume database, the Volumes pane will be blank. Selecting different items in the tree pane filters the lists that are shown in the Volumes pane.



The following figure shows an expanded view of the Media tree pane:

The Media Manager server that you are currently connected to.



If you select Standalone, the Volumes pane contains information for all the volumes that are configured for use with standalone drives and in the volume database on this server (see the Volumes List).

The following points apply to NetBackup Enterprise Server.

Before adding volumes on the selected server, check the volume database host setting for the robot or standalone drive to verify that the volume will be added to the correct volume database. See “Administering Media on Other Servers” on page 106.

If the icon shown for a robotic library contains a red arrow, the current server is *not* the volume database host for the robotic library.

You can view or configure volumes on another master or media server. See “Administering Media on Other Servers” on page 106 for more information.

Volumes Pane

This pane lists the volumes in the volume database located on the current media server (or SAN media server).

▼ To manage the lists in the Volumes Pane

1. The **Edit** menu has commands for finding items and is useful if you are managing many volumes.
2. You can also use **View > Columns > Layout** to rearrange or hide specific columns in the Volumes pane. Some of the columns are hidden initially by default.

The following tables describe the columns in the various volume lists.

- ◆ “Volume Pools List” on page 97
- ◆ “Volume Groups List” on page 98
- ◆ “Robots List” on page 99
- ◆ “Volumes List” on page 100

Volume Pools List

▼ To view the volume pools list

- ❖ Select **Media > Volume Pools** in the tree pane.

The following information for all of the volume pools is then displayed in the Volumes Pane.

Volume Pools List

Column	Description
Volume Pool	<p>Name of the volume pool. Volumes in a pool are grouped together for use by a single application and are protected from access by other applications and users. The following volume pool names are reserved:</p> <ul style="list-style-type: none"> ◆ None is the default pool for users of applications, other than NetBackup and Storage Migrator. ◆ NetBackup is the default pool name for NetBackup. ◆ DataStore is the default pool name for DataStore. ◆ HSM is the default pool name for VERITAS Storage Migrator.
Number	<p>Number assigned to the volume pool. This number is assigned by NetBackup. The following numbers are reserved:</p> <ul style="list-style-type: none"> ◆ 0 is the None (default) pool. ◆ 1 is the NetBackup pool. <p>The DataStore pool is assigned the next available pool number.</p>



Volume Pools List (continued)

Column	Description
User	Contains the value ANY or the user ID (for example, root(0)).
Host	Name of the host that is allowed to request and use the volumes in this volume pool or the value ANYHOST.
Group	Identifies the UNIX user group for this volume pool or contains the value NONE.
Description	Description for the volume pool. You add the description when you configure a volume pool.
Scratch	Contains Yes, if the volume pool is the scratch volume pool. Contains No, if the volume pool is not the scratch volume pool. NetBackup allows only one scratch pool.

Volume Groups List

▼ To view the volume groups list

- ❖ Select **Media > Volume Groups** in the tree pane.

The following information for all of the volume groups is then displayed in the Volumes Pane.

Volume Groups List

Column	Description
Volume Group	<p>Name of the volume group. A volume group defines the volume by location and is a logical group of volumes that are at the same physical location.</p> <p>Volume groups are a convenience for administrating multiple volumes. By using a volume group, you can logically move a set of volumes between a robotic library and a standalone location, or delete them by specifying the group name rather than specifying each individual media ID.</p> <p>More than one volume group can share the same location. For example, a robotic library can contain volumes from more than one volume group and there can be more than one standalone volume group. All volumes in a volume group must have a compatible media type.</p>
Media Type	Media Manager media type of the volume group.

Volume Groups List (continued)

Column	Description
Robot Number	Number of the robot that contains this volume group. If the robot type is NONE, this column contains a hyphen (-).
Robot Type	Type of robot that contains this volume group. NONE in this column means a standalone volume group.
Robot Control Host	Name of the robot control host for the volumes in this volume group. If the robot type is NONE, this column contains a hyphen (-).
Volume Count	Number of volumes in this volume group.

Robots List

▼ To view the robots list

- ❖ Select **Media > Robots** in the tree pane.

The following information for all of the robots is then displayed in the Volumes Pane. Review the Note column for any restrictions.

Robots List

Column	Description	Note
Robot Name	The name of the robot (comprised of the robot type and robot number), for example TLD(3).	
Device Host	The name of the device host where this robot is defined.	
Robot Type	Type of robot that contains this volume. See “Media Manager Robot Types” on page 276 for a list of supported robot types.	
Robot Number	Number of the robot.	
Volume Database Host	The name of the volume database host for the volumes in this robot.	
Serial Number	The serial number of the robot.	



Robots List (continued)

Column	Description	Note
Robot Control Host	Name of the host that is providing the robotic control. This column contains a host name only for robots where the robot control is handled by a different host than the host where the robot is attached.	Applies only to NetBackup Enterprise Server.
Inquiry Information	Contains device information returned from the device. This information is used to identify the device. For example, vendor ID, product ID, and product revision.	

Volumes List

▼ To view the volumes list

- ❖ Select an item under **Volume Pools**, **Volume Groups**, **Robots**, or **Standalone** in the tree pane.

The volumes list is filtered based on the selected item and that information is displayed in the Volumes pane. Review the Note column for any restrictions.

Volumes List

Column	Description	Note
Media ID	A Media Manager ID that identifies the volume in six or less alphanumeric characters. The media ID is specified when you add volumes or generated when you use a robot inventory to add volumes.	
Barcode	The alphanumeric representation of the barcode label attached to a volume. A barcode is used to identify the volume.	
Media Type	Media type of the volume. See “Media Manager Media Types” on page 277 for a list of the supported media types.	
Robot Type	Type of robot that contains this volume. See “Media Manager Robot Types” on page 276 for a list of supported robot types. NONE in this column means a standalone volume.	

Volumes List (continued)

Column	Description	Note
Robot Number	Number of the robot that contains this volume. If the volume is for a standalone drive or the volume is part of a group that was moved out of a robot (with the intent of being moved back into a robot), this column contains a hyphen (-).	
Robot Control Host	Name of the host that controls the robot that contains this volume. This host is providing the robotic control. If this column contains NONE, there is no specific robot control host (the robot is controlled from multiple hosts). If this column is blank, the volume is for a standalone drive.	Applies only to NetBackup Enterprise Server.
Slot	Slot in the robot that contains the volume. This column is blank for API robots, since Media Manager does not track slot information for these robots. For API robots, the robot vendor (or operating system software in the case of RSM robots) tracks the slot information.	
Volume Group	Name of the volume group for this volume. See “Volume Groups List” on page 98 for more information.	
Volume Pool	The volume pool defines the usage for the volume. Volumes in a pool are grouped together for use by a single application and are protected from access by other applications and users. See “Volume Pools List” on page 97 for more information. None is the default pool name for users of applications, other than NetBackup, DataStore, and Storage Migrator. <ul style="list-style-type: none"> NetBackup is the default pool name for NetBackup. DataStore is the default pool name for DataStore. HSM is the default pool name for VERITAS Storage Migrator. 	
Mounts	Number of times that the volume has been mounted (does not apply to cleaning media types).	
Time Assigned	Shows the date when the volume was assigned for use. You cannot delete a volume or change its volume pool while it is assigned to an application.	



Volumes List (continued)

Column	Description	Note
Status	<p>Status applies only to volumes that are assigned to NetBackup, Storage Migrator, or Storage Migrator for Microsoft Exchange.</p> <p>There is also a date in the Time Assigned column for assigned volumes. Values for status are as follows:</p> <ul style="list-style-type: none">♦ 0 - NetBackup The volume is assigned to NetBackup regular backups.♦ 1 - Catalog The volume is assigned to NetBackup catalog (database) backups.♦ 2 - Storage Migrator The volume is assigned to Storage Migrator for UNIX.♦ 3 - Storage Migrator The volume is assigned to Storage Migrator for Microsoft Exchange or Storage Migrator for Windows.	
Side/Face	<p>Location of the volume.</p> <p>If the media type is an optical disk, this column shows A or B, representing the platter side on which the volume is located.</p> <p>For any other media type, this column contains a hyphen (-).</p>	
Partner	<p>For optical disks, this column shows the media ID of the volume on the other side of the optical platter. For all other media types, the column contains a hyphen (-). You define this value as Partner ID when you add the volume.</p>	
Max Mounts	<p>Number of times the volume can be mounted. 0 in this column refers to unlimited mounts. If the maximum mounts value is reached, a message is logged to the system application log and Media Manager allows no further mounts in write mode. Further mounts in read mode are allowed.</p>	
First Mount	<p>Date and time that the volume was first mounted by Media Manager.</p>	
Last Mount	<p>Date and time that the volume was last mounted by Media Manager.</p>	

Volumes List (continued)

Column	Description	Note
Expiration Date	Indicates the age of the volume. If the expiration date is reached, the volume is considered too old to be reliable and Media Manager allows no further mounts in write mode. Further mounts in read mode are allowed, but a message is logged to the system application log indicating that the expiration date has been reached. If the column is blank, the volume has no expiration date.	
Cleanings Remaining	For a cleaning tape, this column shows how many more times the tape can be used. To use a cleaning tape, the value in this column must be greater than zero. You can change this count by selecting the volume and using Edit > Change .	
Created	Date and time that the volume was added to Media Manager.	
Description	Describes the media in 25 or less alphanumeric characters. You specify a description when you add volumes.	
Vault Name	Contains the name of the vault where this volume is located.	Applies only to the NetBackup Vault option.
Date Vaulted	Contains the date this volume was sent to the vault.	Applies only to the NetBackup Vault option.
Return Date	Contains the date when this volume returns from the vault.	Applies only to the NetBackup Vault option.
Vault Slot	Contains the location where this volume is stored in the vault.	Applies only to the NetBackup Vault option.
Session ID	Contains the ID of the vault session that ejected this volume.	Applies only to the NetBackup Vault option.
Vault Container ID	Contains the ID of the container where this volume is stored.	Applies only to the NetBackup Vault option.



Status Bar

The status bar appears at the bottom of the NetBackup Console window. The status bar

- ◆ Shows tool tips (when the mouse is over a toolbar icon or an object).
- ◆ Indicates the name of the master server.
- ◆ Indicates if you are connected to the master server.

▼ To show or hide the status bar

- ❖ Click **View > Status Bar**.

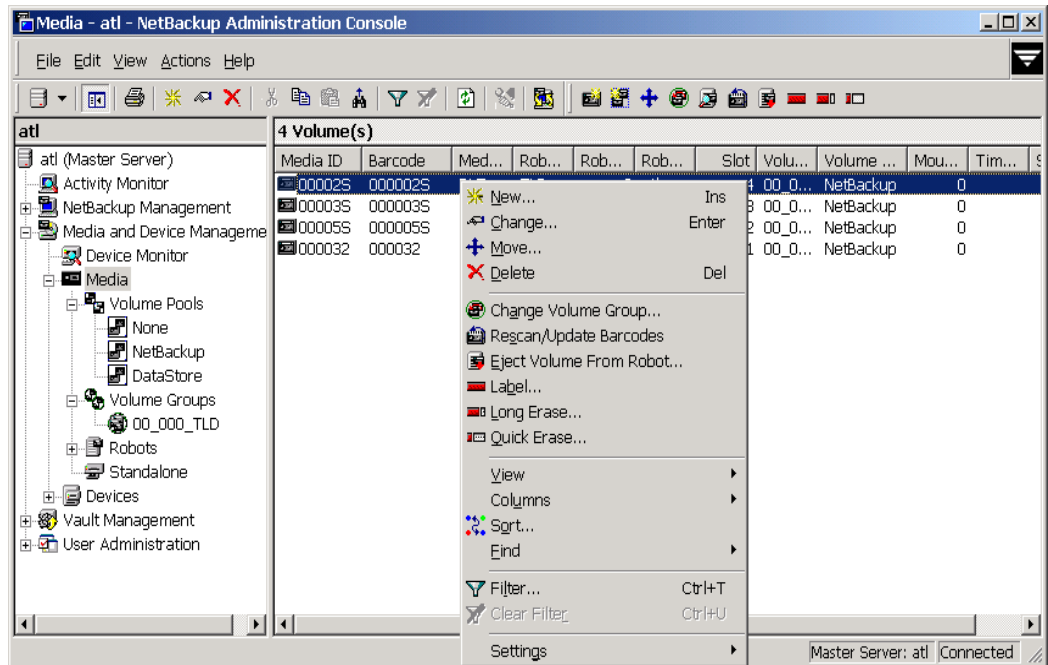
Shortcut Menus and Commands

Shortcut menus work in the context of what object is currently selected in a pane. Shortcut commands are also available on the menus or toolbars.

▼ To display a shortcut menu

- ❖ Click the right mouse button while the pointer is over a pane or a selection of a pane.

Short Cut Menu



Customizing the Window

The **View** menu has options for sorting, filtering, and changing the layout and appearance of the panes.

See the NetBackup administrator's guide for UNIX or the NetBackup administrator's guide for Windows for more details.

▼ To show or hide columns, or rearrange the order of columns

Click **View > Columns > Layout**.

Allowable Media Manager Characters

The following set of characters can be used in user-defined names, such as volume groups, volume pool names (volume pool names are case sensitive), and media IDs that you enter when creating these entities. These characters must be used even when specifying these items in foreign languages.



Do not use a minus as the first character. Spaces are only allowed in a comment for a drive.

- ◆ Alphabetic (A-Z a-z)
- ◆ Numeric (0-9)
- ◆ Period (.)
- ◆ Plus (+)
- ◆ Minus (-)
- ◆ Underscore (_)

Administering Media on Other Servers

This is a NetBackup Enterprise Server topic.

The following topics explain media administration on other servers:

- ◆ “Volume Database Best Practices” on page 106.
- ◆ “Determining the Volume Database Host for a Device” on page 106.
- ◆ “Managing Media on Other Servers” on page 107.

Volume Database Best Practices

This is a NetBackup Enterprise Server topic.

Each host that has Media Manager installed can have a volume database. However to simplify administration, VERITAS recommends that you centralize the volume database on one host and keep the volume databases on other hosts empty. Adding volumes to multiple hosts makes administration more complicated.

You can enforce this practice by adding a `NOT_DATABASE_HOST` entry in the Media Manager configuration file (`vm.conf`). The `vmdb_merge` command can be used to merge volume, pool, and media databases. See the NetBackup commands guide for details.

For recommended practices, see “Media and Device Management Domain Management” on page 271.

Determining the Volume Database Host for a Device

This is a NetBackup Enterprise Server topic.

The configuration for each robotic library or set of standalone drives designates the volume database host that contains the volume information for those devices. Before adding a volume to the volume configuration, you *must* be managing the correct host or the volume will not be found when it is required.

▼ **To determine the volume database host for a drive in a robotic library**

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click the **Robots** tab in the Devices pane.

The Volume Database Host column shows the name of the host for the volumes in this robotic library.

▼ **To determine the volume database host for a standalone drive**

1. In the NetBackup Administration Console, click **Media and Device Management > Devices**.
2. Click the **Hosts** tab in the Devices pane.

The Standalone Volume Database Host column shows the name of the host for all of the standalone drives controlled by this host.

Managing Media on Other Servers

This is a NetBackup Enterprise Server topic.

Initially, you can manage media on the server where you are running NetBackup. The name of this server and its connection status is shown in the status bar (on the lower right side) of the window, for example Master Server: spain Connected

You also can change from the current server to a different master or media server. If you change from a NetBackup Enterprise Server to a NetBackup Server, the functionality available on the new server is limited to the functionality supported by NetBackup Server.

If you change from a NetBackup Server to a NetBackup Enterprise server, complete functionality is available on the new server.

▼ **To change to a different master or media server**

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. Click **File > Change Server**.



(You can also click the **arrow** to the right of the **Change Server** icon on the toolbar and select one of the servers shown in the list.)

3. In the dialog that appears, do *one* of the following to specify the server.

- ◆ Enter the name of the server.
- ◆ Select a server from the servers shown in the list.
- ◆ Click **Browse** and select a server.
- ◆ Login to the current server using a different user name.
- ◆ Login to a different server using a different user name.

You can also click **Remove** to delete a server from the list of available hosts.

4. Click **OK**.

The name of the new server appears and the volumes pane shows the volume information for the new server. This information is obtained from the volume database for the new server.

In addition to using **File > Change Server** to manage media on other servers, you can use **File > Login as New User**. See “Menus and Commands” on page 93.

Configuring Volume Pools

A volume pool identifies a logical set of volumes by type of usage. Associating volumes with a volume pool protects them from access by unauthorized users, groups, or applications.

With the exception of the volume pools that are automatically created by NetBackup, you must create a volume pool before you can add volumes to a volume pool. The following volume pools are automatically created (see “Volume Pools List” on page 97):

- ◆ Media Manager creates a pool, named NetBackup, for NetBackup use.
- ◆ NetBackup creates a pool, named DataStore, for DataStore use.

During initial configuration, it is easiest to create all of your volume pools first. Then as you add volumes, you can assign them to volume pools.

It is also possible to configure a scratch pool from which Media Manager can transfer volumes, when a volume pool has no volumes available.

For background information, see “Volume Pools” on page 315 and “Scratch Volume Pools” on page 318.

The following topics explain volume pool configuration:

- ◆ “Adding a New Volume Pool or Scratch Volume Pool” on page 109
- ◆ “Changing the Attributes of a Volume Pool” on page 111
- ◆ “Changing the Volume Pool Assignment for a Volume” on page 112
- ◆ “Deleting a Volume Pool” on page 113

Adding a New Volume Pool or Scratch Volume Pool

▼ To add a volume pool

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. Click **Actions > New > New Volume Pool**.

To add a scratch volume pool, see “Adding a Scratch Volume Pool” on page 110.

3. In the **Pool name** text box, enter a name for the new volume pool.
The name must be 20 characters or less, and cannot contain any spaces or special characters. See “Allowable Media Manager Characters” on page 105.
4. In the **Description** text box, enter a brief description for the pool.
5. *This step applies only to NetBackup Enterprise Server.*
To allow only a specified host to use the volumes in this pool, do the following:
 - a. Select **Permit only the specified host to access volumes in the pool**.
 - b. In the **Host name** text box, enter the name of the host that is allowed to request and use the volumes in this volume pool.



Caution VERITAS recommends that you *do not* specify a specific host. Allowing any host (the default) is recommended, and is required if you have NetBackup media servers (or SAN media servers) controlled by a master server. Never specify the name of a client.

Adding a Scratch Volume Pool

A scratch pool is a special volume pool that you can optionally configure. There can be only one scratch pool configured. You can not add a scratch pool if one exists.

If a scratch pool is configured, Media Manager moves volumes from the scratch pool to any other pools that do not have volumes available. Media Manager also returns any expired media back to the scratch volume pool automatically.

▼ **To add a scratch volume pool**

1. Specify attributes for the scratch pool as shown in the following table:

For this Attribute	Your Action	Note
Pool Name	Enter any name, except the following pool names: NetBackup, DataStore, or None. It is recommended to use a descriptive name, like scratchpool, as the pool name.	
Description	It is recommended to include “scratch pool” in the description.	
Permit only the specified host to access volumes in the pool	Do not select this check box to specify a specific host. ANYHOST is the default host name.	Applies only to NetBackup Enterprise Server.
Scratch Pool	Select this check box.	

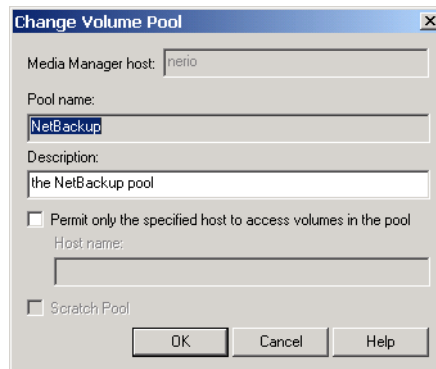
2. Add volumes to the scratch volume pool for each robotic or standalone device that may require them.
- Follow the steps for adding other volumes to pools (see “Adding New Volumes” on page 119). In this case, select the pool name of the scratch pool you created as the volume pool.



Changing the Attributes of a Volume Pool

▼ To change a volume pool

1. In the NetBackup Administration Console, click **Media and Device Management > Media > Volume Pools**.
2. Select a pool from the pools shown under **Volume Pools** in the tree pane.
3. Click **Edit > Change**.



4. In the **Description** text box, enter a new description for the pool.
To change this pool to a scratch volume pool, see “Changing a Volume Pool To be a Scratch Volume Pool” on page 112.
5. *This step applies only to NetBackup Enterprise Server.*
To allow only a specified host to use the volumes in this pool:
 - a. Select **Permit only the specified host to access volumes in the pool**.
 - b. In the **Host name** text box, enter the name of the host that is allowed to request and use the volumes in this volume pool.

Caution VERITAS recommends that you *do not* specify a specific host. Allowing any host (the default) is recommended, and is required if you have NetBackup media servers (or SAN media servers) controlled by a master server. Never specify the name of a client.



Changing a Volume Pool To be a Scratch Volume Pool

A scratch pool is a special volume pool that you can optionally configure. There can be only one scratch pool configured. You can not add a scratch pool if one exists.

If a scratch pool is configured, Media Manager moves volumes from the scratch pool to any other pools that do not have volumes available. Media Manager also returns any expired media back to the scratch volume pool automatically.

▼ To change a pool to be a scratch volume pool

1. Specify attributes for the scratch pool as follows.

For this Attribute	Your Action	Note
Description	It is recommended to include “scratch pool” in the description.	
Permit only the specified host to access volumes in the pool	Do not select this check box to specify a specific host. ANYHOST is the default host name.	Applies only to NetBackup Enterprise Server.
Scratch Pool	Select this check box.	

2. Add volumes to the scratch volume pool for each robotic or standalone device that may require them.

Follow the steps for adding other volumes to pools (see “Adding New Volumes” on page 119). In this case, select the name of the scratch pool as the volume pool.

Changing the Volume Pool Assignment for a Volume

Volumes are grouped in a specific volume pool. The Volume Pool column in the Volumes list shows the name of the volume pool to which the volumes belong. Volume Pool does not apply to cleaning tapes.

▼ To change the volume pool assignment

1. In the NetBackup Administration Console, click **Media and Device Management** > **Media**.
2. Select a volume or volumes from the volumes pane.

Note You are unable to change the volume pool for any assigned volumes until the application deassigns them (see “Deassigning Volumes” on page 142).

3. Click **Edit > Change.**

In the dialog that appears, the volumes you selected in the previous step are listed in the top section of the dialog.

See “Changing the Attributes for a Volume” on page 144 for more information.

4. In the Volume Pool section, click **New Pool and click the **arrow** to view a list of the available volume pools.**

Select a volume pool from the list.

5. Click **OK.**

Deleting a Volume Pool

Note that you *cannot* delete any of the following pools:

- ◆ A volume pool that contains volumes
- ◆ Scratch pools
- ◆ The NetBackup volume pool
- ◆ The None volume pool
- ◆ The HSM volume pool (for VERITAS Storage Migrator)
- ◆ The DataStore volume pool

▼ **To delete a volume pool**

1. In the NetBackup Administration Console, click **Media and Device Management > Media > Volume Pools.**

2. Select a volume pool from the pools shown under **Volume Pools in the tree pane.**

Ensure that the volume pool is empty. If the pool is not empty, change the pool name for any volumes in the pool. If the volumes are not needed, delete them.

3. Click **Edit > Delete.**

Answer the confirmation dialog.



Methods Available for Injecting and Ejecting Volumes

Some robotic libraries implement different functionality for their media access ports. For example, some libraries have front-panel inject and eject features that conflict with the use of the media access port in NetBackup. Other robotic libraries require front-panel interaction when using the media access port.

Read the operator manual for your robotic library to understand the media access port functionality. Libraries such as the ones noted may not be fully compatible with the inject and eject features of NetBackup if not properly handled. Other libraries may not be compatible at all.

See the following topics for more information:

- ◆ “Methods for Injecting Volumes into a Robot” on page 114
- ◆ “Methods for Ejecting Volumes From a Robot” on page 115
- ◆ “Inject and Eject Functions Available by Robot Type” on page 117
- ◆ “Media Ejection Timeout Periods” on page 118

Methods for Injecting Volumes into a Robot

The following methods are available to inject a single volume into a robotic library.

When Adding New Volumes

When specifying dialog entries for adding new volumes, select **Inject volume into robot via the media access port** to inject a volume into a robotic library.

Inject volume into robot via the media access port is available only for the robot types listed in the matrix shown in “Inject and Eject Functions Available by Robot Type” on page 117.

Inject volume into robot via the media access port *may* be enabled for some robots that do not have media access ports, since the robot type for the robotic library only indicates that media access ports are possible.

See “Adding Volumes Using the Actions Menu” on page 122 for complete instructions.

When Moving Volumes

When specifying dialog entries for moving volumes, select **Inject volume into robot via the media access port** to inject this volume into a robotic library.

Inject volume into robot via the media access port is available only if the following are true:

- ◆ You are moving a single volume from standalone to a robotic library.
- ◆ Media Manager supports inject for the robot type involved (see “Inject and Eject Functions Available by Robot Type” on page 117).

Inject volume into robot via the media access port *may* be enabled for some robots that do not have media access ports, since the robot type for the robot only indicates that media access ports are possible.

See “Moving Volumes” on page 130 for complete instructions.

When Performing a Volume Configuration Update Using Robot Inventory

When performing a volume configuration update for a robot, select **Empty media access port prior to update** to inject a volume into a robot.

Any volumes to be injected must be in the media access port before the operation begins. If **Empty media access port prior to update** is selected and there are no volumes in the port, you are *not* prompted to place volumes in the media access port and the update operation continues.

Each volume located in the media access port is moved into the robotic library. If the robotic library has a port that can hold multiple volumes, volumes are moved to empty slots in the robotic library until the media access port is empty or all the slots are full.

After the volume or volumes have been moved, the configuration update proceeds as usual.

Empty media access port prior to update is available only for the robot types listed in the matrix shown in “Inject and Eject Functions Available by Robot Type” on page 117.

Empty media access port prior to update *may* be available for some robots that do not have media access ports, since these robot types only indicate that media access ports are possible.

See “Updating the Volume Configuration for a Robot” on page 162 for complete instructions.

Methods for Ejecting Volumes From a Robot

The following methods are available to eject single or multiple volumes.



When Moving Volumes

When specifying dialog entries for moving volumes, select **Eject volume from robot via the media access port** to eject one or more selected volumes using the robot's media access port.

You can eject volumes that reside in multiple robots. In this case, multiple eject dialogs will appear for each robot type.

Eject volume from robot via the media access port is available only if the following are true:

- ◆ You are moving a volume from a robotic library to standalone.
- ◆ Media Manager supports eject for the robot type involved (see “Inject and Eject Functions Available by Robot Type” on page 117).

Eject volume from robot via the media access port *may* be enabled for some robots that do not have media access ports, since the robot type for the robotic library only indicates that media access ports are possible.

For the robot types shown in the 4th column of the matrix, selecting multiple volumes to eject requires operator intervention. The selected volumes will be ejected one volume at a time. Operator intervention is required to remove the ejected volume and answer the prompts.

For the robot types shown in the 3rd column of the matrix, operator intervention is only required if the robotic library does not have a media access port large enough to eject all of the selected volumes. For these robot types, the operator is prompted to remove the media from the media access port so the eject can continue with the remaining volumes. See “Media Ejection Timeout Periods” on page 118.

See “Moving Volumes” on page 130 for complete instructions.

Using the Eject Volumes From Robot Command

Select **Actions > Eject Volume(s) From Robot** to eject one or more selected volumes from a robotic library.

Eject Volume(s) From Robot is only available for the robot types shown in the matrix in “Inject and Eject Functions Available by Robot Type” on page 117.

You can eject volumes that reside in multiple robots. In this case, multiple eject dialogs will appear for each robot type.

For the robot types shown in the 4th column of the matrix, selecting multiple volumes to eject requires operator action. The selected volumes will be ejected one volume at a time. Operator intervention is required to remove the ejected volume and answer the prompts.

For the robot types shown in the 3rd column of the matrix, operator intervention is only required if the robotic library does not have a media access port large enough to eject all of the selected volumes. For these robot types, you are prompted to remove the media from the media access port so the eject can continue with the remaining volumes. See “Media Ejection Timeout Periods” on page 118.

See “Ejecting Volumes From Robots (Actions Menu Command)” on page 137 for complete instructions.

Inject and Eject Functions Available by Robot Type

The following matrixes show the availability of inject and eject functions provided with the Media Manager functions listed in the 1st column. The availability of the inject and eject functions listed in the column headings depends on the robot type being used. NA in a cell of a matrix means *Not Applicable*.

The following matrix applies to NetBackup Server. For ODL and TSH robot types the robot must be attached to a UNIX server running NetBackup.

Inject / Eject Functions Available for NetBackup Server Robot Types

Media Manager Function	Inject Single Volume	Eject Single or Multiple Volumes (Dialog Type 1)	Eject Single or Multiple Volumes (Dialog Type 2)
New Volumes	ODL, TL8, TLD, TSH	NA	NA
Move Volumes	ODL, TL8, TLD, TSH	TL8, TLD	ODL, RSM, TSH
Robot Inventory	TL8, TLD	NA	NA
Eject Volumes	NA	TL8, TLD	ODL, RSM, TSH

The following matrix applies to NetBackup Enterprise Server. For LMF, ODL, and TSH robot types, the robot must be attached to a UNIX server running NetBackup.

Inject / Eject Functions Available for NetBackup Enterprise Server Robot Types

Media Manager Function	Inject Single Volume	Eject Single or Multiple Volumes (Dialog Type 1)	Eject Single or Multiple Volumes (Dialog Type 2)
New Volumes	LMF, ODL, TL8, TLD, TSH	NA	NA



Inject / Eject Functions Available for NetBackup Enterprise Server Robot Types

Media Manager Function	Inject Single Volume	Eject Single or Multiple Volumes (Dialog Type 1)	Eject Single or Multiple Volumes (Dialog Type 2)
Move Volumes	LMF, ODL, TL8, TLD, TSH	ACS, TL8, TLD, TLH, TLM	LMF, ODL, RSM, TSH
Robot Inventory	TL8, TLD, TLM	NA	NA
Eject Volumes	NA	ACS, TL8, TLD, TLH, TLM	LMF, ODL, RSM, TSH

Media Ejection Timeout Periods

The media ejection period (the amount of time before an error condition occurs) varies depending on the capability of each robot. The following table shows the ejection timeout periods for robots.

Robot Types	Timeout Period	Note
Automated Cartridge System (ACS) Tape Library Multimedia (TLM)	One week	Applies only to NetBackup Enterprise Server.
Tape Library 8MM (TL8) Tape Library DLT (TLD)	30 minutes.	
Tape Library Half-inch (TLH)	None. The robot allows an unlimited period to remove media.	Applies only to NetBackup Enterprise Server.

Caution If media is not removed and a timeout condition occurs, the media is returned to (injected into) the robot. If this occurs, you should inventory the robot and then eject the media that was returned to the robot.

Some robots do not have media access ports. For these robots, the operator must remove the volumes from the robot manually.

Note After manually adding or removing volumes, it is recommended to run an inventory on the robot.

Adding New Volumes

Media Manager volumes are logical units of data storage or cleaning capability on media that have been assigned media IDs and other attributes, which are recorded in the Media Manager volume database. The attributes in the volume database include information to show the robotic location. This residence information for a volume includes the robot host, robot type, robot number, and slot location.

When you add a new volume, there is no default expiration date. See the following topics:

- ◆ “Methods Available for Adding Volumes” on page 119
- ◆ “Adding Volumes Using a Robot Inventory Update” on page 121
- ◆ “Adding Volumes Using the Actions Menu” on page 122
- ◆ “Dialog Entries for New Volumes” on page 123

Methods Available for Adding Volumes

The methods available to add volumes depend on how the volume will be used.

If your storage devices are supported by the Volume Configuration wizard, using this wizard is an easy method for adding volumes. See “Using the Volume Configuration Wizard” on page 129 for more details.

See the following topics:

- ◆ “Robotic Volumes (Volumes Located in a Robot)” on page 119
- ◆ “Standalone Volumes (Volumes To Be Used in Standalone Drives)” on page 120
- ◆ “NetBackup Catalog Backup Volumes” on page 120
- ◆ “Notes on Labeling NetBackup Volumes” on page 120

Robotic Volumes (Volumes Located in a Robot)

- ◆ The easiest way to add robotic volumes is to use the Volume Configuration wizard. See “Using the Volume Configuration Wizard” on page 129 for more details.
- ◆ To use robot inventory to add robotic volumes, perform the Update Volume Configuration procedure. During the update, Media Manager assigns the media IDs and other attributes.

See “Adding Volumes Using a Robot Inventory Update” on page 121.
- ◆ To add volumes using the menu, see “Adding Volumes Using the Actions Menu” on page 122.



Standalone Volumes (Volumes To Be Used in Standalone Drives)

- ◆ The easiest way to add standalone volumes is to use the Volume Configuration wizard. See “Using the Volume Configuration Wizard” on page 129 for more details.
- ◆ You can also configure volumes automatically by inserting the media into a standalone drive. For an unused volume, NetBackup assigns a media ID, labels the volume, and uses it (if it needs a volume of that type for a backup). Media Manager adds the media ID (designated by NetBackup) and other attributes for the volume.

The `DISABLE_STANDALONE_DRIVE_EXTENSIONS` configuration option turns off NetBackup’s automatic use of standalone volumes. See the NetBackup system administrator’s guide for more information.

- ◆ To manually choose the media IDs, label the volume with the NetBackup `bplabel` command and then follow the instructions in “Adding Volumes Using the Actions Menu” on page 122. See the NetBackup commands guide for more information on this command.

Even if you normally use NetBackup’s assignment capabilities for standalone volumes, manually adding extra standalone volumes prevents "out of media" errors in some situations.

For example, if a volume in a standalone drive is full or unusable because of errors, NetBackup requests that Media Manager eject the volume. NetBackup then searches for another unused volume. If another appropriate volume is not defined, NetBackup exits with an error.

Labeling a volume and adding it prevents this problem, because Media Manager displays a mount request for that volume rather than returning an error to NetBackup.

NetBackup Catalog Backup Volumes

- ◆ Prior to using volumes for NetBackup catalog backups, you must add them. You can also use the NetBackup `bplabel` command to label the volume.

See “Adding Volumes Using the Actions Menu” on page 122.

Notes on Labeling NetBackup Volumes

Labeling volumes is controlled by the application. Refer to the NetBackup system administrator’s guide for Windows servers, the NetBackup system administrator’s guide for UNIX, or the Storage Migrator system administrator’s guide for more information.

NetBackup controls the labeling of its volumes and in most cases performs this operation automatically.

- ◆ If a volume in a robotic library has not been labeled, NetBackup labels it with the media ID assigned by Media Manager the first time that it uses the volumes for a backup.

This action is done unless those volumes were last used for NetBackup catalog backups (you do not want to label these volumes unless they are no longer being used for catalog backups), or the volumes contain data from a recognized non-NetBackup application (the NetBackup configuration option, `ALLOW_MEDIA_OVERWRITE` can be set to allow the volume to be overwritten).

- ◆ If you prefer to assign specific media IDs to NetBackup volumes, label them using the NetBackup `bplabel` command and add them using the manual update procedure.
- ◆ Media Manager uses a default prefix of the letter A, when assigning media IDs to volumes without barcodes (for example, A00001). To change this default, use the `MEDIA_ID_PREFIX` configuration option.
- ◆ If the robotic library supports barcodes, by default NetBackup generates media IDs for new volumes based on the last six characters of the barcode obtained from the robot. To change this default action, you can specify and select specific characters using Media ID generation rules (see “Media ID Generation Tab (Advanced Options)” on page 184).

Adding Volumes Using a Robot Inventory Update

The update includes the generation of media IDs for new volumes as follows.

If the robot

- ◆ Supports barcodes and the volumes have readable barcode labels, the update part of the operation generates Media Manager media IDs for new volumes based on the last six characters of the barcodes (as the default method) or the specific characters that you specify if you are using Media ID generation rules.
- ◆ Does not support barcodes or the volumes do not have readable barcodes, the new media IDs are based on a media ID prefix that you specify.

See “Updating the Volume Configuration for a Robot” on page 162 for more information on robot inventory and media ID generation rules.

When you use barcode rules, new volumes that are added through a barcode rule are assigned a media type, volume pool, maximum number of mounts (or maximum cleanings), and description.



▼ **To add volumes using a robot inventory update**

1. Insert the volume into the robotic library.
2. In the NetBackup Administration Console, click **Media and Device Management > Media > Robots**.
3. Select the robotic library where you inserted the volume.
4. Click **Actions > Inventory Robot**.
5. In the Inventory operation section, select **Update volume configuration**.
6. For more options, click **Advanced Options**
7. To clear any previous display in the Results section, click **Clear Results**.
8. Click **Start** to start the update.

Adding Volumes Using the Actions Menu

This is not the recommended method to add volumes. See “Adding Volumes Using a Robot Inventory Update” on page 121.

▼ **To add volumes using the Actions menu**

1. If you are adding new volumes to a robotic library, insert them into the proper slots.
2. In the NetBackup Administration Console, click **Media and Device Management > Media**.
3. *This step applies only to NetBackup Enterprise Server.*
Verify that you are adding volumes on the volume database host for the robotic library or a standalone device that will be using the new volumes.
See “Determining the Volume Database Host for a Device” on page 106.

4. Click **Actions > New > New Volumes**.

The 'New Volumes' dialog box is shown with the following settings:

- Media type: 1/2" cartridge tape 3
- Robot: TLD[0] - nerio
- Number of volumes: 4
- First Media ID: ZZ1234
- First slot number: 3
- Volume group: test77
- Media ID naming style: 2 character and 4 digits
- Media Description: test
- Maximum mounts/maximum cleanings: 3
- Volume pool: NetBackup
- ☐ Inject volume into robot library via the media access port

5. Specify the properties for the volumes as explained in “Dialog Entries for New Volumes” on page 123.

Note Be careful when specifying properties, since you cannot change properties (such as the media ID or media type) later. To change these properties, you need to delete the volumes and add them again.

6. Click **OK** to execute the add. If you selected **Inject volume into robot library via the media access port**, an inject prompt appears.

The volumes pane now shows the new volume information. If the robot has a barcode reader, Media Manager does the following actions:

- Adds an entry in the volume database, using the specified media ID.
- Reads the barcode of each new volume.
- Adds the barcodes as attributes in the volume database.

Note If you are making multiple additions, clicking **Apply** updates the configuration without closing the dialog or refreshing the display. This allows you to add another volume by modifying the dialog contents and then clicking **Apply** or **OK**.

Dialog Entries for New Volumes

- ◆ “Media Type” on page 124
- ◆ “Robot” on page 124



- ◆ “Find Robots” on page 125
- ◆ “Number of Volumes” on page 125
- ◆ “Media ID Naming Style” on page 125
- ◆ “Media ID or First Media ID” on page 126
- ◆ “Media Description” on page 126
- ◆ “First Slot Number” on page 126
- ◆ “Maximum Mounts or Maximum Cleanings” on page 127
- ◆ “Volume Group” on page 127
- ◆ “Volume Pool” on page 128
- ◆ “Inject Volume Into Robot via the Media Access Port” on page 129

Media Type

Media Manager running on a Windows host does not support optical disk volumes.

Media Type specifies the media type for the volume that you are going to add.

▼ To specify a media type

- ❖ Click the **arrow** and select from the list.

If you are adding a cleaning tape, choose one of the cleaning tape media types.

Robot

Robot specifies the robotic library to which you are adding the volumes. You can specify a different robot.

▼ To add volumes to a different robot

- ❖ Click the **arrow** and select one of the robots in the list.

The list shows the robot type, number, and control host for any robot, that already has at least one volume in the volume database.

▼ To add volumes to a standalone drive

- ❖ Click the **arrow** and select **Standalone**.

Find Robots

Use **Find Robots** to add volumes to a robot that does not appear in the **Robot** box (for example, a new robot).

▼ **To specify a robot that does not appear in the box**

1. Select **Find Robots**.
2. Select a robot in the dialog that appears.
3. Click **OK**.

The name of the robot that you select appears in the **Robot** box, and is also the robot name that will be in the volume database, for the volumes you are adding.

Number of Volumes

Specifies the number of volumes you are adding. For a robotic library, this refers to the number of slots that must be reserved for the new volumes. Depending on the number of volumes you are adding, you must also specify additional information as shown in the following table:

If You are Adding	You Must Also Specify	See
One volume	Media ID	“Media ID or First Media ID” on page 126
More than one volume	First Media ID	“Media ID or First Media ID” on page 126
	Media ID naming style	“Media ID Naming Style” on page 125

▼ **To specify the number of volumes**

- ❖ Click an **arrow** and select a number for the volumes.

Media ID Naming Style

Media IDs can be from 1 to 6 characters in length.

Media Manager media IDs for an API robot must match the barcode on the media (for API robots, Media Manager supports barcodes from 1 to 6 characters). This means that you must get a list of the barcodes prior to adding the volumes. You can obtain this information through a robotic inventory or from the robot vendor’s software.



▼ **To specify a naming style**

1. Click the **arrow** to open a list of possible combinations of alphanumeric characters.
2. Select a style to use in creating the media IDs for this range of new volumes.

Media ID or First Media ID

Media IDs can be from 1 to 6 characters in length.

Media Manager media IDs for an API robot must always match the barcode on the media (for API robots, Media Manager supports barcodes from 1 to 6 characters). This means that you must get a list of the barcodes prior to adding the volumes. You can obtain this information through a robotic inventory or from the robot vendor's software.

To specify a media ID for one volume

- ❖ Enter an ID for the new volume in the **Media ID** text box.

To specify media IDs for more than one volume

- ❖ Enter an ID for the new volumes in the **First Media ID** text box.

Use the same pattern that you chose in the **Media ID naming style** box. This is the ID for the first volume in the range of volumes that you are adding. Media Manager names the remaining volumes by incrementing the digits.

Media Description

Enter a 1 to 25 ASCII character description of the media that you are adding.

First Slot Number

For new volumes in a robot, you must specify the first slot number to be used by the range of volumes that you are adding. Media Manager assigns the remainder of the slot numbers sequentially.

Note You cannot enter slot information for volumes in an API robot. The robot vendor or the operating system software (in the case of RSM robots) tracks the slot locations for these robot types.

▼ **To specify the first slot number**

- ❖ Click an **arrow** and specify the first slot number.

Maximum Mounts or Maximum Cleanings

For volumes intended for backups, you specify the maximum number of times that Media Manager should mount the volumes. When a volume reaches this mount limit, the volume can be read, but not written.

For a cleaning tape, you specify the number of cleanings that can be performed. The number must be greater than zero.

See “Drive Cleaning” on page 309 for background information on manual cleaning and cleaning tapes.

▼ **To specify maximum mounts**

1. To help determine the maximum mount limit to use, consult your vendor documentation for information on the expected life of the volume.
2. Click an **arrow** and specify the maximum mounts.

Note Specify zero to permit an unlimited number of mounts.

▼ **To specify maximum cleanings**

- ❖ Click an **arrow** and specify the number of cleanings

Note The number that you specify must be greater than zero.

Volume Group

Volume groups are not the same as volume pools. Refer to “Volume Pools and Volume Groups” on page 314 for an explanation of the differences.

The following table shows the results if you do not specify a volume group (you leave the volume group blank):

If You Leave the Volume Group Blank for	Media Manager
Standalone volumes	Does not assign a volume group.
Robotic volumes	Generates a name using the robot number and type. For example, if the robot is a TS8 and has a robot number of 50, the group name will be 00_050_TS8.



Rules for Assigning Volume Groups

- ◆ All volumes in a group must be the same media type. However, a media type and its corresponding cleaning media type are allowed in the same volume group (for example, DLT and DLT_CLN).
- ◆ All volumes in a robotic library *must* belong to a volume group. You cannot add volumes to a robotic library without specifying a group or having Media Manager generate a name.
- ◆ The only way to clear a volume group name is to move the volume to standalone and not specify a volume group.
- ◆ More than one volume group can share the same location. For example, a robotic library can contain volumes from more than one volume group and you can have more than one standalone volume group.
- ◆ All members of a group must be in the same robotic library or be standalone. That is, Media Manager will not let you add a group (or part of a group) to a robotic library, if it already exists in another robotic library.

▼ To enter a volume group

- ❖ Enter a name for the volume group in the box.

▼ To select a volume group

- ❖ Click the **arrow** and select from the list of previously configured volume groups.

Volume Pool

▼ To select a volume pool

- ❖ Click the **arrow** and select from the list of volume pools as follows.

Select	To Make the Volume Available
None	To any user or application (Note: cleaning tapes must be in the None pool).
NetBackup	Only to NetBackup.
DataStore	Only to DataStore.

Select	To Make the Volume Available
One of the other volume pools in the list	For a specific volume pool. (Other volume pools appear only if you created them earlier as explained in “Configuring Volume Pools” on page 108.)

Inject Volume Into Robot via the Media Access Port

See “Methods for Injecting Volumes into a Robot” on page 114 for a list of the robot types that determine when **Inject volume into robot library via the media access port** is available, and for more information on using this function.

- ▼ **To insert a single volume into the media access port**
 1. Select **Inject volume into robot library via the media access port**.
 2. Insert the volume in the robotic library so it can be injected into the correct slot in the robot. Media Manager will add it to its volume configuration.

Using the Volume Configuration Wizard

You can use this wizard to accomplish the following tasks:

- ◆ Inventory your robots.
- ◆ Identify cleaning media in your robots.
- ◆ Add volumes for standalone drives.
- ◆ Update the Media Manager volume database.

After running this wizard to configure media, each media will have a unique media ID in the volume database that is used in Media Manager and NetBackup to track the media. The wizard will create media that has a media type determined by type of drive. The default media type for the drive will be used.

Learning More About the Volume Configuration Wizard

You can obtain detailed information about this wizard before you start, including what to expect in the wizard, a wizard overview, and limitations of the wizard.



▼ **To learn about this wizard**

1. Start the wizard (see “Starting the Volume Configuration Wizard” on page 130).
2. From the welcome screen of the wizard, click **Help**.
3. When finished reviewing the help information in the wizard, exit the help and then click **Cancel** to exit the wizard.

Starting the Volume Configuration Wizard

This wizard is available from the list of wizards displayed in the right pane of the **Media and Device Management** window of the NetBackup Administration Console or from the Getting Started wizard.

Be sure to review the limitations of this wizard before starting.

▼ **To start the volume configuration wizard**

- ❖ In the NetBackup Administration Console, click **Media and Device Management > Configure Volumes**.

Moving Volumes

When you move volumes in or out of a robotic library, you must physically *and* logically move the volume.

When moving volumes from one robotic library to another robotic library, you must move the volumes to standalone as an intermediate step, and then to the new robotic library.

For background information, see “Moving Volumes” on page 320.

You can move volumes using one of the following methods:

- ◆ “Moving Volumes Using the Robot Inventory Update Option” on page 130
- ◆ “Moving Volumes Using the Actions Menu” on page 131

Moving Volumes Using the Robot Inventory Update Option

The robot must have a barcode reader and the volumes must have readable barcodes to use the following procedure. But you can also use this procedure to move volumes *out* of a robot, even if the volumes do not have barcodes or if the robot does not have a reader.

▼ To move volumes using a robot inventory update

1. Physically move the volumes to their new location.
2. Click **Actions > Inventory Robot** to update the volume database to agree with the contents of the robot.

See “Updating the Volume Configuration for a Robot” on page 162 for more information.

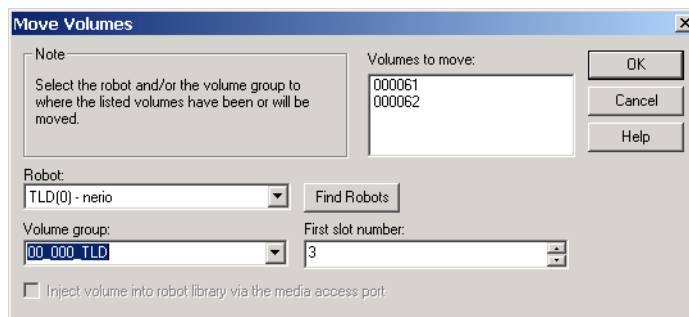
Moving Volumes Using the Actions Menu

If you move a volume to a robotic library that has a barcode reader, Media Manager updates the media database to show the correct barcode for the volume.

When moving volumes from one robotic library to another, you must move the volumes to standalone as an intermediate step and then to the new robotic library.

▼ To move volumes using the Actions menu

1. Physically move the volumes to their new location.
You can also use the inject and eject options when moving volumes to or from a robotic library that has a media access port. Inject can be used for single volumes and eject can be used for multiple volumes.
2. In the NetBackup Administration Console, click **Media and Device Management > Media**.
3. In the volumes pane, select the volumes you want to move.
4. Click **Actions > Move**.



If you selected volumes of different media types or volume residences, a Move Volumes dialog appears for each residence and media type.



For example, if you selected two full volumes to move out of a robotic library and two standalone volumes to move in as replacements for these volumes, a dialog appears for the two full volumes and another dialog for the two replacement volumes. In this example, you must complete both move dialogs to execute the move (complete the move for the volumes that are full first).

Note These multiple Move Volumes dialogs may appear on top of each other and need to be repositioned.

The following is an example of a move involving multiple types or residences:

Step 1. Move volumes to Standalone

The 'Move Volumes' dialog box has a title bar with a close button. It contains a 'Note' section with the text: 'Select the robot and/or the volume group to where the listed volumes have been or will be moved.' To the right of the note is a list box titled 'Volumes to move:' containing two entries: 'A00001' and 'A00002'. Below the note is a 'Robot:' dropdown menu set to 'Standalone' and a 'Find Robots' button. Below that is a 'Volume group:' dropdown menu set to an empty field. To the right of the volume group dropdown is a 'First slot number:' dropdown menu set to '2'. At the bottom left is a checkbox labeled 'Inject volume into robot library via the media access port' which is unchecked. On the right side are three buttons: 'OK', 'Cancel', and 'Help'.

Step 2. Move volumes to the robot

The 'Move Volumes' dialog box is similar to the one in Step 1. The 'Note' section is the same. The 'Volumes to move:' list box contains two entries: 'A00004' and 'A00005'. The 'Robot:' dropdown menu is now set to 'TL4(0) - maygrass' and the 'Find Robots' button is disabled. The 'Volume group:' dropdown menu is set to '00_000_TL4'. The 'First slot number:' dropdown menu is set to '5'. The 'Inject volume into robot library via the media access port' checkbox remains unchecked. The 'OK', 'Cancel', and 'Help' buttons are on the right.

5. Specify the properties for the move as explained in “Dialog Entries for Move Volumes” on page 133.
6. Click **OK** to execute the move.

If you selected **Eject volume from robot via the media access port**, an eject dialog appears. See “Ejecting Volumes From Robots (Actions Menu Command)” on page 137 for more information on the eject dialogs.

Dialog Entries for Move Volumes

- ◆ “Volumes to Move” on page 133
- ◆ “Robot” on page 133
- ◆ “Find Robots” on page 133
- ◆ “Volume Group” on page 134
- ◆ “First Slot Number” on page 135
- ◆ “Eject Volume From Robot via the Media Access Port” on page 135
- ◆ “Inject Volume Into Robot via the Media Access Port” on page 135

Volumes to Move

The **Volumes to Move** section of the dialog shows the Media IDs of the volumes that you selected to move.

If you selected only one side of an optical disk platter that side is shown, but both sides will be moved.

Robot

Robot specifies the robotic library to which you are moving the volumes. You can specify a different robot.

▼ To move volumes to a different robot

- ❖ Click the **arrow** and select one of the robots in the list.

The list shows the robot type, number, and control host for any robot that already has at least one volume in the volume database.

▼ To move volumes to a standalone robot

- ❖ Select **Standalone**.

Find Robots

Use **Find Robots** to move volumes to a robot that does not appear in the **Robot** box (for example, a new robot).



▼ To specify a robot that does not appear in the box

1. Select **Find Robots**.
2. Select a robot in the dialog that appears.
3. Click **OK**.

The name of the robot that you select appears in the **Robot** box, and is also the robot name that will be in the volume database, for the volumes you are moving.

Volume Group

The following table shows the results if you do not specify a volume group (you leave the volume group blank):

If you Leave Volume Group Blank for	Media Manager
Standalone volumes	Does not assign a volume group.
Robotic volumes	Generates a volume group name by using the robot number and type. For example, if the robot is a TS8 and has a robot number of 50, the group name will be 00_050_TS8.

Rules for Moving Volumes Between Groups

- ◆ You must move volumes to a new volume group or to an existing volume group that has the same type of volumes as you are moving.
- ◆ All volumes in a robotic library *must* belong to a volume group. You cannot move volumes into a robotic library without specifying a group or having Media Manager generate a volume group name.
- ◆ More than one volume group can share the same location. For example, a robotic library can contain volumes from more than one volume group and you can have more than one standalone volume group.
- ◆ All members of a group must be in the same robotic library or be standalone. That is, Media Manager will not let you add a group (or part of a group) to a robotic library, if it already exists in another robotic library.

▼ To enter a volume group

- ❖ Enter the name of the volume group for the volumes that you are moving.

▼ **To select a volume group**

- ❖ Click the **arrow** and select from the list of previously configured volume groups.

First Slot Number

For volumes in a robotic library, specify the first slot number to be used in the destination robotic library. By default, this box shows the slot number that the volume is coming from. Media Manager assigns the remainder of the slot numbers sequentially.

Note You cannot enter slot information for volumes in an API robot. The robot vendor or the operating system software (in the case of RSM robots) tracks the slot locations for these robot types.

▼ **To specify the first slot number**

- ❖ Click an **arrow** and specify the number.

Eject Volume From Robot via the Media Access Port

See “Methods for Ejecting Volumes From a Robot” on page 115 for a list of the robot types and the cases that determine when **Eject volume from robot via the media access port** is available, and for more information on using this function.

▼ **To eject one or more volumes using the media access port**

- ❖ Select **Eject volume from robot via the media access port**.

Inject Volume Into Robot via the Media Access Port

See “Methods for Injecting Volumes into a Robot” on page 114 for a list of the robot types and the cases that determine when **Inject volume into robot via the media access port** is available, and for more information on using this function.

▼ **To insert a single volume using the media access port**

- ❖ Select **Inject volume into robot via the media access port**.
The robotic library will move the volume to the correct slot.



When to Delete Volumes

There may be times when you want to delete volumes, for example if any of the following situations apply. The volume is

- ◆ No longer used and you want to recycle it by relabeling it with a different media ID.
- ◆ Unusable because of repeated media errors.
- ◆ Past its expiration date or has too many mounts, and you want to replace it with a new volume.
- ◆ Lost and you want to clean up the volume database.

Once a volume is deleted, you can discard it or add it back under the same or a different media ID.

Before deleting and reusing, or discarding a volume, ensure that it does not have any important data. NetBackup and Storage Migrator volumes have an extra safeguard against accidental deletion. Volumes assigned to either of these applications cannot be deleted while they are still assigned. See “Deassigning Volumes” on page 142.

Deleting Volumes

▼ To delete volumes

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. In the volumes pane select the volumes that you want to delete.

Note You cannot delete any assigned volumes until any application using them deassigns them.

3. Click **Edit > Delete**.

A dialog appears asking you to confirm the action.

Note If you selected only one side of an optical platter, the volume on other side is also deleted.

4. Remove the deleted volumes from the storage device.

Deleting a Volume Group

▼ To delete volume groups

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. In the volumes list, look at the Time Assigned column to check if any of the volumes in the group you want to delete are currently assigned.

If any of the volumes are assigned, you cannot delete the group until these volumes are deassigned by the application (see “Deassigning Volumes” on page 142).

Use the procedure (“Deleting Volumes” on page 136) to delete individual volumes that are unassigned.

3. Select a volume group in the tree pane.
4. Click **Edit > Delete**.
A dialog appears asking you to confirm the action.
5. Remove the deleted volumes from the storage device.

Ejecting Volumes From Robots (Actions Menu Command)

You can eject single or multiple volumes. See “Methods for Ejecting Volumes From a Robot” on page 115 for a list of robot types that determine when this command is available and more information on using this command.

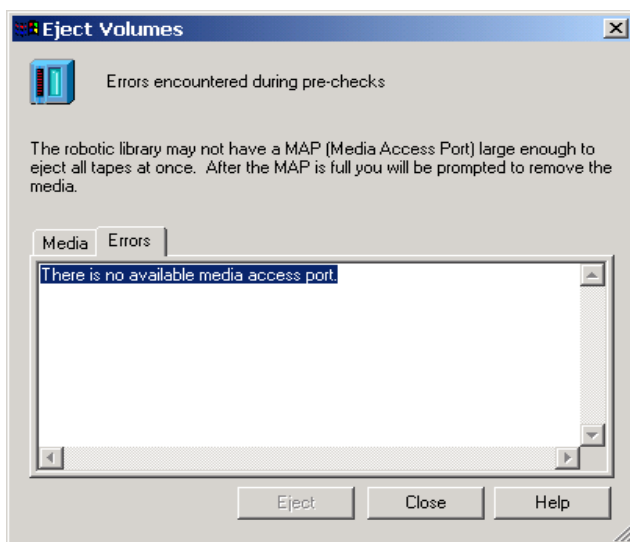
▼ To eject volumes

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. In the volumes pane, select one or more volumes that you want to eject.
3. Click **Actions > Eject Volume(s) From Robot**.
4. Depending on the robot type, you will see one of the following eject dialogs:
 - ◆ Eject Volumes Dialog Type 1
 - ◆ Eject Volumes Dialog Type 2



Eject Volumes Dialog Type 1

For some robot types, the following dialog is displayed showing the volumes you selected. See “Inject and Eject Functions Available by Robot Type” on page 117 for an explanation of the robot types where this dialog type applies.



1. In normal cases after the pre-checks for the eject are complete, the **Media** tab shows the volumes that you selected to eject and the **Errors** tab is empty.

The eject may not be possible because of an error or a hardware limitation. If an error occurs, the **Errors** tab is opened. The following two classes of errors can occur:

- ◆ For more serious errors, **Eject** will not be available and the cause of the error must be corrected.
- ◆ For other errors, the **Errors** tab shows an explanation of the error. You may continue the eject action (select **Eject**) or exit (select **Close**) depending on the type of error.

2. *The following step applies only to NetBackup Enterprise Server.*

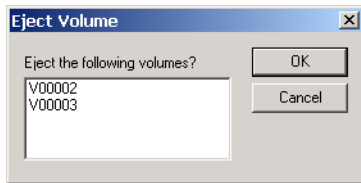
For ACS and TLM robot types only, you must select the media access port that will be used for the eject.

3. Click **Eject** to execute the eject.

The robotic library may not have a media access port large enough to eject all of the selected volumes. For most robot types, you are prompted to remove the media from the media access port so the eject can continue with the remaining volumes.

Eject Volumes Dialog Type 2

For some robot types, the following dialog is displayed, showing the volumes you selected. See “Inject and Eject Functions Available by Robot Type” on page 117 for an explanation of the robot types where this dialog type applies.



If you selected multiple volumes, operator action is required to remove each volume after each eject (prompt dialogs are used). Click **OK** to execute the eject.

Labeling Media

You can label new media or relabel used media. The media must be currently unassigned by NetBackup and have no valid NetBackup images on it.

Caution If you use this function, any data written on the media will no longer be available for a restore or import.

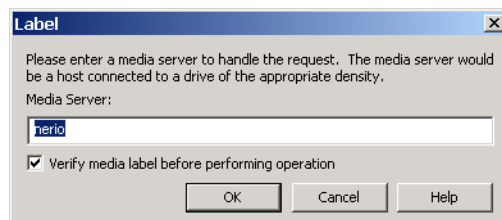
▼ To label or relabel media

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.

2. In the volumes pane, select a volume or volumes that you want to label. If multiple volumes are selected, they must all have identical robot-residence information.

The media must be currently unassigned by NetBackup and have no valid NetBackup images.

3. Click **Actions > Label**.



4. Specify the name of the media server where the drive is located that will receive the mount request for the volume.

If you want existing labels that are found on the media to be overwritten, do *not* select **Verify media label before performing operation**.

Click **OK**.

5. A dialog warning you that this action is irreversible appears.

Click **OK**, if you are certain you want to start the labeling action.

6. A dialog reminding you to use the Activity Monitor to view the progress and status of the action appears. Click **OK**.

If you selected **Verify media label before performing operation** in step 4 and the label found on the volume does not match the expected label of the volume that you specified in step 2, the media will not be relabeled. Use the Activity Monitor to view the status of the action.

Caution Canceling a label or relabel job from the Activity Monitor may not be possible for many types of drives.

Erasing Media Functions

You can do a quick (short) or long erase of used media. The media must be currently unassigned by NetBackup and have no valid NetBackup images on it. After the media is erased, a NetBackup media label is written on the media.

Note Media erase functions are not supported on NDMP drives.

Caution If you use this function, any data written on the media will no longer be available for a restore or import.

SCSI Quick Erase

If you select a quick (or short) erase, Media Manager will perform a SCSI Quick Erase. For a SCSI Quick Erase, the media is rewound and an erase gap is recorded on the media. The format of this gap is drive dependent, and can be an end-of-data (EOD) mark or a recorded pattern that is recognized by the drive as not being data.

Some drives do not support a quick erase, (for example QUANTUM DLT7000). For drives that do not support a quick erase, the new tape header that is written acts as an application-specific quick erase.

SCSI Long Erase

If you select a long erase, Media Manager will do a SCSI Long Erase. For this erase, the media is rewound and the data on the tape is overwritten with a known data pattern. A SCSI Long Erase is also called a secure erase, since it erases the recorded data completely.

Caution A long erase is a time-consuming operation and can take as long as 2 to 3 hours. For example, it takes about 45 minutes to erase a 4mm tape on a standalone drive

Erasing Media

▼ To erase media

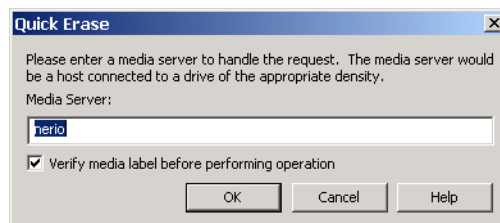
1. In the NetBackup Administration Console, click **Media and Device Management > Media**.

2. In the volumes pane, select a volume or volumes that you want to erase. If multiple volumes are selected, they must all have identical robot-residence information.

The media must be currently unassigned by NetBackup and have no valid NetBackup images.

3. For a short erase, click **Actions > Quick Erase**.

For a long erase, click **Actions > Long Erase**.



4. Specify the name of the media server where the drive is located that will receive the mount request for the volume.

If you want existing labels that are found on the media to be overwritten, do *not* select **Verify media label before performing operation**.



Click **OK**.

5. A dialog warning you that this action is irreversible appears. Click **OK** if you are certain you want to start the erase action.
6. A dialog reminding you to use the Activity Monitor to view the progress and status of the action appears. Click **OK**.

If you selected **Verify media label before performing operation** in step 4 and the label found on the volume does not match the expected label of the volume that you specified in step 2, the media will not be erased. Use the Activity Monitor to view the status of the action.

Caution Canceling an erase job from the Activity Monitor may not be possible for many types of drives.

Deassigning Volumes

An assigned volume is currently assigned for exclusive use by NetBackup or Storage Migrator (but not both). A volume is set to the assigned state when either of these applications first starts using it to store data. The time of the assignment appears in the Time Assigned column for the volume in the volumes pane. When a volume is assigned, you cannot delete it or change its volume pool.

A volume remains assigned until the application deassigns it. NetBackup and Storage Migrator deassign a volume only when they no longer need the data.

In the case of a NetBackup volume:

- ◆ A regular backup volume is deassigned when the retention period has expired for all the backups on the volume.
- ◆ A catalog backup volume is deassigned when you stop using it for catalog backups.

Determining Which Application is Using a Volume

▼ To determine which application is using the volume

- ❖ Check the Status column of the Volumes list (see “Volumes Pane” on page 96).

Deassigning NetBackup Volumes

Caution It is recommended that you *do not* manually deassign NetBackup volumes. If you do, be certain that the volumes do not have any important data. If you are uncertain, copy the images to another volume.

The procedure is different depending on whether the volume is currently being used for regular backups or for backing up the NetBackup catalogs. See the following two topics for instructions.

Deassigning NetBackup Regular Backup Volumes

NetBackup deassigns a regular backup volume when the retention periods have expired for all backups on the volume. If you do not need the data and do not want to wait for normal expiration to occur, you can expire the backup by using the `bpexpdate` command on the master server.

This command is located in the `install_path\NetBackup\bin\admincmd` directory and has the following format. *install_path* is the directory where NetBackup is installed.

```
bpexpdate -d 0 -m media id [-host hname]
```

media id is the media ID to be expired and *hname* is the name of the NetBackup media server (or SAN media server) that has the media ID (the server where media ID was written).

The following point applies only to NetBackup Enterprise Server.

Specify *hname* only if your configuration uses master servers and media servers.

The following example assumes there is only one NetBackup server and expires all the backups on media ID ABC001:

```
install_path\NetBackup\bin\admincmd\bpexpdate -d 0 -m ABC001
```

If you use this command to expire the volume, NetBackup stops tracking the backups that are on it and deassigns it. This makes the volume available to be reused, deleted, or its volume pool to be changed. You can manually expire the backups regardless of the volume's prior state (frozen, suspended, and so on).

Expiring the volume does not change anything on the volume itself. When a media is expired, however, you must use the NetBackup import feature before restoring the backups it contains (a restore is possible only if the volume has not been overwritten).

Deassigning NetBackup Catalog Backup Volumes

Volumes used for backing up the NetBackup catalogs are tracked separately from regular backup volumes.



To deassign these volumes (assuming they do not contain any important data), specify None or a different media ID for catalog backups. Then the media is available to be reassigned or deleted, or its volume pool can be changed.

See the NetBackup system administrator's guide for UNIX or the guide for Windows servers for more information.

Deassigning Storage Migrator Volumes

If a volume is assigned to Storage Migrator, you must wait for Storage Migrator to deassign them. Storage Migrator deassigns a volume when the images are no longer required. Attempting to manually deassign Storage Migrator volumes could result in loss of data. For more information on how Storage Migrator manages its volumes, see the Storage Migrator system administrator's guide for UNIX.

Changing the Attributes for a Volume

▼ To change volume attributes

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. In the volumes pane, select a volume or volumes.
3. Click **Edit > Change**.

A dialog appears and shows the media ID and other attributes for each selected volume.

Media ID	Media ...	Descri...	Max M...	Expirati...	Volum...	Cleani...
000061	HCART	Added b..	0		NetBac...	
000062	HCART	Added b..	0		NetBac...	

Maximum mounts:

☐ Do not change

☐ Unlimited

☒ Number

Expiration date:

☐ Do not change

☐ Never

☒ Date

Media description:

☐ Do not change

☒ New Description

Volume pool:

☐ Do not change

☒ New Pool

Number of cleanings remaining:

☒ Do not change

☐ New Count

4. In the dialog, change the attributes for the volume as explained in “Dialog Entries for Change Volumes” on page 145.
5. Click **OK** to apply the changes to the selected volumes.

Dialog Entries for Change Volumes

- ◆ “Maximum Mounts” on page 145
- ◆ “Expiration Date” on page 146
- ◆ “Description” on page 147
- ◆ “Volume Pool” on page 147
- ◆ “Number of Cleanings Remaining” on page 147

Maximum Mounts

Maximum Mounts does not apply to cleaning tapes.



Controls the number of times that the selected volumes can be mounted. To help determine the maximum mount limit to use, consult your vendor documentation for information on the expected life of the volume.

▼ **To not make any changes to Maximum mounts**

- ❖ Select **Do not change**.

▼ **To allow an unlimited number of mounts**

- ❖ Select **Unlimited** (**Unlimited** is the default).

▼ **To set a specific limit for the number of mounts**

1. Click **Number**.
2. Enter a number or click an **arrow** to specify the number.

When the limit is passed the volume can still be read, but it will not be mounted for a write.

Specifying zero (the default) is the same as selecting **Unlimited**.

Expiration Date

Expiration Date does not apply to cleaning tapes.

You can change the expiration date for the selected volumes. This date refers to the age of the volume and is the time at which the volume is considered too old to be reliable. When the expiration date has passed, a volume can still be read but will not be mounted for a write.

When you add a new volume, there is no default expiration date.

The expiration date is not the same as the retention period for the backup data on the volume. The expiration date that you can set in this dialog refers only to the physical expiration of the volume and is independent of the backup data written on the volume.

The backup data expiration date is managed separately by the application that is using the volume. In the case of NetBackup, the expiration date for the data is set as the retention level during schedule configuration.

▼ **To not make any changes to Expiration date**

- ❖ Select **Do not change**.

▼ **To use no expiration date**

- ❖ Select **Never**.

▼ **To set an expiration date**

1. Click **Date**.
2. Enter a number or click an **arrow** to specify the date and time.

Description

Specifies a description of how the selected volumes are being used or any other relevant information about the volumes.

▼ **To not make any changes to Description**

- ❖ Select **Do not change**.

▼ **To add a description**

1. Click **New Description**.
2. Enter the description.

Volume Pool

Volume Pool does not apply to cleaning tapes.

Specifies the desired volume pool.

▼ **To not make any changes to Volume pool**

- ❖ Select **Do not change**.

▼ **To specify a volume pool**

1. Click **New Pool**.
2. Click the **arrow** and select from the list of previously configured volume pools.

Number of Cleanings Remaining

Number of Cleanings Remaining applies only to cleaning tapes.



Specifies the number of cleanings that are allowed for the cleaning tape. This number is decremented with each cleaning and when it is zero, Media Manager stops using the tape. At this point, you can change the cleaning tape or increase the number of cleanings allowed.

▼ **To not make any changes to Number of cleanings remaining**

- ❖ Select **Do not change**.

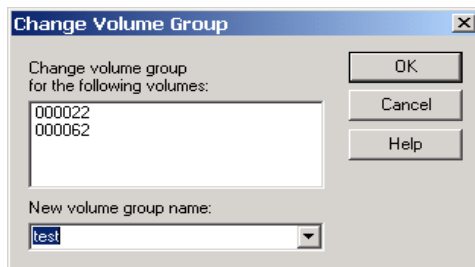
▼ **To change the number of cleanings**

1. Click **New Count**.
2. Enter a number or click an **arrow** to specify the number.

Changing the Volume Group of a Volume

▼ **To change the volume group**

1. In the NetBackup Administration Console, click **Media and Device Management > Media**.
2. In the volume list, select the volumes that you want to change the volume group assignment for.
3. Click **Actions > Change Volume Group**.



4. Enter a name in the **New volume group name** box or click the **arrow** to select a name from the list of volume groups.
5. Click **OK**.

The name change is reflected in the volume list entry for the selected volumes. If you specified a new volume group, the group appears under **Volume Groups** in the tree pane.

Exchanging Volumes

In general, you should exchange volumes (replace one volume with another volume) if the volumes meet any of the following conditions:

- ◆ Full (in this case, to exchange a volume means moving the volume out of a robotic tape library).
- ◆ Past their maximum allowable number of mounts.
- ◆ Too old (past their expiration date).
- ◆ Unusable (for example, because of repeated media errors).

The following are procedures for replacing volumes, depending on whether you want to reuse the old media ID or not.

Exchanging a Volume and Using a New Media ID

Use this procedure when the volume you are replacing has unexpired and valid NetBackup images, and you require slots in the robotic library for additional backups, duplications, vault functions, or other purposes.

In the following example the volume may be full and you require more library capacity.

▼ To exchange a volume and use a new media ID

1. Move the volume to another location (see “Moving Volumes” on page 130).

If the volume is in a robotic library, you may want to take it out of the robotic library and move it to a standalone group.

2. Add a new volume or move an existing volume in as a replacement for the volume you removed.

If you add a new volume, specify some of the same attributes as the old volume (such as, robotic residence, volume pool, and the media type). Make sure you specify a new media ID. See “Adding New Volumes” on page 119.

3. Physically replace the old volume, but do not delete the volume entry for that Media ID (in case the data on the volume needs to be retrieved).



Exchanging a Volume and Using the Old Media ID

This procedure allows you to reuse the same set of existing media IDs, which may be convenient in some instances.

Caution Reuse a media ID only if all data on the old volume is no longer needed and you are going to recycle it later, or if the volume is damaged and you are going to discard it. Otherwise, you may encounter serious operational problems and a possible loss of data.

▼ To exchange a volume and use the old media ID

1. Delete the volume entry (this will clear the mount, origination, and access statistics for the volume) and physically remove the old volume from the storage device. See “When to Delete Volumes” on page 136.
2. Physically add the new volume to the storage device.
3. Logically add the new volume to the Media Manager configuration and specify the same attributes as the old volume, including the old media ID. See “Adding New Volumes” on page 119.
4. Set a new Expiration Date for this volume. See “Changing the Attributes for a Volume” on page 144.
5. Optionally, relabel the volume. Relabeling is not required for robotic library-based media, but relabeling puts the media in a known state (the external and recorded media labels match, and the mode is known to be compatible with the drives in the robotic library).

Recycling Volumes

Caution Recycle a volume only if all NetBackup data on the volume is no longer needed, or if the volume is damaged and unusable. Otherwise, you may encounter serious operational problems and a possible loss of data.

Recycling Volumes Using the Existing Media ID

Recycling a NetBackup or Storage Migrator volume without changing its media ID is usually done when the last valid image expires. If the volume has unexpired NetBackup or Storage Migrator images, see “Deassigning Volumes” on page 142.



Recycling Volumes Using a New Media ID

Use the following procedure if a volume was previously a duplicate copy of another volume with the same media ID, or your site convention for naming volumes changes and you want to match the barcodes on the volume.

1. Physically remove the volume from the storage device.
2. If the volume is in a robotic library, move it to standalone. See “Moving Volumes” on page 130.
3. Record the current number of mounts and expiration date for the volume.
4. Delete the volume entry. See “When to Delete Volumes” on page 136.
5. Add a new volume entry, and physically add the volume to the storage device. See “Adding New Volumes” on page 119.
6. Set the maximum mounts to a value that is equal to or less than the following value that you calculate. Calculate *value* as follows:
$$\text{value} = (\text{number of mounts that the manufacturer recommends}) - (\text{the value that you recorded in step 3})$$

This is necessary because the count will start from zero for the new volume entry.
7. Set the expiration date to the value you recorded in step 3.



Managing Media in Robots

See “Starting Media Management” on page 92 for an explanation of the **Media** window that you use in the procedures of this chapter, and a list of characters that are supported by Media Manager.

Most of the operations used to manage media in robots are done using the Robot Inventory dialog (see “Overview of Robot Inventory Operations” on page 153).

In addition to the functions available in the Robot Inventory dialog, you can check the barcodes of volumes in certain robot types and update the volume database to agree with the contents of the robotic library. For detailed instructions, see “Rescanning and Updating Barcodes for a Robot” on page 207.

- ◆ If you have Backup Exec volumes to manage, see the Backup Exec tape reader topics in the NetBackup system administrator’s guide for Windows servers.
- ◆ If you have volumes without barcodes to manage, see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 325.

Overview of Robot Inventory Operations

To use the Robot Inventory dialog for robot management, you need to perform a set of common initial steps. See “Accessing the Robot Inventory Dialog” on page 155 to access and initiate these operations.

The following operations are available using the functions of the Robot Inventory dialog:

◆ Show contents

Inventories the selected robotic library and generates a report. This operation does not check or change the volume database, but is useful for determining the contents of a robot as shown in the following table:

Type of Robot	Report Contents
Robot has a barcode reader and the robot contains media with barcodes.	Shows if each slot has media and lists the barcode for the media.



Type of Robot	Report Contents
Robot does not have a barcode reader or robot does not contain media with barcodes.	Shows if each slot has media.
API robot.	Shows a list of volumes found in the robot.

For detailed instructions, see “Showing the Contents of a Robot” on page 157.

◆ **Compare contents with volume configuration**

Compares the contents of a robotic library with the contents of the Media Manager volume database. Regardless of the result the volume database is not changed. For robots without barcode readers and also containing media with barcodes, this operation is useful for determining if volumes have been physically moved within a robot.

For detailed instructions, see “Comparing Robot Contents with the Volume Configuration” on page 160.

◆ **Update volume configuration**

Inventories the selected robotic library and compares the results with the contents of the Media Manager volume database. If there are differences, Media Manager updates the volume database to match the contents of the robot.

For detailed instructions, see “Procedure To Update the Volume Configuration” on page 165.

If you select **Update volume configuration**, you also have the following capabilities available:

◆ **Advanced Options**

If you select **Advanced Options ...**, you have the following additional update capabilities available. (If the option is not applicable for a particular robotic library, the tab is not available.)

Media Settings

You can specify the volume group for existing media and specify media options for new media.

Barcode Rules

A barcode rule specifies criteria for assigning attributes to new robotic volumes. The attributes are assigned according to the barcode label that is read by the robotic library.

Media ID Generation

Using media ID generation rules allows you to override the default Media Manager media ID naming method. The default method uses the last six characters of the barcode to generate the media ID.

You control how media IDs are created by defining rules that specify which characters of a barcode label will be used in the media ID.

Media Type Mappings

You can assign media-type mappings for API robots.

- ◆ **Preview changes**

Inventories the selected robotic library and compares the results with the contents of the volume database. If there are differences, the results section shows a list of recommended changes. You can then update the volume configuration with the changes or reject the changes.

- ◆ **Empty media access port prior to update**

Allows you to move (inject) volumes in the robot's media access port into the robot.

Accessing the Robot Inventory Dialog

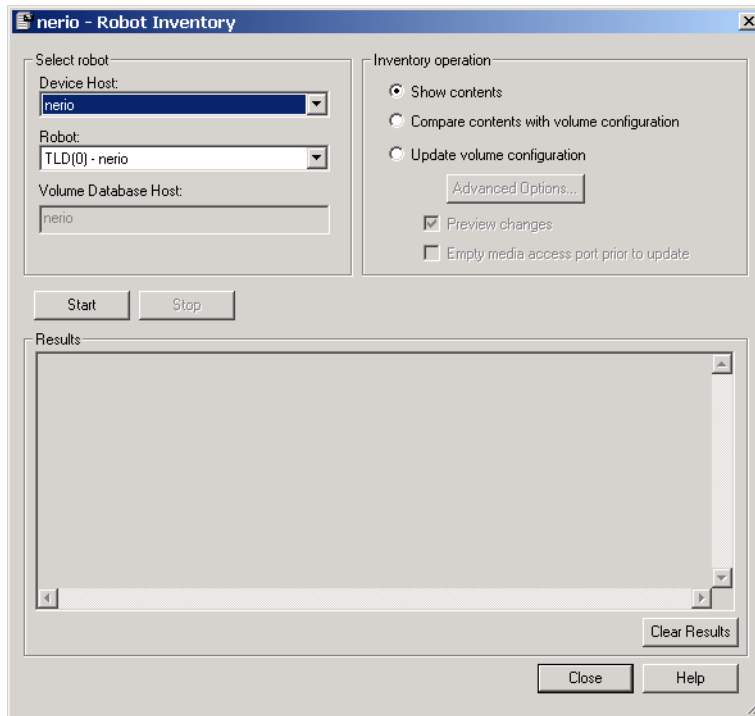
To use the Robot Inventory dialog for robot management tasks (for example, “Comparing Robot Contents with the Volume Configuration” on page 160), you will first need to perform the following set of common steps to access the Robot Inventory dialog. These steps are always required, but are not repeated in the task descriptions in this chapter.

- ▼ **To access the Robot Inventory dialog**

1. In the NetBackup Administration Console, click **Media and Device Management > Media > Robots**.
2. Select the robot you want to inventory.



3. Click **Actions > Inventory Robot**.



In the dialog, the **Device host** box contains the name of the host that controls the robot and the **Robot** box contains the selected robot.

4. *This step applies only to NetBackup Enterprise Server.*

To select a robot on a different host, click the **arrow** and select a device host from the list.

5. To select a different robotic library on a host, click the **arrow** and select from the list of robots on that host.

In the dialog, the **Device host** box contains the name of the host that controls the robot and the **Robot** box contains the robot you selected.

Showing the Contents of a Robot

▼ To show robot contents

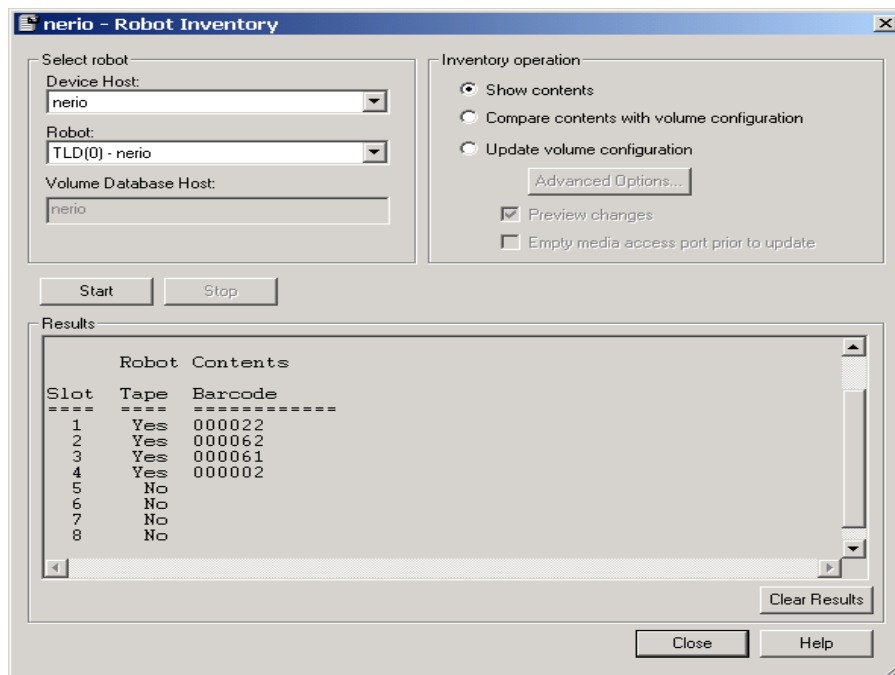
1. Perform the steps described in “Accessing the Robot Inventory Dialog” on page 155.
2. In the Inventory operation section of the Robot Inventory dialog, select **Show contents**.

To clear any previous display in the Results section, click **Clear Results**.

3. Click **Start** to start the inventory.

The inventory report appears in the Results section of the dialog.

Show Contents Report (non API robot)



For robots (other than API robots) that have a barcode reader, Media Manager obtains the barcode from the robot and includes it in the report.

See “Robot Attributes” on page 279 for information on the robots that support barcode readers and the supported barcode length.

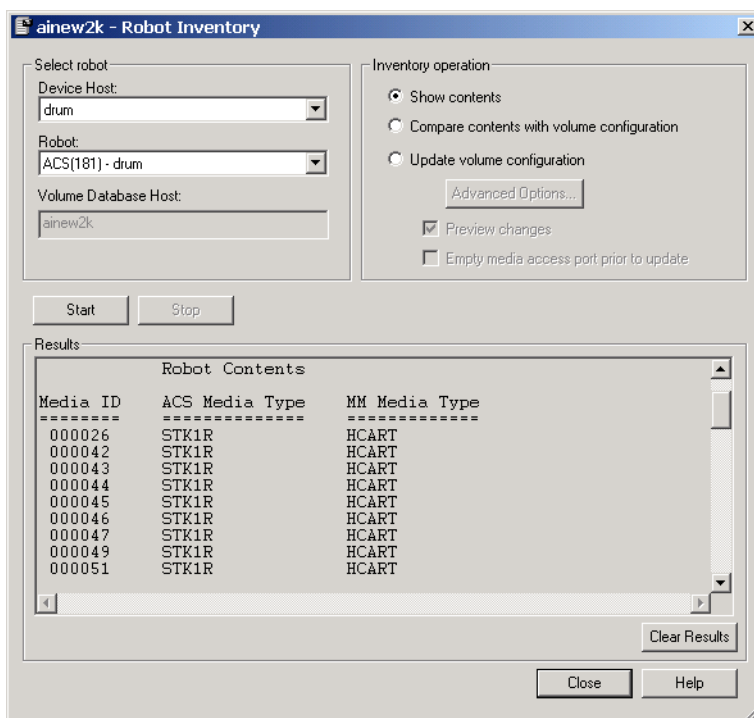


See “How Contents Reports for API Robots are Generated” on page 158 for information on the reports that are generated for API robots.

How Contents Reports for API Robots are Generated

The following figure shows an example report for an ACS robot. The reports for other API robots are similar to this report.

Show Contents Report (API Robot)



ACS Robots

This is a NetBackup Enterprise Server topic.

Media Manager reports what it receives from ACS library software. The resulting report shows the ACS library software volume ID, the ACS media type, and the Media Manager media type.

- ◆ The Media Manager media ID corresponds to the ACS library software volume ID.

- ◆ The report shows the mapping between the ACS library software media type and the corresponding Media Manager media type (without considering optional barcode rules).

See “Robot Inventory Operations” on page 386 for more information on how Media Manager reports what it receives from ACS library software.

LMF Robots

This is a NetBackup Enterprise Server topic.

Media Manager reports what it receives from the Library Management Facility (LMF). The resulting report shows the volser (volume serial number), the LMF media type, and the Media Manager media type.

- ◆ The Media Manager media ID corresponds to the LMF volser.
- ◆ The report shows the mapping between the LMF media type and the corresponding Media Manager media type (without considering optional barcode rules).

See the LMF appendix in the NetBackup Media Manager system administrator’s guide for UNIX for more information on how Media Manager reports what it receives from LMF.

RSM Robots

Media Manager reports what it receives from the Windows Removable Storage service. The resulting report shows a list of media (by media name) obtained from the service along with their RSM and Media Manager media types.

See the RSM appendix, “Microsoft Removable Storage Manager (RSM)” on page 391 for more information on how Media Manager translates what it receives from the Removable Storage service.

TLH Robots

This is a NetBackup Enterprise Server topic.

Media Manager reports what it receives from the Automated Tape Library (ATL) library manager. The resulting report shows the volser (volume serial number), the ATL media type, and the Media Manager media type.

- ◆ The Media Manager media ID corresponds to the ATL volser.
- ◆ The report shows the mapping between the ATL media type and the corresponding Media Manager media type (without considering optional barcode rules).



See the TLH appendix, “IBM Automated Tape Library (ATL)” on page 399 for more information on how Media Manager reports what it receives from the IBM ATL library manager.

TLM Robots

This is a NetBackup Enterprise Server topic.

Media Manager reports what it receives from DAS/SDLC server. The resulting report shows the volser (volume serial number), the DAS/SDLC media type, and the Media Manager media type.

- ◆ The Media Manager media ID corresponds to the DAS/SDLC volser.
- ◆ The report shows the mapping between the DAS/SDLC media type and the corresponding Media Manager media type (without considering optional barcode rules).

See the TLM appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 411 for more information on how Media Manager reports what it receives from the DAS/SDLC server.

Comparing Robot Contents with the Volume Configuration

▼ To compare robot contents with the volume configuration

1. Perform the steps described in “Accessing the Robot Inventory Dialog” on page 155.
2. In the Inventory operation section of the Robot Inventory dialog, select **Compare contents with volume configuration**.

To clear any previous display in the Results section, click **Clear Results**.

3. Click **Start** to start the compare.

Media Manager requests an inventory from the selected robotic library and compares the results from the robot with the contents of the volume database.

See “Compare Volume Configuration Reports” on page 161 for information on the reports that are generated.

4. If the report shows that the volume database does not match the contents of the robotic library, do *one* of the following:

- a. Physically move the volume.
- b. Correct the condition by using **Media and Device Management > Media > Actions > Move** or by updating the volume configuration as explained in “Procedure To Update the Volume Configuration” on page 165.

Compare Volume Configuration Reports

The Results section of the dialog shows any discrepancies as follows:

- ◆ If the robot can read barcodes (see “Robot Attributes” on page 279), the report includes barcode information. Media Manager determines if the barcodes in the robot match those in the volume database.

The following figure shows a sample compare report.

Note *Selecting a device host applies only to NetBackup Enterprise Server.*

Compare Contents Report (Non-API Robot That Can Read Barcodes)

Robot Contents			Volume Configuration		
Slot	Tape	Barcode	Media ID	Barcode	Mismatch Det
1	Yes	000022	000022	000022	
2	Yes	000062	000062	000062	
3	Yes	000061	000061	000061	
4	Yes	000002	000002	000002	
5	No				
6	No				
7	No				
8	No				

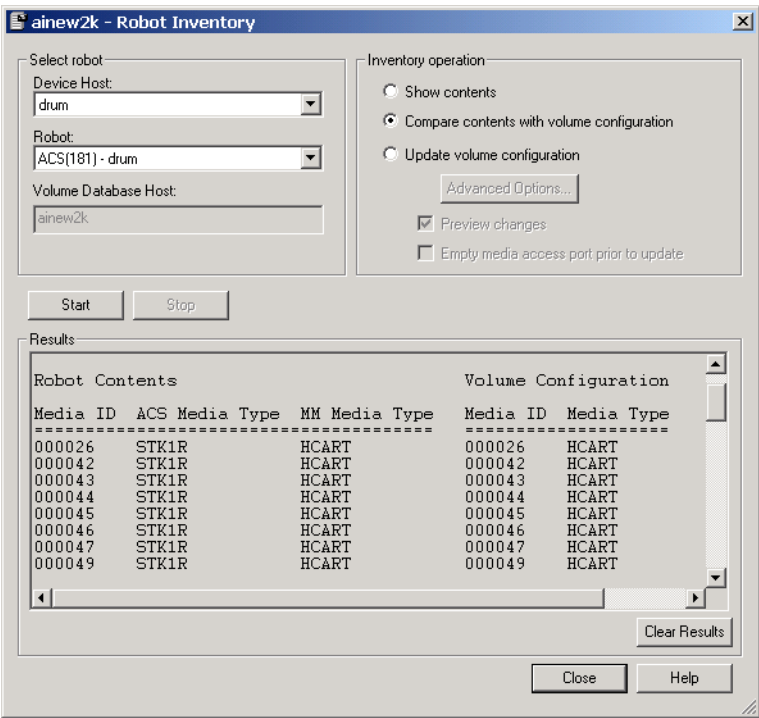


- ◆ For API robots, Media Manager determines whether the media ID and media type in the Media Manager volume database matches what it receives from the vendor’s service library software database or from Windows Removable Storage in the case of RSM robots.

The following figure shows an example compare report for an ACS robot. Reports for other API robots are similar to this report.

See “Robot Inventory Operations” on page 386 for more information on what Media Manager receives from ACS library software.

Compare Contents Report (API Robot)



- ◆ If the robotic library cannot read barcodes, Media Manager verifies only whether the volume database correctly shows whether a slot contains a volume.

Updating the Volume Configuration for a Robot

The following topics explain how to inventory a robotic library and optionally update the volume database to match the contents of the robotic library.

- ◆ “When to Use Update Volume Configuration” on page 163

- ◆ “When Not to Use Update Volume Configuration” on page 164
- ◆ “Updating the Volume Configuration for Non-Barcoded Media” on page 165
- ◆ “Procedure To Update the Volume Configuration” on page 165
- ◆ “Media Settings Tab (Advanced Options)” on page 168
- ◆ “Barcode Rules Tab (Advanced Options)” on page 179
- ◆ “Media ID Generation Tab (Advanced Options)” on page 184
- ◆ “Media Type Mappings Tab (Advanced Options)” on page 188

When to Use Update Volume Configuration

You can use this operation on robots that Media Manager supports, regardless of whether they can read barcodes or not. The update volume configuration operation is useful for updating the volume’s configuration information that is stored in the Media Manager volume database, after performing one of the following tasks:

- ◆ Removing existing volumes from a robotic library.

This operation updates the residence information in the volume database to show the new standalone location. You specify the volume group to use.

- ◆ Inserting new volumes into a robotic library.

The configuration update includes creation of media IDs (based on barcodes or a prefix that you specify).

When you use barcode rules, a new volume that is added by using a barcode rule is also assigned a media type, volume pool, maximum number of mounts (or maximum number of cleanings), and description. For instructions on setting up barcode rules see “Barcode Rules Tab (Advanced Options)” on page 179.

If the robotic library supports barcodes and the volume has readable barcode labels, the operation creates new volume entries in the volume database with media IDs that are based on the last six characters of the barcodes as the default. The specific characters that you specify are used, if you are using media ID generation rules (see “Media ID Generation Tab (Advanced Options)” on page 184).

If the robotic library does not support barcodes or the volumes do not have readable barcodes, the new media IDs are based on a media ID prefix that you specify.

For more information, see “Adding New Volumes” on page 119.

If the robotic library supports barcodes and the volume has a readable barcode, you can use this operation in the following cases. If you are

- ◆ Inserting existing volumes into a robotic library.



The operation updates the residence information in the Media Manager volume database, to show the new robotic location. This includes the robot host, robot type, robot number, and slot location. You specify the volume group to use.

- ◆ Physically moving existing volumes within a robotic library.

The operation updates the residence information in the volume database, to show the new slot location.

- ◆ Physically moving volumes between robotic and standalone.

The operation updates the residence information in the volume database, to show the new robotic or standalone location.

- ◆ Physically moving volumes from one robotic library to another.

If the volumes for the robots are in the same volume database (the default for NetBackup Server), you must perform two separate updates. These updates move the volumes to standalone as an intermediate step, and then to the new robot. If these updates are not done, Media Manager is unable to update the entries and you receive an “Update failed” error.

See “Example 6: Moving Existing Volumes Between Robots” on page 204.

When Not to Use Update Volume Configuration

The following situations require a move operation or use of the Media Manager physical inventory utility (see “Updating the Volume Configuration for Non-Barcoded Media” on page 165), rather than using Update volume configuration:

- ◆ After inserting existing volumes into a robotic library, and the volume does not have readable barcodes or the robotic library does not support barcodes.

Without barcodes, Media Manager cannot identify the volume and assigns a new media ID that uses the media ID prefix you select for the update. A volume entry for the old media ID remains in the volume database. An error may occur later, if an application attempts to use the new or old volume.

- ◆ After physically moving existing volumes that do not have readable barcodes or if the volumes are in a robot that does not support barcodes.

If you swap volumes between two different locations, Media Manager is unable to detect the change and cannot update the volume database.

If you remove a volume from a slot and place it in an empty slot, Media Manager assumes it is a new volume. Media Manager then adds a new logical volume entry with a generated media ID at its new robotic location. The volume entry for the old media ID is moved to standalone.

An error may occur if an application attempts to use the volume entry with the new or old media ID. See “Example 7: Adding Existing Volumes when Barcodes are Not Used” on page 205.

Updating the Volume Configuration for Non-Barcoded Media

If the robotic library does not support barcodes or the volumes do not have readable barcodes, consider using the Media Manager physical inventory utility. `vmphyinv`, the physical inventory utility, performs a physical inventory on non-barcoded tape libraries by mounting the tape, reading the tape header, identifying the tape in each slot, and updating the Media Manager volume database.

See “Using the Physical Inventory Utility for Non-Barcoded Media” on page 325 for more information.

Procedure To Update the Volume Configuration

The following point applies only to NetBackup Enterprise Server.

Before adding a volume to the Media Manager volume database, you *must* be managing the correct server or the volume will not be found when it is requested later.

▼ To determine the capabilities of a robot

1. Check the barcode capabilities of the robotic library and the volume by performing the procedure “Comparing Robot Contents with the Volume Configuration” on page 160.

Determine if the robotic library supports barcodes *and* if any new volume that was inserted into the library has readable barcodes.

2. If the robotic library does *not* support barcodes or the volume does *not* have readable barcodes, you may want to save the results of the compare operation, as it may be useful in deciding on a media ID prefix if you use the **Media Settings** tab in **Advanced Options** to assign a prefix later in the following procedure.

You also may want to consider using the Media Manager physical inventory utility (see “Updating the Volume Configuration for Non-Barcoded Media” on page 165).

▼ To update the volume configuration for a robot

1. Perform the steps described in “Accessing the Robot Inventory Dialog” on page 155.
2. In the Inventory operation section of the Robot Inventory dialog, select **Update volume configuration**.



3. For more options, click **Advanced Options** For most configurations, the default settings work well. You should only change the settings if your configuration has special hardware or usage requirements.

The advanced update options allow you to do the operations shown in the following table:

Advanced Operation	For More Information
Assign media settings for new and existing media.	See “Media Settings Tab (Advanced Options)” on page 168.
Create barcode rules.	See “Barcode Rules Tab (Advanced Options)” on page 179.
Create media ID generation rules.	See “Media ID Generation Tab (Advanced Options)” on page 184.
Map media for API robots. If you do not map media, default media types are used.	See “Media Type Mappings Tab (Advanced Options)” on page 188.

4. To preview any update changes for the configuration, select **Preview changes**.
During a preview session, Media Manager lists any recommended changes and lets you confirm whether to proceed with the update. This allows you to preview and ensure that all new media have barcodes before they are added to the Media Manager volume database.
5. To move (inject) one or more volumes in the robot’s media access port into the robotic library before initiating the update, select **Empty media access port prior to update**.
Any volumes to be injected must be in the media access port before the operation begins. If **Empty media access port prior to update** is selected and there are no volumes in the port, you are *not* prompted to place volumes in the media access port and the update operation continues.
Review “Methods for Injecting Volumes into a Robot” on page 114 for a list of robot types that determine when **Empty media access port prior to update** is available and more information on using this function.

Note If you have recently ejected volumes from the robot with the eject or move volume Media Manager commands, remove the volumes from the media access ports before performing an inject with **Empty media access port prior to update** selected. Otherwise, if the entry and exit ports are the same, the volumes that you ejected could be injected back into the robotic library.

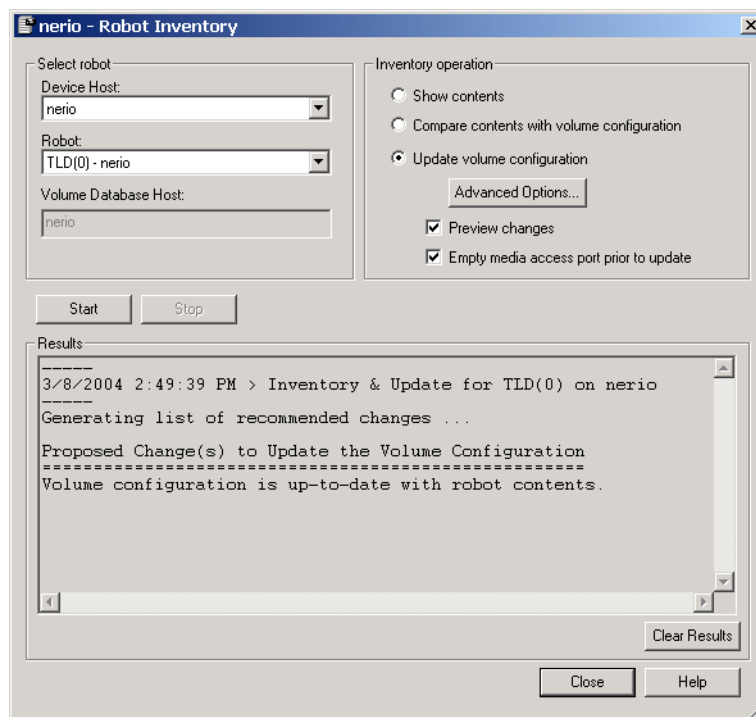
6. To clear any previous display in the Results section, click **Clear Results**.
Click **Start** to start the update (or the preview).
7. If you selected **Preview changes** and any recommended changes are found, the dialog will ask if you want to accept the recommended changes shown in the Results section.
Select **Yes** to perform the update with the recommended changes.

Example Update Volume Configuration Reports

The following figure shows example results for a robotic library that is not an API robot.

Note *Selecting a device host applies only to NetBackup Enterprise Server.*

Update Volume Configuration Report (Not an API Robot)

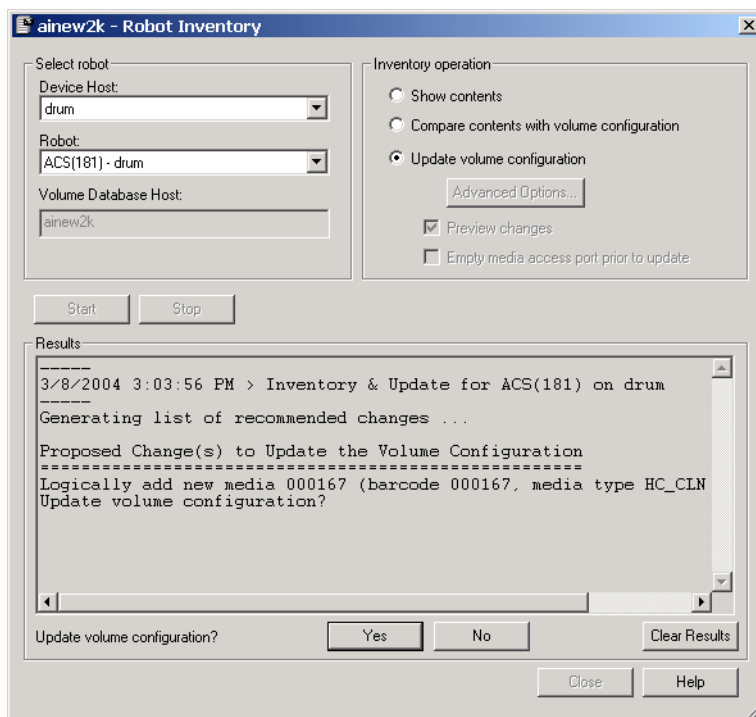


The following figure shows an example report for an ACS robot. Reports for other API robots are similar to this report.

Robot inventory update will return an error if it encounters unsupported characters in the volume serial number or media identifier that are returned by API robots.



Update Volume Configuration Report (API Robot)



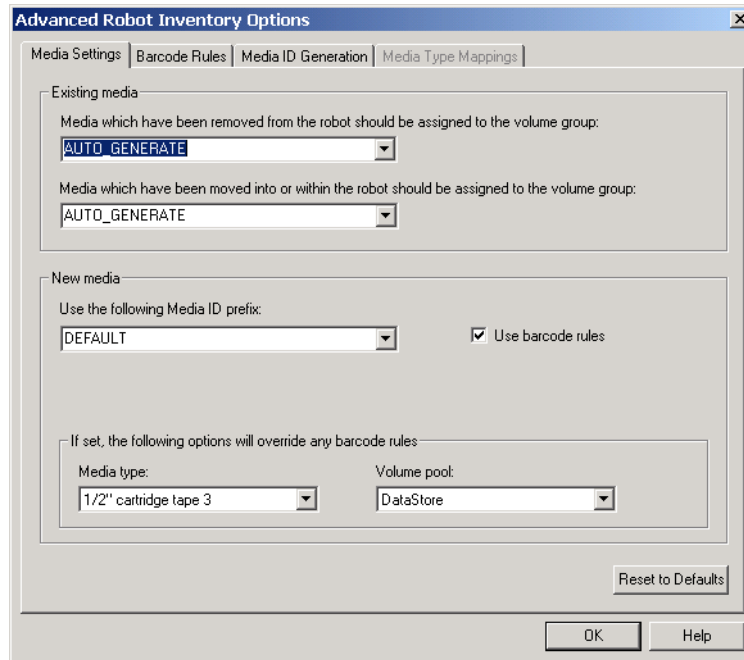
Media Settings Tab (Advanced Options)

You can use the options on this tab to specify the volume group for existing media and specify media options for new media.

Setting Media Options

▼ To use the Media Settings tab

1. In the Advanced Robot Inventory Options dialog, click **Media Settings**.



2. Specify the properties for this tab, as explained in “Properties for the Media Settings Tab” on page 169.

To reset all properties on this tab to their defaults, click **Reset to Defaults**.

3. When you are satisfied with your settings, click **OK** to return to the Robot Inventory dialog to continue the update.

Properties for the Media Settings Tab

The following sections explain the settings you can use on this tab.

- ◆ “Media Which Have Been Removed From the Robot ...” on page 170
- ◆ “Media Which Have Been Moved Into or Within the Robot ...” on page 171
- ◆ “Use the Following Media ID Prefix” on page 172
- ◆ “Use Barcode Rules” on page 173



- ◆ “Media Type” on page 173
- ◆ “Volume Pool” on page 178

Media Which Have Been Removed From the Robot ...

This property specifies the volume group that Media Manager assigns to existing media that you have removed from the robot.

If you leave the volume group set at `DEFAULT` and there is an existing group with a compatible residence for the volume, the volume is added to that group. If a suitable volume group does not exist, Media Manager generates a new volume group name.

▼ **To specify a volume group other than `DEFAULT`**

Do *one* of the following:

- ❖ Enter a volume group name in the box.
- ❖ Click the **arrow** and select from the list of choices for the volume group that Media Manager can assign to volumes that you have removed from the robot. The list always has the choices shown in the following table.

Select	To
DEFAULT	Let Media Manager choose the volume group.
AUTO-GENERATE	Automatically generate a new volume group.
NO VOLUME GROUP	Not assign a volume group.

The other available volume group choices shown in the list depend on the Media type selection as shown in the following table. See “Media Type” on page 173.

If the Media Type is	The List Shows Existing Volume Groups that are Valid for
DEFAULT	The robot’s default media type (see “Specifying Media Type (when not using barcode rules)” on page 175).
Not DEFAULT	The specified media type.

Media Which Have Been Moved Into or Within the Robot ...

This property specifies the volume group that Media Manager assigns to existing media that you have inserted into the robot (or moved to a new location within the robot).

If you leave the volume group set at `DEFAULT` and there is an existing group with a compatible residence for the volume, the volume is added to that group. If a suitable volume group does not exist, Media Manager generates a new volume group name.

▼ To specify a volume group other than `DEFAULT`

Do *one* of the following:

- ❖ Enter a volume group name in the box.
- ❖ Click the **arrow** and select from the list of choices for the volume group that Media Manager can assign to volumes that you have moved into the robot. The list always has the choices shown in the following table.

Select	To
DEFAULT	Let Media Manager choose the volume group.
AUTO-GENERATE	Automatically generate a new volume group.

Note If the robotic library contains multiple media types, it is better to leave the volume group setting at `DEFAULT`. If you specify a volume group and volumes of different media types have been moved into or within the robotic library since the last update, the new update will fail. This occurs because volumes of differing media types cannot have the same volume group.

The other available volume group choices shown in the list depend on the Media type selection as shown in the following table. See “Media Type” on page 173.

If the Media Type is	The List Shows Existing Volume Groups that are Valid for
DEFAULT	The robot’s default media type (see “Specifying Media Type (when not using barcode rules)” on page 175).
Not DEFAULT	The specified media type.



Use the Following Media ID Prefix

You should specify a Media ID prefix for any new media, if either of the following conditions exist:

- ◆ The robotic library does not support barcodes.
- ◆ The volume that was inserted does not have readable barcodes.

If the robotic library supports barcodes and the volume has readable barcodes, a prefix is *not* required because Media Manager creates the media ID in one of the following ways. This is true whether or not a barcode rule is used.

- ◆ As the default, Media Manager assigns the last six characters of the barcode as the media ID.
- ◆ You specify specific characters for the media ID using Media ID generation rules. See “Media ID Generation Tab (Advanced Options)” on page 184.

The list of available prefixes displayed will be similar to the following example list. The first two items in this example list are configured media ID prefixes. These prefixes are based on `MEDIA_ID_PREFIX` entries that were added to the `vm.conf` file on the host where you are running NetBackup administration.

NV
NETB
DEFAULT
NOT USED

See “The Media Manager Configuration File (`vm.conf`)” on page 355 for an overview of this configuration file.

DEFAULT always appears in the selection list. If you select DEFAULT, Media Manager checks the configuration file for `MEDIA_ID_PREFIX` entries, as shown in the following table:

If the <code>vm.conf</code> File	Then Media Manager
Contains prefix entries	Assigns the last entry as the default prefix.
Does <i>not</i> contain prefix entries	Uses the letter A, as the default prefix.

NOT USED also always appears in the selection list. If you select NOT USED, the operation succeeds only if the robotic library supports barcodes and the volume has readable barcodes. Otherwise, Media Manager is unable to assign new media IDs and the operation fails. NOT USED may be useful if you are using barcoded volumes and want updates to fail when unreadable or missing barcodes are encountered.

If you want media IDs for media generated based on a specific prefix, you can specify a media ID prefix using either of the following methods:

▼ **To specify a media ID prefix by entering a new value**

- ❖ Enter a new value for the prefix in the text box.

The prefix that you enter is used only for the current operation. It is *not* added to the `vm.conf` file.

You can specify a prefix having from one to five alpha-numeric characters. Media Manager assigns the remaining numeric characters to create six characters. For example, if the prefix is NETB, the media IDs are: NETB00, NETB01, and so on.

▼ **To specify a media ID prefix by selecting from the list**

- ❖ Click the **arrow** and select a choice for the prefix.

Use Barcode Rules

Use this check box to specify whether or not you are using barcode rules for new media. Your choices and the resulting actions are shown in the following table:

If You	Then Media Manager
Select Use barcode rules	Searches existing barcode rules and applies the rules to new volumes that have been inserted into a robot.
Clear Use barcode rules	Ignores barcode rules.

▼ **To specify if you are using barcode rules**

- ❖ Select or clear the check box.

Media Type

Media type is not available for API robots (for example, an ACS robot or RSM robot). Media type is always set to DEFAULT for API robots.

See “Media Type Mappings Tab (Advanced Options)” on page 188 for instructions for specifying media types for API robots.

Use **Media type** to specify the media type for new media that is being added to a robot. The list displayed shows the media types that are valid for the robot. The following is an example list for a TLD robotic library:



DEFAULT
1/2 cartridge tape
1/2 cartridge tape 2
8MM cartridge tape
8MM cartridge tape 2
8MM cartridge tape 3
DLT cartridge tape
DLT cartridge tape 2
DLT cartridge tape 3
DTF cartridge tape
1/2 cleaning tape
1/2 cleaning tape 2
8MM cleaning tape
8MM cleaning tape 2
8MM cleaning tape 3
DLT cleaning tape
DLT cleaning tape 2
DLT cleaning tape 3
DTF cleaning tape

▼ **To specify the media type for new media**

The steps you follow to select a media type depend on whether or not you are using barcode rules, as shown in the following table:

Are You Using Barcodes? See the Instructions in	
No	“Specifying Media Type (when not using barcode rules)” on page 175.
Yes	“Specifying Media Type (when using barcode rules)” on page 176.

Specifying Media Type (when not using barcode rules)

Click the **arrow** to select from the list of media types that are valid for this robotic library. If you want to use the media type shown in first column of the following table, select the type as described in the second column.

Media Type	Select
The default media type	<p>DEFAULT.</p> <p>If <i>all</i> of the drives in the robotic library (configured on this robot host) are</p> <ul style="list-style-type: none"> ♦ The same type and at least one drive is configured on the robot control host, then Media Manager uses the media type for the drives. ♦ <i>Not</i> the same type, then Media Manager uses the default media type for the robotic library.
A media type other than the default media type	<p>A media type from the list.</p> <p>Selecting a type from the list is required, if the robotic library supports multiple media types and you do not want the default media type.</p> <p><i>The following point applies only to NetBackup Enterprise Server.</i></p> <p>Selecting a type from the list is required if your drives are not configured on the robot control host and the drives are not the default media type for the robot.</p>

The following table shows the default media types for robots when drives are not configured on the robot control host:

Default Media Types for Robots (Not API robots)

Robot Type	Default Media Type
Optical Disk Library (ODL)	<p>Rewritable optical disk.</p> <p>Also supports write-once read-many (WORM) operations.</p>
Tape Library 4MM (TL4)	4MM cartridge tape.
Tape Library 8MM (TL8)	<p>8MM cartridge tape.</p> <p>Also supports 8MM cartridge tape 2 and 8MM cartridge tape 3.</p>



Default Media Types for Robots (Not API robots) (continued)

Robot Type	Default Media Type
Tape Library DLT (TLD)	DLT cartridge tape. Also supports DLT cartridge tape 2, DLT cartridge tape 3, 1/2-inch cartridge tape, 1/2-inch cartridge tape 2, 1/2-inch cartridge tape 3, 8MM cartridge tape, 8MM cartridge tape 2, 8MM cartridge tape 3, DTF cartridge tape, and 1/4-inch cartridge tape.
Tape Stacker 8MM (TS8)	8MM cartridge tape. Also supports 8MM cartridge tape 2 and 8MM cartridge tape 3.
Tape Stacker DLT (TSD)	DLT cartridge tape. Also supports DLT cartridge tape 2 and DLT cartridge tape 3.
Tape Stacker Half-inch (TSH)	1/2-inch cartridge. Also supports 1/2-inch cartridge tape 2 and 1/2-inch cartridge tape 3.

Specifying Media Type (when using barcode rules)

Click the **arrow** to select from the list of media types that are valid for this robotic library. If you want

- ◆ To let the barcode rule determine the media type that is assigned, select **DEFAULT** as the media type.

For example, assume you want to add DLT and half-inch cartridges to a TLD robot with a single update operation. First create separate barcode rules for DLT and half-inch cartridges and select the specific media types in the barcode rules. Then, select **DEFAULT** on the **Media Settings** tab. Media Manager now will use the media type in the barcode rules when it does the update.

Note If you choose **DEFAULT** on the **Media Settings** tab and **DEFAULT** in the barcode rule, Media Manager assigns the default media type for the robotic library.

- ◆ To use a media type other than the default, select a specific media type from the list.
For example, to use the same barcode rule to add DLT or half-inch cartridges to a TLD robot, select a specific media type on the **Media Settings** tab and select **DEFAULT** for the barcode rule media type when you create the barcode rule. Now you can perform one update for DLT and another for half-inch cartridge and use the same rule for both.

The media type on the **Media Settings** tab always overrides the media type of the barcode rule. If you specify any value other than `DEFAULT` on the **Media Settings** tab, the media type for the barcode rule must be the same media type or be `DEFAULT` in order to obtain a match (except for cleaning media).

The following table shows some example combinations of media types on the **Media Settings** tab and barcode rule media types for a TLD (non-API) robot and the result:

Media Type (Media Settings tab)	Barcode Rule Media Type	Rule Matches?	Media Type Added to Volume Configuration
DLT	DEFAULT	Yes	DLT
HCART	DEFAULT	Yes	HCART
DLT	DLT	Yes	DLT
DLT	DLT_CLN	Yes	DLT_CLN
DLT_CLN	DLT	No	DLT_CLN
DLT_CLN	DLT_CLN	Yes	DLT_CLN
DLT_CLN	DEFAULT	Yes	DLT_CLN
DLT	8MM, 4MM, and so on	No	DLT
DEFAULT	DEFAULT	Yes	DLT
DEFAULT	DLT	Yes	DLT
DEFAULT	DLT_CLN	Yes	DLT_CLN
DEFAULT	8MM, 4MM, and so on	No	Depends on robot type.

The fourth barcode rule in the table shows Media Manager's ability to add cleaning cartridges with regular volumes when you execute an update for a robotic library.

If the volumes that you insert include a cleaning tape, Media Manager adds the volumes correctly. This happens if the following are all true:

- ◆ The media type on the **Media Settings** tab is for regular media (DLT, in this example).
- ◆ The barcode matches a barcode tag.
- ◆ The media type for the barcode rule is cleaning media (DLT_CLN).



Also see “Example 5: Adding Cleaning Tapes to a Robot” on page 203.

The sixth and seventh rules in the table illustrate how to add only a cleaning tape. In the sixth rule, you specify the cleaning media type on the **Media Settings** tab and in the barcode rule. In the seventh rule, you specify the cleaning media on the **Media Settings** tab and choose default when you configure the barcode rule.

Volume Pool

Use this property to specify the volume pool to which you want to assign the new media. The list displayed will be similar to the following example list:

DEFAULT
None
NetBackup
DataStore
a_pool
b_pool

▼ **To specify a volume pool**

- ❖ Click the **arrow** and select from the list of volume pools as shown in the following table:

If You are Using Barcode Rules and You Want	Then Select
To let the barcode rule determine the volume pool that is assigned to new volumes.	DEFAULT from the list.
To use a volume pool other than the default.	That volume pool name in the list. The volume pool on the Media Settings tab always overrides the rule.
If You are <i>Not</i> Using Barcode Rules and You Want	Then Select
To use the NetBackup volume pool for data volumes and no volume pool for cleaning tapes.	DEFAULT from the list.
To use a volume pool other than the default.	That volume pool name in the list.

Barcode Rules Tab (Advanced Options)

A barcode rule specifies criteria for assigning attributes to new robotic volumes. The attributes are assigned according to the barcode label that is read by the robotic library. You choose whether to use barcode rules when you assign media settings (see “Use Barcode Rules” on page 173).

The following topics explain how to manage barcode rules:

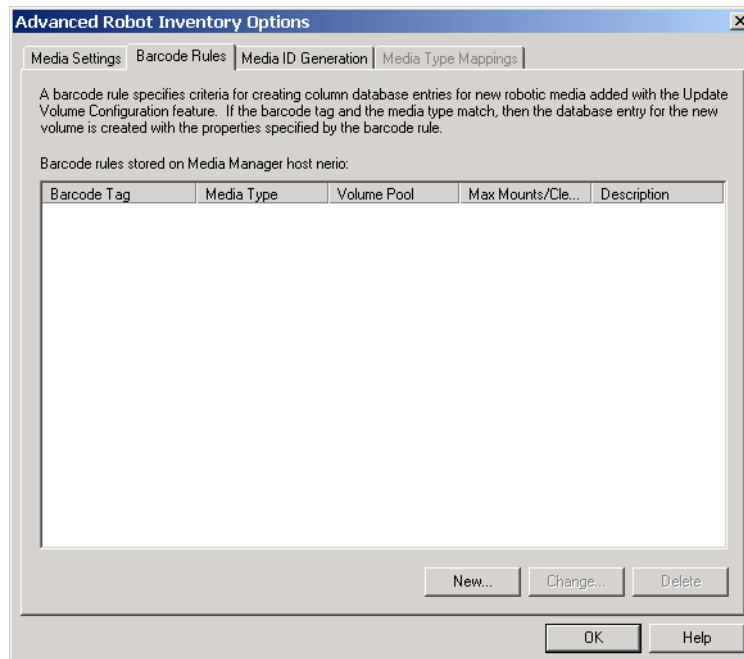
- ◆ “Adding a New Barcode Rule” on page 179
- ◆ “Changing a Barcode Rule” on page 180
- ◆ “Deleting a Barcode Rule” on page 181
- ◆ “Dialog Properties for Adding or Changing Barcode Rules” on page 181

For background information, see “Barcode Rules” on page 323.

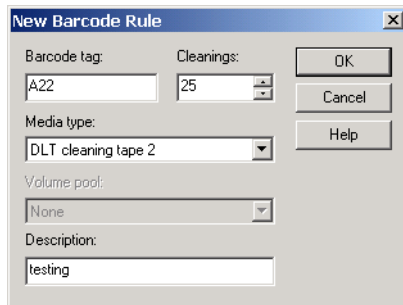
Adding a New Barcode Rule

▼ To add a barcode rule

1. In the Advanced Robot Inventory Options dialog, click **Barcode Rules**.



2. On the **Barcode Rules** tab, click **New ...**



3. Specify the properties for the new barcode rule.
See “Dialog Properties for Adding or Changing Barcode Rules” on page 181 for help on specifying these properties.
4. When you are satisfied with your settings, click **OK** to return to the Robot Inventory dialog and proceed with the update.

Changing a Barcode Rule

▼ To change a barcode rule

1. In the Advanced Robot Inventory Options dialog, click **Barcode Rules**.
2. In the **Barcode Rules** tab, select the rule that you want to change from the rules that are listed.
3. Click **Change ...**
4. In the dialog that appears, specify your changes. See “Dialog Properties for Adding or Changing Barcode Rules” on page 181 for help in changing the properties of the rule.

You cannot change the barcode tag of a barcode rule using the change dialog. To change a barcode tag, you must first delete the old rule and then add a rule with a new barcode tag.
5. When you are satisfied with your settings, click **OK** to return to the Robot Inventory dialog and proceed with the update.

Deleting a Barcode Rule

▼ To delete a barcode rule

1. In the Advanced Robot Inventory Options dialog, click **Barcode Rules**.
2. In the **Barcode Rules** tab, select the rule you want to delete from the list of rules.
3. Click **Delete**.
In the confirmation dialog, confirm or cancel the delete.
4. When you are done, click **OK** to return to the Robot Inventory dialog and proceed with the update.

Dialog Properties for Adding or Changing Barcode Rules

The following topics explain the settings you can make in this dialog.

- ◆ “Barcode Tag” on page 181
- ◆ “Maximum Mounts” on page 182
- ◆ “Media Type” on page 182
- ◆ “Volume Pool” on page 184
- ◆ “Description” on page 184

Barcode Tag

The barcode tag can have from 1 to 16 characters, but cannot contain any spaces (or special characters that appear as spaces). In the Media Manager barcode rule and volume databases, a barcode tag can have a maximum of 16 characters. But in the volume database not all 16 characters for the tag are used for all robot types.

See the Barcode Support attribute of the tables listed in “Robot Attributes” on page 279 for the maximum barcode lengths that are supported by Media Manager for each robot type.

The following rules can have special characters in the barcode tags:

- ◆ <NONE> - Matches when rules are used and the volume has an unreadable barcode or the robotic library does not support barcodes.
- ◆ <DEFAULT> - For volumes with barcodes, this tag matches when none of the other barcode tags match, providing the media type in the <DEFAULT> rule and the media type on the **Media Settings** tab are compatible.

Use the **Media Settings** tab to set up the criteria for a robot update (see “Media Settings Tab (Advanced Options)” on page 168).



▼ To specify a barcode tag

- ❖ Enter a tag for the rule.

Maximum Mounts

This setting is used to specify the maximum number of mounts (or cleanings) that are allowed for this volume. When a barcode rule is used, Media Manager adds the number you select to the volume database for the media ID.

Note When you specify zero (unlimited), a cleaning tape whose barcode label matches the rule will be assigned a zero for Cleanings. This means the tape will not be used unless you subsequently change Cleanings to another value. You can avoid this situation by carefully selecting the barcodes for your cleaning media.

▼ To specify maximum mounts

- ❖ Click an **arrow** and select a number for the volume as shown in the following table:

For	Select
Media other than cleaning tapes	The maximum number of mounts to allow.
Cleaning tapes	The number of cleanings to allow.

Media Type

This setting is used to select the media type for the barcode rule.

For a non-API robot, a barcode rule is not used unless the media type in the barcode rule is compatible with the media type you select on the **Media Settings** tab.

The media type specified on the **Media Settings** tab always overrides the media type of the barcode rule. If you specify any value other than `DEFAULT` on the **Media Settings** tab, the media type specified for the barcode rule must be the same (except for cleaning media) or be `DEFAULT` to obtain a match for the media type.

To enable barcode rule support for API robots you must add an `API_BARCODE_RULES` entry in the `vm.conf` file.

For an API robot, the media type is always set to `DEFAULT` on the **Media Settings** tab. A barcode rule is not used unless the media type specified in the barcode rule is compatible with the media type on the **Media Type Mappings** tab. See “Media Type Mappings Tab (Advanced Options)” on page 188 for more information.

See “Specifying Media Type (when using barcode rules)” on page 176 for more information, and examples showing combinations of **Media Settings** tab media types and barcode rule media types, and the results.

▼ **To specify a media type**

Click the **arrow** and select the media type.

Select the media type for non-API robots as explained in the following table:

If you want the media type for the barcode rule to match	Select the following media type for the barcode rule	Resulting media type that is used
Any media type that you select on the Media Settings tab	DEFAULT.	The media type that you select on the Media Settings tab. If you also select DEFAULT on the Media Settings tab, the Media Manager default media type for the robot is used.
Only when you select a specific media type or you select DEFAULT on the Media Settings tab	The same specific media type.	The media type that you select for the barcode rule.

Select the media type for API robots as explained in the following table. For API robots, you must add an `API_BARCODE_RULES` entry in the `vm.conf` file and the media type is always set to `DEFAULT` on the **Media Settings** tab.

Select the following media type for the barcode rule	Resulting media type that is used
DEFAULT.	Any media type you select in the Media Type Mappings tab. If this tab is not used, the Media Manager default media type for the robot is used.
A specific media type.	The media type that you select for the barcode rule.



Volume Pool

This property is used to select a volume pool for the volume. This is the pool that the volume will be placed in when a barcode matches the rule. Whenever the barcode rule is used and the **Media Settings** tab shows

- ◆ DEFAULT for the volume pool, then the volume is assigned to the pool you specified in the barcode rule.
- ◆ A specific volume pool, then that selection overrides the pool you specified in the barcode rule.

▼ To specify a volume pool

- ❖ Click the **arrow** and select a pool.

Description

Enter a description for the barcode rule. This could be a description of how the barcode rule will be used or any useful description determined by your site. You can enter from 1 to 25 characters.

Media ID Generation Tab (Advanced Options)

To use media ID generation rules, the robotic library must support barcodes and the robot cannot be an API robot.

Media ID generation rules allows you to override the default Media Manager media ID naming method. The default method uses the last six characters of the barcode label returned by the robot to generate the media ID. You can control how media IDs are created by defining Media ID generation rules that specify which characters of a barcode label will be used for the media ID.

The following topics explain how to use media ID generation rules:

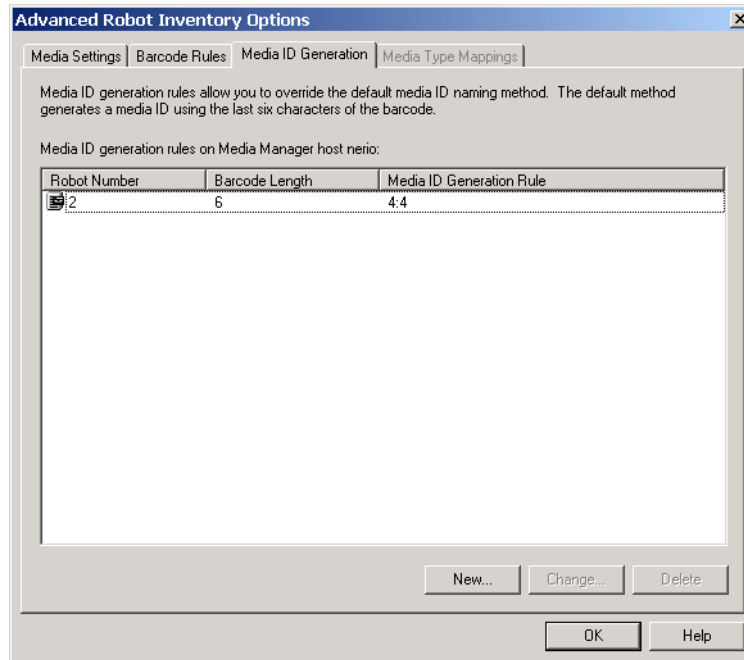
- ◆ “Adding a New Media ID Generation Rule” on page 185
- ◆ “Changing a Media ID Generation Rule” on page 186
- ◆ “Deleting a Media ID Generation Rule” on page 186
- ◆ “Dialog Properties for Adding or Changing Media ID Generation Rules” on page 186

For background information see “Media ID Generation Rules” on page 325.

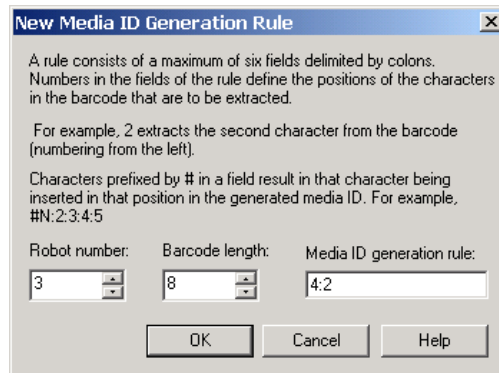
Adding a New Media ID Generation Rule

▼ To add a rule

1. In the Advanced Robot Inventory Options dialog, click **Media ID Generation**.



2. On the **Media ID Generation** tab, click **New ...**



3. Specify the properties for the new media ID generation rule. See “Dialog Properties for Adding or Changing Media ID Generation Rules” on page 186 for help on specifying rules.



4. When you are satisfied with your settings, click **OK** to return to the Robot Inventory dialog and proceed with the update.

Changing a Media ID Generation Rule

▼ To change a rule

1. In the Advanced Robot Inventory Options dialog, click **Media ID Generation**.
2. On the **Media ID Generation** tab, select a rule from list.
3. Click **Change ...**
4. In the dialog specify your changes for the rule. You cannot change the Robot Number or Barcode Length fields.
See “Dialog Properties for Adding or Changing Media ID Generation Rules” on page 186 for help in changing the rule.
5. When you are satisfied with your settings, click **OK** to return to the Robot Inventory dialog and proceed with the update.

Deleting a Media ID Generation Rule

▼ To delete a rule

1. In the Advanced Robot Inventory Options dialog, click **Media ID Generation**.
2. On the **Media ID Generation** tab, select a rule or rules from list.
3. Click **Delete**.
In the dialog, confirm or cancel the delete action.
4. When you are done, click **OK** to return to the Robot Inventory dialog and proceed with the update.

Dialog Properties for Adding or Changing Media ID Generation Rules

The following topics explain the settings you can make on this dialog.

Robot Number

▼ To specify a robot number

- ❖ Click an **arrow** and select a robot number where this rule will apply.

Barcode Length

▼ To specify a barcode length

- ❖ Click an **arrow** and select the length of the barcode for tapes in this robotic library and for this rule.

Media ID Generation Rule

▼ To specify a rule

- ❖ Enter a generation rule for media IDs.

A rule consists of a maximum of six fields that must be delimited by colons. Numbers in the fields of the rule define the positions of the characters in the barcode that are to be extracted. For example, 2 in a field extracts the second character from the barcode (the numbering is done from the left). The numbers can be specified in any order.

Characters prefixed by # in a field result in that character being inserted in that position in the generated ID. Any alphanumeric characters that are specified must be valid for a media ID.

The following table shows some examples of rules and the resulting media IDs. You can use rules to create media IDs of many varied formats, but remember that the difference in the label on the media and the generated media ID may make it difficult to keep track of your media.

Eight-character Tape Barcode	Media ID Generation Rule	Generated Media Manager Media ID
032945L1	1:2:3:4:5:6	032945
032945L1	3:4:5:6:7	2945L
032945L1	#N:2:3:4:5:6	N32945
543106L1	#9:2:3:4	9431



Eight-character Tape Barcode	Media ID Generation Rule	Generated Media Manager Media ID
543106L1	1:2:3:4:#P	5431P

Media Type Mappings Tab (Advanced Options)

This tab is available only for API robots. API robots are ACS, LMF, RSM, TLH, or TLM robot types on NetBackup Enterprise Server; and the RSM robot type on NetBackup Server.

For API robots, the Media type setting on the **Media Settings** tab is always set to DEFAULT (see “Media Type” on page 173). Media Manager uses the mappings on the **Media Type Mappings** tab to set the media type for new volumes for API robots.

The following topics explain how to use media type mappings:

- ◆ “How the Mapping Defaults Shown on the Tab are Determined” on page 188
- ◆ “Using the Tab to Change Media Type Mappings” on page 189
- ◆ “Adding Mapping Entries to vm.conf” on page 190
- ◆ “Default and Allowable Media Types for API Robots” on page 190

How the Mapping Defaults Shown on the Tab are Determined

Media Manager determines the default media types shown on the **Media Type Mappings** tab as follows:

1. The tab shows the default media types shown in the second column of the API robot tables (see “Default and Allowable Media Types for API Robots” on page 190).
2. In addition, the tab also shows any robot-specific media mappings you have added to the Media Manager configuration file (see “Adding Mapping Entries to vm.conf” on page 190).

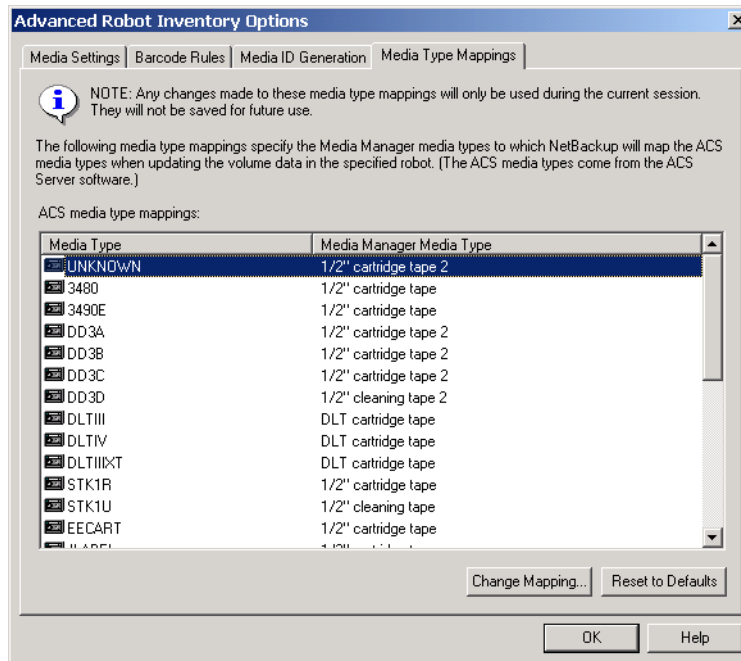
If the `vm.conf` file does not exist or it does not contain media mapping entries for that robot and media type, the tab shows only the default media types.

Using the Tab to Change Media Type Mappings

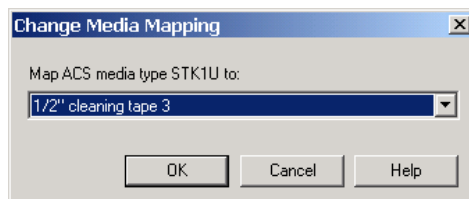
On the **Media Type Mappings** tab you can change the media types for a particular robot vendor (or operating system software in the case of RSM robots) that is shown, to one of the allowable Media Manager types for that robot vendor. Media Manager uses any mappings that you have set on this tab for this update. Your mapping changes apply only to the current volume configuration update.

▼ To change media type mappings

1. In the Advanced Robot Inventory Options dialog, click **Media Type Mappings**. The list that is presented on the tab contains mappings only for the robot type that has been selected for inventory.



2. Select the row that contains the robot-vendor media type mapping that you would like to change and click **Change Mapping**.



3. In the Change Media Mapping dialog, click the **arrow** and select a Media Manager type from the list of allowable choices.

Click **OK**.

To reset the **Media Type Mappings** tab to show the original default mappings, click **Reset to Defaults** (the defaults shown also include any robot-specific media mappings you have added to the Media Manager configuration file).

4. When you are satisfied with your mappings, click **OK** to return to the Robot Inventory dialog and proceed with the volume configuration update.

Adding Mapping Entries to `vm.conf`

If the default choices on the **Media Type Mappings** tab do not provide the desired mappings, you can change the default that appears in this tab by adding robot-specific media mappings (for example, `RSM_mediatype` entries for RSM robots) to the Media Manager configuration file (`vm.conf`) on the host where you are running NetBackup administration.

The following table shows some examples of robot-specific media mappings:

vm.conf Entry	Result	Default Without a vm.conf Entry
ACS_3490E = HCART2	Maps the ACS 3490E to the HCART2 media type.	Media Manager assigns HCART to ACS 3490E media types.
ACS_DLTIV = DLT2	Maps ACS DLTIV to the DLT2 media type.	Media Manager assigns DLT to all ACS DLT media types, including DLTIV.
RSM_UNKNOWN = 8MM	Maps the RSM unknown to the 8MM media type.	Media Manager assigns HCART to unknown media types.
TLH_3490E = HCART2	Maps the TLH 3490E to the HCART2 media type.	Media Manager assigns HCART to TLH 3490E media types.

See “The Media Manager Configuration File (`vm.conf`)” on page 355 for an overview of the configuration file.

Default and Allowable Media Types for API Robots

The following tables contain the default and allowable media types for the API robots. The second column of each table shows the default media type and the third column shows the allowable media types to which you can change the defaults, by creating map entries in the `vm.conf` file.



For example, the Allowable Media Types Through Mappings column of the third and fourth rows of the following table shows that for ACS robots you cannot specify either of the following map entries in the configuration file:

```
ACS_DD3A = DLT
ACS_DD3A = HCART4
```

Default and Allowable Media Types for ACS Robots

ACS Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
3480	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
3490E	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
DD3A	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
DD3B	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
DD3C	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
DD3D	1/2-inch cartridge cleaning tape 2 (HC2_CLN)	HC_CLN, HC2_CLN, HC3_CLN
DLTIII	Digital Linear Tape (DLT)	DLT, DLT2, DLT3
DLTIIIXT	Digital Linear Tape (DLT)	DLT, DLT2, DLT3
DLTIV	Digital Linear Tape (DLT)	DLT, DLT2, DLT3
STK1R	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
STK1U	1/2-inch cartridge cleaning tape (HC_CLN)	HC_CLN, HC2_CLN, HC3_CLN
EECART	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
JLABEL	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
STK2P	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
STK2W	1/2-inch cartridge cleaning tape 2 (HC2_CLN)	HC_CLN, HC2_CLN, HC3_CLN



Default and Allowable Media Types for ACS Robots (continued)

ACS Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
KLABEL	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_200G	1/2-inch cartridge (HCART2)	HCART, HCART2, HCART3
LTO_100G	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_50GB	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_35GB	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_10GB	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_CLN2	1/2-inch cartridge cleaning tape (HC_CLN)	HC_CLN, HC2_CLN, HC3_CLN
LTO_CLN3	1/2-inch cartridge cleaning tape (HC_CLN)	HC_CLN, HC2_CLN, HC3_CLN
LTO_CLN1	1/2-inch cartridge cleaning tape (HC_CLN)	HC_CLN, HC2_CLN, HC3_CLN
SDLT	Digital Linear Tape 3 (DLT3)	DLT, DLT2, DLT3
VIRTUAL	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3, HC_CLN, HC2_CLN, HC3_CLN, DLT, DLT2, DLT3, DLT_CLN, DLT2_CLN, DLT3_CLN
LTO_CLNU	1/2-inch cartridge cleaning tape (HC_CLN)	HC_CLN, HC2_CLN, HC3_CLN
UNKNOWN (for unknown ACS media types)	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3, HC_CLN, HC2_CLN, HC3_CLN, DLT, DLT2, DLT3, DLT_CLN, DLT2_CLN, DLT3_CLN



Default and Allowable Media Types for LMF Robots

LMF Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
18/36TRK	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
128TRK	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
UNKNOWN (for unknown LMF media types)	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3

Default and Allowable Media Types for RSM Robots

RSM Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
DDS_4MM	4mm cartridge (4MM)	4MM
MINI_QIC	1/4-inch cartridge (QCART)	QCART
TRAVAN	1/4-inch cartridge (QCART)	QCART
QIC	1/4-inch cartridge (QCART)	QCART
MP_8MM	8mm cartridge (8MM)	8MM, 8MM2, 8MM3
AME_8MM	8mm cartridge (8MM)	8MM, 8MM2, 8MM3
AIT1_8MM	8mm cartridge (8MM)	8MM, 8MM2, 8MM3
DLT	Digital Linear Tape (DLT)	DLT, DLT2, DLT3
IBM_MAGSTAR_3590	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
IBM_MAGSTAR_MP	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
STK_DATA_D3	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3



Default and Allowable Media Types for RSM Robots (continued)

RSM Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
CLEANER_CARTRIDGE	1/2-inch cartridge (HC_CLN)	HC_CLN, HC2_CLN, HC3_CLN, 4MM_CLN, 8MM_CLN, 8MM_CLN2, 8MM_CLN3, DLT_CLN, DLT2_CLN, DLT3_CLN
MP2_8MM	8mm cartridge (8MM)	8MM, 8MM2, 8MM3
UNKNOWN (for unknown RSM media types)	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3, 4MM, 8MM, 8MM2, 8MM3, QCART, DLT, DLT2, DLT3
STK_EAGLE	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_ULTRIUM	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
LTO_ACCELIS	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3

Default and Allowable Media Types for TLH Robots

TLH Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
3480	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
3490E	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
3590J	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
UNKNOWN (for unknown TLH media types)	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
3590K	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3

Default and Allowable Media Types for TLM Robots

TLM Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
3480	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
OD_THICK	NONE (OD_THICK is translated to media type REWR_OPT for robot contents reports. OD_THICK is ignored for all other robotic inventory operations)	NONE
DECDLT	Digital Linear Tape (DLT)	DLT, DLT2, DLT3
8MM	8mm cartridge (8MM)	8MM, 8MM2, 8MM3
4MM	4mm cartridge (4MM)	4MM
3590	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
DTF	DTF cartridge (DTF)	DTF
SONY_AIT	8mm cartridge (8MM)	8MM, 8MM2, 8MM3
LTO	1/2-inch cartridge (HCART)	HCART, HCART2, HCART3
UNKNOWN (for unknown TLM media types)	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3, DLT, DLT2, DLT3, 8MM, 8MM2, 8MM3

Note The following TLM media types are not supported: OD_THIN, D2, VHS, CD, TRAVAN, BETACAM, AUDIO_TAPE, BETACAMCL, DVCM, and DVCL.

Examples of Updating a Volume Configuration

The following examples show only the relevant dialog and volume attributes.



Example 1: Removing a Volume from a Robot

The following is an example of removing a volume from a robotic library. It does not matter whether the robot supports barcodes.

1. The following are the attributes for media ID 800001.

media ID	800001
media type	8MM cartridge tape
barcode	TL800001
media description	tl8 backup volume
volume pool	NetBackup
robot type	TL8 - Tape Library 8MM
volume group	EXB220
max mounts allowed	0 (unlimited)

2. Assume that you remove the volume from the robotic library, specify the following on the **Media Settings** tab, and then execute the update.

media type	DEFAULT
volume group	NONROB_8MM
volume pool	DEFAULT

3. The resulting volume attributes for media ID 800001 are as follows:

media ID	800001
media type	8MM cartridge tape
barcode	TL800001
media description	tl8 backup volume

volume pool	NetBackup
robot type	NONE - Not Robotic
volume group	NONROB_8MM
max mounts allowed	0 (unlimited)

The new residence information in the volume database shows a standalone location in the volume group, specified by the volume group on the **Media Settings** tab. The media type and volume pool remain unchanged.

The results are the same for a volume that does not have a barcode.

Example 2: Adding Existing Standalone Volumes to a Robot

The following is an example of adding a standalone volume, that has a barcode, to a robotic library that supports barcodes (TL8).

Note When moving volumes from robot to robot, you must do two separate updates, as explained in “Example 6: Moving Existing Volumes Between Robots” on page 204.



1. The following are the volume attributes for media ID 800021, which has a readable barcode and already exists as a standalone volume.

media ID	800021
media type	8MM cartridge tape
barcode	TL800021
media description	8MM standalone
volume pool	None
robot type	None (Standalone)
volume group	NONROB_8MM
max mounts allowed	0 (unlimited)

2. Assume that you insert the volume into a TL8 robot, specify the following on the **Media Settings** tab, and then execute the update.

media type	DEFAULT
volume group	EXB220
use barcode rules	YES (selected)
volume pool	NetBackup

The barcode rules shown in the following table exist:

Barcode Tag	Media Type	Volume Pool	Max Mounts/ Cleanings	Description
CLND	DLT_CLN	None	30	dlt cleaning
CLN8	8MM_CLN	None	20	8mm cleaning
TL8	8MM	NetBackup	0	tl8 backup
DLT	DLT	d_pool	200	dlt backup



Barcode Tag	Media Type	Volume Pool	Max Mounts/ Cleanings	Description
TS	8MM	None	0	8mm no pool
<NONE>	DEFAULT	None	0	no barcode
<DEFAULT>	DEFAULT	NetBackup	0	other barcodes

- Media Manager recognizes that the media ID exists and changes the volume database to reflect the new robotic location, rather than creating a new media ID. The resulting volume attributes for media ID 800021 are as follows:

media ID	800021
media type	8MM cartridge tape
barcode	TL800021
media description	8MM standalone
volume pool	NONE
robot type	TL8 - Tape Library 8MM
robot number	0
robot slot	1
robot host	shark
volume group	EXB220
max mounts allowed	0 (unlimited)

Because the barcode matches the barcode of an existing standalone volume in the configuration, the residence information in the volume database is updated to reflect the new robotic location. Since the volume is not new, barcode rules are ignored.

The only setting used on the **Media Settings** tab is the volume group for added or moved volumes. The media type setting was not used because this example was for a single existing volume that already had a media type.



Example 3: Moving Existing Volumes Within a Robot

The following is an example of moving a volume from one slot to another within the same robot. The robot supports barcodes and the volume has a readable barcode.

Caution For volumes moved within a robotic library, use Update volume configuration only if the robotic library supports barcodes and the volumes have readable barcodes. Otherwise, Media Manager is unable to properly recognize the move (see “When Not to Use Update Volume Configuration” on page 164 and “Example 7: Adding Existing Volumes when Barcodes are Not Used” on page 205).

1. The following are the attributes for media ID 800002, which currently resides in slot 1 of the robotic library.

media ID	800002
media type	8MM cartridge tape
barcode	TL800002
media description	tl8 backup
volume pool	NetBackup
robot type	TL8 - Tape Library 8MM
robot number	0
robot slot	1
robot host	shark
volume group	EXB220
max mounts allowed	0 (unlimited)

2. Assume that you move the volume to empty slot 10, specify the following on the **Media Settings** tab, and then execute the update.

media type	DEFAULT
volume group	EXB220



use barcode rules	NO (not selected)
volume pool	DEFAULT

3. The resulting volume attributes are:

media ID	800002
media type	8MM cartridge tape
barcode	TL800002
media description	tl8 backup
volume pool	NetBackup
robot type	TL8 - Tape Library 8MM
robot number	0
robot slot	10
robot host	shark
volume group	EXB220
max mounts allowed	0 (unlimited)

The updated volume attributes show the new slot number, but all other information is unchanged.

Example 4: Adding New Volumes to a Robot

The following is an example of adding new volumes with barcodes to a robot that supports barcodes. Assume the following:

- ◆ The new volume is an 8MM tape with a readable barcode of TL800002.
- ◆ There are no media generation rules defined.
- ◆ The drives in the robot all have a drive type of 8MM or there are no drives configured on the robot control host.



1. You specify the following on the **Media Settings** tab and execute the update.

media type	DEFAULT
volume group	EXB2220
use barcode rules	YES (selected)
volume pool	DEFAULT

The barcode rules shown in the following table exist:

Barcode Tag	Media Type	Volume Pool	Max Mounts/ Cleanings	Description
CLND	DLT_CLN	None	30	dlt cleaning
CLN8	8MM_CLN	None	20	8mm cleaning
TL8	8MM	NetBackup	0	tl8 backup
DLT	DLT	d_pool	200	dlt backup
TS	8MM	None	0	8mm no pool
<NONE>	DEFAULT	None	0	no barcode

2. The barcode on the media matches the barcode rule named TL8 and the resulting volume attributes for the new volume are as follows:

media ID	800002
media type	8MM cartridge tape
barcode	TL800002
media description	tl8 backup
volume pool	NetBackup
robot type	TL8 - Tape Library 8MM



robot number	0
robot slot	1
robot host	shark
volume group	EXB220
max mounts allowed	0 (unlimited)

The media ID is from the last six characters of the barcode since there are no media ID generation rules. The new residence information in the volume database, shows the robot host, robot type, robot number, slot, and host. The volume group is from the **Media Settings** tab. The volume pool and max mounts allowed are from the barcode rule.

If barcode rules (or barcodes) had not been used, the media description, volume pool, and max mounts allowed would be set to the following defaults:

- ◆ Media description: added by Media Manager
- ◆ Volume pool: NetBackup for data tapes or None for cleaning tapes
- ◆ Max mounts: 0 (unlimited)

Note If the robot does not support barcodes or the barcode is unreadable, you must specify a Media ID prefix (or DEFAULT) on the **Media Settings** tab or Media Manager will not add new media IDs.

Example 5: Adding Cleaning Tapes to a Robot

A special case exists when adding cleaning tapes. For example, assume you are doing an update for a TLD robot.

1. The tapes you inserted include regular tapes with barcodes ranging from DLT00000 to DLT00010 and a cleaning tape with a barcode of CLN001.

The barcode rules shown in the following table exist:

Barcode Tag	Media Type	Volume Pool	Max Mounts/ Cleanings	Description
CLN	DLT_CLN	None	30	dlt cleaning
DL	DLT	d_pool	200	dlt backup



Barcode Tag	Media Type	Volume Pool	Max Mounts/ Cleanings	Description
<NONE>	DEFAULT	None	0	no barcode

2. You specify the following on the **Media Settings** tab and then execute the update.

media type	DLT
volume group	STK7430
use barcode rules	YES (selected)

3. The barcodes on the regular tapes match the DL barcode rule and the media type of the DL barcode rule matches the Media type on the **Media Settings** tab. These tapes are added as DLT.

The cleaning tape matches the CLN barcode rule and Media Manager recognizes that DLT_CLN is the cleaning tape for DLT. The cleaning tape CLN001 is added as DLT_CLN type media along with the regular volumes.

This illustrates Media Manager's ability to add cleaning cartridges along with regular volumes when you use Update volume configuration.

If the volumes you insert include a cleaning tape, Media Manager adds the volumes correctly if the following are true:

- ◆ The Media type on the **Media Settings** tab is the regular media (DLT in this example).
- ◆ The barcode on the volume matches a barcode tag (CLN in this example).
- ◆ The media type for the barcode rule is the correct cleaning media (DLT_CLN in this example).

To add only cleaning media, specify the cleaning media type on the **Media Settings** tab and in the barcode rule (DLT_CLN in this example).

Example 6: Moving Existing Volumes Between Robots

When you move volumes from one robot to another and the volumes in both robots are in the same volume database, you must perform two separate updates.

These updates move the volumes to standalone, as an intermediate step, and then to the new robot. Otherwise, Media Manager is unable to update the entries and you receive an "Update request failed" error.

Caution This procedure assumes that robot 2 is able to read barcodes and the volume has readable barcodes. Otherwise, you will encounter the problem mentioned in “Example 7: Adding Existing Volumes when Barcodes are Not Used” on page 205.

1. Remove the volume from robot 1.
Insert the volume in robot 2.
2. Perform an Update volume configuration on robot 1.
This updates the volume attributes to show the volume as standalone.
3. Perform an Update volume configuration on robot 2.
This updates the configuration to show the volume in robot 2.

Example 7: Adding Existing Volumes when Barcodes are Not Used

Caution This example is *NOT* recommended and is included only to illustrate the undesirable results.

The following is an example of adding an existing standalone volume to a TL4 robot. A TL4 robot supports media inventory (detects media presence), but not barcodes.



1. The following are the attributes for media ID 400021, which already exists as a standalone volume.

media ID	400021
media type	4MM cartridge tape
barcode	-----
media description	4MM standalone
volume pool	None
robot type	NONE - Not Robotic
volume group	NONROB_4MM
max mounts allowed	0 (unlimited)

2. Assume that you insert the volume into the robot, specify the following on the **Media Settings** tab, and then execute the update.

media type	DEFAULT
volume group	00_000_TL4
media ID prefix	C4
volume pool	DEFAULT

3. The resulting volume attributes are:

media ID	C40000
media type	4MM cartridge tape
barcode	-----
media description	Added by Media Manager
volume pool	NetBackup

robot type	TL4 - Tape Library 4MM
robot number	0
robot slot	1
robot host	shark
volume group	00_000_TL4
max mounts allowed	0 (unlimited)

It is *important* to note that Media Manager assigned a new media ID to the volume (C40000). This undesired result occurs if you use Update volume configuration to add volumes that do not have readable barcodes or if the robot does not support barcodes. Without a barcode, Media Manager cannot identify the volume and assumes it is new. The media ID C40000 is generated from the media ID prefix specified on the **Media Settings** tab.

The old media ID (400021) remains in the configuration unchanged. The information for the new media ID (C40000) shows the robotic location, including the robot host, robot type, number, slot, and host. The volume group and volume pool are according to the **Media Settings** tab selections. The max mounts allowed is set to the default (0).

This is an example of a situation where the physical inventory utility should be used. See “Updating the Volume Configuration for Non-Barcoded Media” on page 165.

Rescanning and Updating Barcodes for a Robot

Use the **Rescan/Update Barcodes** command to check the barcodes attached to volumes in a robotic library, and update the Media Manager volume database to agree with the contents of the robotic library.

Note *The Rescan/Update Barcodes command does not apply to volumes in API robot types.*

“Robot Attributes” on page 279 lists the robots that support barcodes.

See the following topics:

- ◆ “When to Use Rescan/Update” on page 208
- ◆ “When Not to Use Rescan/Update” on page 208
- ◆ “Procedure To Rescan/Update Barcodes” on page 208



When to Use Rescan/Update

Use **Rescan/Update Barcodes** only to fill in barcodes that are missing from the Media Manager volume database.

For example, if you added a new volume to your configuration but did not physically insert the volume into the robotic library when the logical volume entry was added, the volume database will not include the barcode. In this case, you can use this command to fill in the missing barcode, provided that the media has since been physically inserted in the robotic library.

When Not to Use Rescan/Update

Do not use **Rescan/Update Barcodes** to correct reports that show a media ID in the wrong slot. In this case, you must do *one* of the following to correct the problem:

- ◆ Logically move the volume by selecting a volume and using **Actions > Move**.
- ◆ Logically move the volume using an Update volume configuration operation. See “Updating the Volume Configuration for a Robot” on page 162.
- ◆ Physically move the volume into the correct slot to agree with the volume database.

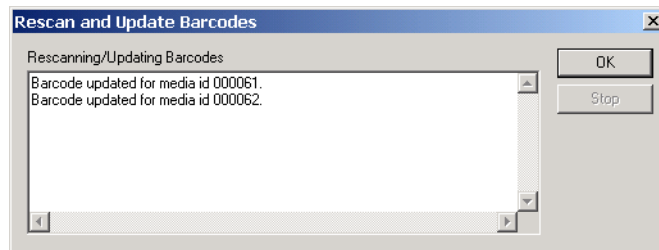
To obtain an inventory of the robotic library without updating the barcode information in the volume database, select **Show contents** in the Robot Inventory dialog. See “Showing the Contents of a Robot” on page 157 for more information.

Procedure To Rescan/Update Barcodes

▼ To check barcodes and update the volume database

1. In the NetBackup Administration Console, click **Media and Device Management > Media > Robots**.
2. Select the robotic library that has the volumes that you want to scan and update.
3. In the volume pane, select the volumes.
4. Click **Actions > Rescan/Update Barcodes**.

A dialog appears with the results of the update.



The Device Monitor provides menus and commands that are used to manage drives and operator service requests.

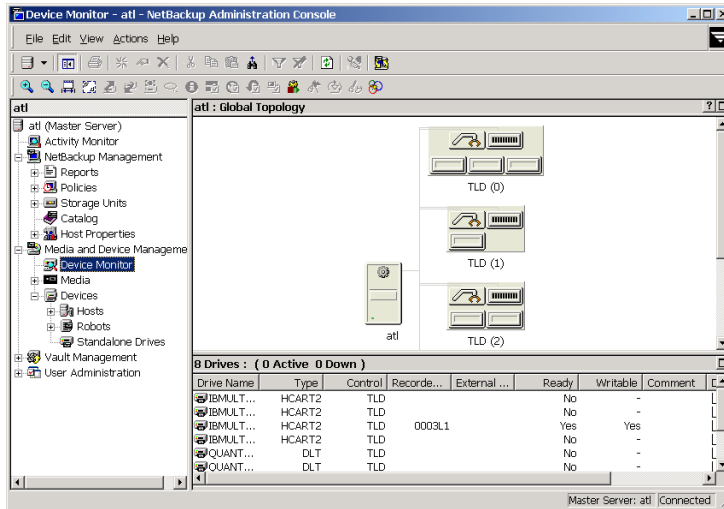
This chapter explains the Device Monitor interface and contains the following topics:

- ◆ “Starting the Device Monitor” on page 212
- ◆ “Using the Device Monitor Window” on page 212
- ◆ “Controlling the NetBackup Device Manager Service” on page 230
- ◆ “Monitoring Devices on Other Servers” on page 230
- ◆ “Changing the Operating Mode of a Drive” on page 232
- ◆ “Resetting a Drive” on page 233
- ◆ “Drive Cleaning Functions” on page 234
- ◆ “Adding or Changing a Drive Comment” on page 236
- ◆ “Handling Pending Requests and Pending Actions” on page 237
- ◆ “Resolving Pending Requests” on page 238
- ◆ “Resolving Pending Actions” on page 241
- ◆ “Resubmitting Requests” on page 242
- ◆ “Denying Requests” on page 243



Starting the Device Monitor

In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**. The Device Monitor window similar to the following appears.



In addition to the tree pane on the left, two panes are initially displayed on the right when you start the Device Monitor:

- ◆ A pane showing global device topology.
- ◆ A pane showing drive information.
- ◆ In addition, a third pane for pending requests (or pending actions) is displayed, if there is a pending request or pending action that is active.

Using the Device Monitor Window

The following topics provide an overview of the Device Monitor window:

- ◆ “Menus and Commands” on page 213
- ◆ “Toolbars” on page 216
- ◆ “Global Topology Pane” on page 217
- ◆ “Drives Status Pane” on page 220
- ◆ “Pending Requests Pane” on page 224
- ◆ “Status Bar” on page 227
- ◆ “Shortcut Menus and Commands” on page 227



- ◆ “Customizing the Window” on page 228
- ◆ “Allowable Media Manager Characters” on page 229

Menus and Commands

The Device Monitor window has available the menus and commands shown in the following table. Review the Note column for any restrictions.

The items on the menus are enabled based on what objects are currently selected in the topology, drive status, or pending requests panes. For example, if a drive is selected in the topology pane, **Up Drive** is enabled on the **Actions** menu.

Device Monitor Menus and Commands

Menu	Commands	Note
File	<p>Change Server - Displays a dialog that allows you to change to a different NetBackup media server (or SAN media server). See “Monitoring Devices on Other Servers” on page 230 for details</p> <p>New Console - Starts another instance of NetBackup Administration Console.</p> <p>New Window from Here - Starts another instance of the NetBackup Administration Console node that was active.</p> <p>Login as New User - Log into NetBackup as a different user without exiting NetBackup. This is useful if a NetBackup Administrator wants to log in again as the Security Administrator to administer Access Management. Controlling access to NetBackup is discussed in the NetBackup system administrator’s guide.</p> <p>Backup, Archive, and Restore - Starts the NetBackup backup, archive, and restore GUI.</p> <p>MS SQL Client - Shortcut to access the SQL server NetBackup client, if it is installed on the selected host.</p> <p>Print Setup - Displays a setup dialog for printing.</p> <p>Print Preview - Previews the print image.</p> <p>Print - Prints the topology, drive status, or pending requests pane (when one of these panes is selected).</p> <p>Close - Closes the current window.</p> <p>Exit - Closes all open windows.</p>	



Device Monitor Menus and Commands (continued)

Menu	Commands	Note
Edit	Undo - Allows you to cancel the last action. Cut, Copy, Paste - Commands for managing items in the display lists. Find, Find Next, Find Prev, Find All - Commands for finding items in the display lists.	
View	Contains commands for specifying your viewing preferences for the Device Monitor, including showing and hiding the toolbar or tree, using the topology window, and refreshing the display. See “Customizing the Window” on page 228.	
Actions	Up Drive - Sets the operating mode of the drive to up in automatic volume recognition (AVR) mode. This is the normal and default mode for drives. In AVR mode, a robotic library automatically retrieves, mounts, unmounts, and stores volumes. Manual intervention is necessary only when a request causes an error. For standalone drives using labeled volumes, when the volume is mounted and the tape drive is ready, Media Manager automatically reads the recorded media ID and assigns the tape drive. For standalone drives using unlabeled volumes, you assign tape drives to requests using Actions > Assign Request . Up Drive, Operator Control - Sets the operating mode of the drive to up in operator control mode (OPR). This mode is normally used only for security reasons. Do not use this mode for drives that are being used by NetBackup. This command appears on the menu only if it has been enabled. To enable this command, click View > Options > Device Monitor and select Allow Drive Up, Operator Controlled . By default, all operations in this mode are similar to AVR mode. If standalone drive extensions have been disabled, all operations are similar to AVR mode, except that labeled volumes are not automatically assigned to standalone drives. You must assign a standalone drive to a request using Actions > Assign Request . You can disable drive extensions by selecting Host Properties > Media Servers > Media . Down Drive - Sets the operating mode of the drive to the DOWN mode, so it is not available to Media Manager. In this mode, drives are not under control of Media Manager and cannot be assigned to requests. When changing the operating mode of drives in SSO configurations, also see “Changing the Operating Mode of a Drive” on page 232.	Applies only to NetBackup Enterprise Server.



Device Monitor Menus and Commands (continued)

Menu	Commands	Note
	<p>Reset Drive - Resets the specified drive, terminating the drive assignment and taking control away from the assigned user.</p> <p>For more information, see “Resetting a Drive” on page 233.</p> <p>Drive Cleaning - Displays a sub-menu with choices for performing drive cleaning functions.</p> <p>Change Drive Comment - Displays a dialog for changing the comment for the selected drive.</p> <p>For SSO configurations also see “Adding or Changing a Drive Comment” on page 236.</p>	Applies only to NetBackup Enterprise Server.
	<p>Drive Details - Displays a dialog with information about the selected drive, including drive properties, drive status, and robotic library information.</p> <p>Assign Request - Assigns a drive to a pending request.</p> <p>Deny Request - Denies a pending request.</p> <p>Resubmit Request - Resubmits a pending request.</p> <p>Display Pending Action - Displays information about the pending action.</p> <p>Stop/Restart Device Manager Service - Controls the Media Manager device service.</p> <p>View SAN Point Control - Launches VERITAS SANPoint Control. This web-based application helps you locate the cause of problems on your SAN or direct fibre-channel attached storage.</p> <p>See “Using SANPoint Control to Investigate SAN Problems” on page 77.</p>	



Device Monitor Menus and Commands (continued)

Menu	Commands	Note
Help	Help Topics - Provides online help information for the NetBackup Console. Troubleshooter - Helps you to debug errors. VERITAS Web Page - Displays the VERITAS web page, if the host has a browser configured. License Keys - Provides information about your active and registered license keys. About Administration Console - Displays program information, version number, and copyright information. You can click More for detailed information. Current NBAC User - Provides NetBackup Access Control information for the current user. Gives the permissions for the user that you are currently logged in as.	

Toolbars

The toolbar buttons of the Device Monitor window provide shortcuts for commands that are on the menus. Also see “Customizing the Window” on page 228.

▼ To show or hide the toolbar buttons

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. Click **View > Toolbar**.

▼ To customize the toolbar buttons

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. Click **View > Customize...**

In the **Customize Toolbar** dialog you can reorder the buttons on the current toolbar, add buttons, or remove toolbar buttons. Use **Default** to reset the buttons on the toolbar.

Global Topology Pane

The Device Monitor topology view shows the state of all devices in the global database. This view is different from the NetBackup activity monitor topology in that it is a device-centric view.

A description bar is displayed at the top of this pane. Tool tips are also provided for all of the objects displayed in the topology pane.

Your view and use of the topology pane can be customized. See “Customizing the Window” on page 228 (many of these commands are also available using the right mouse button in the topology pane).

Device hosts that are shown cannot be filtered by modifying the Media Manager `vm.conf` file. The topology information that is displayed is taken from the Media Manager global device database.

The following point applies to NetBackup Enterprise Server.

The topology view may also show multiple NetBackup servers that are sharing the same devices (shared drives).

▼ To customize your view and use of the topology pane

- ❖ See “Customizing the Window” on page 228 (many of these commands are also available using the right mouse button in the topology pane).

Also see the following topics:

- ◆ “Topology Images” on page 217
- ◆ “Topology Connections” on page 219
- ◆ “Selecting Topology Objects” on page 219

Topology Images

The following are some of the images that can appear in the topology pane.

Description

Topology Image

NetBackup master server



NetBackup media server (or SAN
media server)



Robot



Volume database (robot media)



Drive









Drive that is shared










There are also a number of state indicators for drives.

The following point applies to NetBackup Enterprise Server.

The images for shared drives are similar, with the shared drive images having a hand at the bottom of the image.

Drive State Indicator	Drive	Shared Drive
Empty		
Tape loaded		
Down		

Drive State Indicator	Drive	Shared Drive
Reading		
Writing		
Active (reading or writing)		
The control mode for a shared drive is not the same on all hosts sharing the drive.	Not applicable.	

Topology Connections

Connections in the topology indicate physical and logical connections of the devices, as follows:

- ◆ Master server and media server (or SAN media server) relationships are indicated and each has a different icon. Robots and drives are connected to a media server.
- ◆ Drives that are physically located in a robotic library are shown directly below the robotic library. Standalone drives are represented as individual drive objects.
- ◆ Drive to device host connections are shown only if the drive is being used for a request and the drive is in use by NetBackup. Robot to server connections and robotic library to volume database connections are always shown.
- ◆ Media is represented as located in a robotic library.
- ◆ The topology also indicates a connection to a volume database host.

Selecting Topology Objects

If you use the **Show only items in list selected in topology** option (see “Customizing the Window” on page 228) and select objects in the topology pane you can filter the contents of the lists in the Drives status pane. This action also highlights the connection lines in the topology.

If you do not use the **Show only items in list selected in topology** option and select an object, the object is highlighted in the other panes.



Multiple objects of the same type can be selected by pressing the Ctrl key and selecting another object. If the Ctrl key is used and an object of a different type is selected, the selection is allowed and the other objects will not be selected. If the Ctrl key is not used and an object is selected, the previous selection will be unselected.

Drives Status Pane

This pane shows the status of the drives that Media Manager controls on this server. Information in the drive status pane is taken from the Media Manager global device database. The following table describes the columns displayed in this pane. Review the Note column for any restrictions.

Also see “Managing the Drives Status Pane” on page 224.

Drives Status Pane

Column	Description	Note
Drive Name	Drive name assigned to the drive during configuration.	
Control	Control mode for the drive can be any of the following: <i>robot_designation</i> . For example, TLD. The robotic daemon managing the drive has connected to ltid (the device daemon and Device Manager service) and is running. The drive is in the usable state. AVR is assumed to be active for the drive, as all robotic drives must be in AVR mode (not OPR mode). DOWN- <i>robot_designation</i> . For example, DOWN-TLD. The drive is in an usable state because it was downed by an operator or by NetBackup; or when the drive was configured, it was added as a down drive. DOWN. In this mode, the drive is not available to Media Manager. A drive can be in a DOWN mode because of problems or because it was set to that mode using Actions > Down Drive . PEND- <i>robot_designation</i> . For example, PEND-TLD.	Applies only to robotic drives. Applies only to robotic drives. Applies only to standalone drives. Applies only to robotic drives.



Drives Status Pane

Column	Description	Note
	<p>PEND.</p> <p>If the drive reports a SCSI RESERVATION CONFLICT status, this column will show PEND. This status means that the drive is reserved when it should not be reserved.</p> <p>Some server operating systems (Windows, Tru64, and HP-UX) may report PEND if the drive reports Busy when opened. You can use the AVR_D_PEND_DELAY entry in the Media Manager configuration file to filter out these reports.</p>	<p>Applies only to standalone drives.</p>
	<p>AVR.</p> <p>The drive is in a usable state with automatic volume recognition enabled, but the robotic daemon managing the drive is not connected or is not working. Automated media mounts do not occur with a drive in this state (unless the media is in a drive on the system), but the operator can physically mount a tape in the drive or use robtest to cause a tape mount as needed.</p>	<p>Applies only to robotic drives.</p>
	<p>AVR.</p> <p>The drive is running with automatic volume recognition enabled.</p>	<p>Applies only to standalone drives.</p>
	<p>OPR.</p> <p>The drive is running in a secure mode where operators must manually assign mount requests to the drive. avrd is not scanning this drive when in this mode. This mode gives operators control over which mount requests can be satisfied.</p>	<p>Applies only to standalone drives.</p>
	<p>NO-SCAN.</p> <p>A drive is configured for SSO, but has no available scan host (to be considered available, a host must register with a SSO_SCAN_ABILITY factor of non-zero and have the drive in the UP state).</p> <p>NO-SCAN may be caused if all available scan hosts have the drive in the DOWN state. Other hosts (that are not scan hosts) may want to use the drive, but they registered with a scan factor of zero. The drive is unusable by NetBackup until a scan host can be assigned.</p> <p>Use Actions > Drive Details to view the drive control mode for each host that is sharing this drive.</p>	<p>Applies only to NetBackup Enterprise Server.</p>



Drives Status Pane

Column	Description	Note
	<p><Mixed>.</p> <p>The control mode for a shared drive may not be the same on all hosts sharing the drive. For shared drives each host can have a different status for the drive. If the control modes <i>are</i> all the same, that mode is displayed.</p> <p>Use Actions > Drive Details to view the drive control mode for each host that is sharing this drive.</p>	Applies only to NetBackup Enterprise Server.
Drive Index	<p>Drive index assigned to the drive during configuration.</p> <p>This column contains <Shared> for shared drives. Use Actions > Drive Details to view the drive index for each host that is sharing this drive.</p>	Applies only to NetBackup Enterprise Server.
Host Name	<p>The name of the device host that has the drive.</p> <p>This column contains <Shared> for shared drives. Use Actions > Drive Details to view a list of hosts that are sharing this drive.</p>	Applies only to NetBackup Enterprise Server.
Type	<p>Drive type. Use the contents of this column to find a drive that supports the density required by a request. The valid drive types are as follows:</p> <p>4MM (4mm cartridge)</p> <p>8MM (8mm cartridge)</p> <p>8MM2 (8mm cartridge 2)</p> <p>8MM3 (8mm cartridge 3)</p> <p>DLT (DLT cartridge)</p> <p>DLT2 (DLT cartridge 2)</p> <p>DLT3 (DLT cartridge 3)</p> <p>DTF (DTF cartridge)</p> <p>HCART (1/2-inch cartridge)</p> <p>HCART2 (1/2-inch cartridge 2)</p> <p>HCART3 (1/2-inch cartridge 3)</p> <p>ODISK (optical disk)</p> <p>QSCSI (1/4-inch cartridge)</p>	

Drives Status Pane

Column	Description	Note
Shared	Yes, means this drive is configured as a shared drive. No, means the drive is not a shared drive.	Applies only to NetBackup Enterprise Server.
Assigned Host	This column shows the device host that currently has the drive assigned. If the selected drive is not assigned, this column is blank.	
User	User ID of the person or application whose request is currently assigned to this drive. If the selected drive is not assigned, this column is blank.	
Media Label	Shows whether a labeled or unlabeled volume is mounted on this drive. Yes, means labeled. No, means unlabeled. Labeled volumes can also be Backup Exec volumes. A dash (-) in this column means there is no volume mounted on the drive.	
Recorded Media ID	ID recorded on the volume mounted on this drive. This identifier is the same as the media ID and should match the external media ID. If no volume or a Backup Exec volume is mounted, this column is blank.	
External Media ID	External ID of the volume mounted on this drive. This identifier should match the recorded media ID. If no volume is mounted, this column is blank.	
Ready	Status of the drive, indicating if it is ready to perform an operation on the loaded volume. Yes, means ready. No, means not ready. See the vendor's manual for the drive for instructions to make it ready, if the drive does not become ready automatically.	
Writable	Shows whether the volume currently mounted on this drive is write-enabled. Yes, in this column means the volume is write-enabled. No, means the volume is write-protected. A dash (-) in this column means there is no volume in the drive.	



Drives Status Pane

Column	Description	Note
Drive Use History	Shows a graph of relative drive usage. The data for the graph is obtained from the Windows performance monitor. The graph is shown only if the following are true: <ul style="list-style-type: none">• The drive is connected to a Windows media server (or SAN media server).• A NetBackup job is active (the drive is in use).• The user has permissions to read the Windows registry.• Performance data collection is enabled (select Host Properties > Media Servers > Universal Settings).	
Drive Index	Drive index assigned to the drive during configuration. This column contains <Shared> for shared drives. Use Actions > Drive Details to view the drive index for each host that is sharing this drive.	Applies only to NetBackup Enterprise Server.
Request ID	If this drive is assigned to a request, this column contains the ID of the request.	
Comment	Comments that have been added for this drive. See “Adding or Changing a Drive Comment” on page 236.	

Managing the Drives Status Pane

The **Edit** menu has commands for finding items and is useful if you are managing many devices. You can also use **View > Columns > Layout** to rearrange or hide specific columns in this display. Some of the columns are hidden initially by default.

Pending Requests Pane

This pane shows pending requests (or pending actions) for volumes. These usually originate from NetBackup, but can come from a user or VERITAS Storage Migrator.

This pane is not normally displayed until a pending request or pending action appears. After all requests have been resolved by Media Manager (automatically) or by operator intervention, the Pending Requests pane is again hidden from view. See “Handling Pending Requests and Pending Actions” on page 237 for more information.

Also see “Managing the Pending Requests Pane” on page 227.

The following table describes the columns that are displayed in this pane for a pending request or action.

Pending Requests Pane

Column	Description
Request ID	Identification number for the request or action. This is a system-assigned number that identifies the request. Note A pending action is indicated by an asterisk to the left of the request ID. Note
Host Name	The name of the device host that has the pending request.
User	User ID of the person or application making the request.
Recorded Media ID	Media ID of the volume that is detected when the recorded media label was read. It should match the media ID that is in the volume database. The ID consists of up to six alphanumeric characters that are recorded at the beginning of the volume to identify the volume. A volume with a recorded media ID is a labeled volume. Unlabeled volumes do not have recorded media IDs. The recorded and external media IDs should be the same.
External Media ID	External media ID of the volume requested by the user. This ID consists of up to six alphanumeric characters and is usually written on an external label attached to the volume. The external media ID is used to identify the volume.



Pending Requests Pane

Column	Description
Density	<p>Density of the volume required by the user. You must mount the volume on a drive that supports the required density. dlt is the default density.</p> <p>The following is the list of valid densities. To find a drive of the correct type, view the Type column in the drive status list.</p> <p>4mm (4mm cartridge tape)</p> <p>8mm (8mm cartridge tape)</p> <p>8mm2 (8mm cartridge tape 2)</p> <p>8mm3 (8mm cartridge tape 3)</p> <p>dlt (DLT cartridge tape)</p> <p>dlt2 (DLT cartridge tape 2)</p> <p>dlt3 (DLT cartridge tape 3)</p> <p>dtf (DTF cartridge)</p> <p>hcart (1/2-inch cartridge tape)</p> <p>hcart2 (1/2-inch cartridge tape 2)</p> <p>hcart3 (1/2-inch cartridge tape 3)</p> <p>odiskwm (optical disk-write many)</p> <p>odiskwo (optical disk-write once)</p> <p>qscsi (1/4-inch cartridge tape)</p>
Mode	<p>Specifies whether the volume should be write-enabled. W in this column means you must write-enable the volume. R in this column means you do not have to write-enable the volume, unless specified by site policy. To write-enable a cartridge volume, move the tab off the safe position.</p>
Time	<p>Time of day the user made the request for access.</p>
Barcode	<p>Alphanumeric representation of the barcode label on the volume that was requested by the user.</p>
Volume Group	<p>Volume group to which this volume belongs. A volume group defines the volume by location and is a logical group of volumes that are at the same physical location.</p>
Media Description	<p>Describes the media in 25 or less alphanumeric characters. You create the description when you configure volumes.</p>

Managing the Pending Requests Pane

The **Edit** menu has commands for finding items and is useful if you are managing many devices. You can use **View > Columns > Layout** to rearrange or hide specific columns in this display. Many of the columns are hidden by default.

Status Bar

The status bar appears at the bottom of the NetBackup Console window. The status bar provides the following:

- ◆ Shows tool tips (when the mouse is over a toolbar icon or an object).
- ◆ Indicates the name of the media server.
- ◆ Indicates if you are connected to the device host you are trying to monitor.

▼ To show or hide the status bar

- ❖ Click **View > Status Bar**.

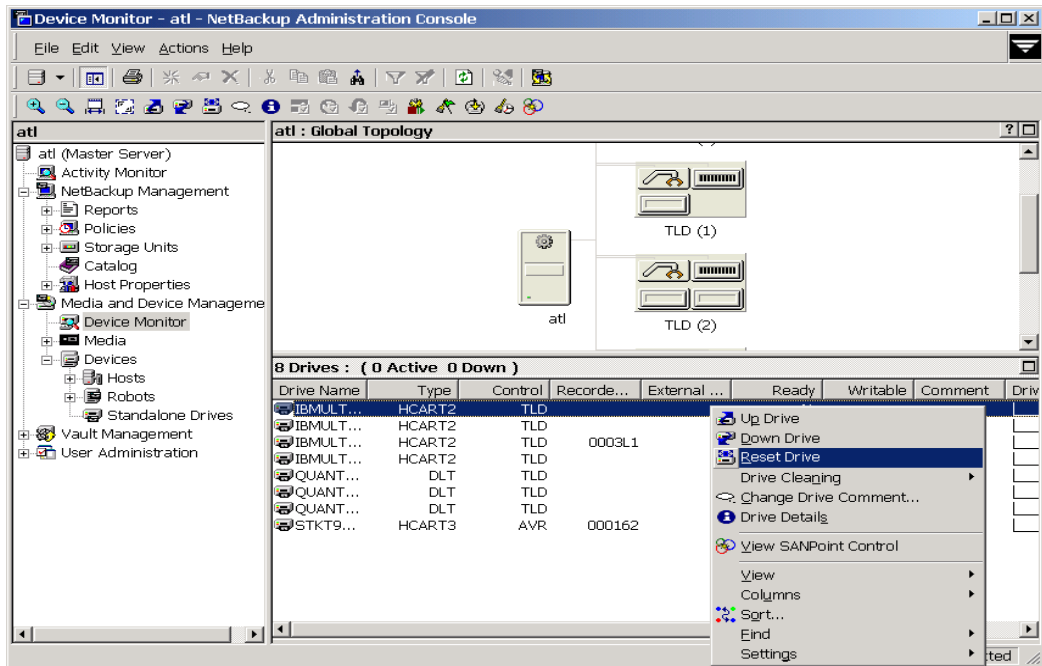
Shortcut Menus and Commands

Clicking the right mouse button while the pointer is over a pane or a selection in a pane, displays a shortcut menu with commands that apply to that context. These shortcut commands are also available on the menus or tool bars.

Help for the topology pane is available using the right mouse button in the topology pane (select **Topology Info**).



Short Cut Menu



Customizing the Window

The **View** menu has options for sorting and changing the layout and appearance of the panes of the Device Monitor window.

- ▼ **To show or hide columns, or rearrange the columns**
 - ❖ Click **View > Columns > Layout**
- ▼ **To fit the topology diagram to the pane and ignore the default startup size**
 1. Click **View > Options > Device Monitor**.
 2. Select **Fit topology to window on startup**.

- ▼ **To filter the Drives status pane to show drives based on selections in the topology diagram**
 1. Click **View > Options > Device Monitor**.
 2. Select **Show only items in list selected in topology**.
- ▼ **To enlarge the topology diagrams (this can be done multiple times)**
 - ❖ Click **View > Zoom > Zoom In**.
- ▼ **To decrease the size of the topology diagrams (this can be done multiple times)**
 - ❖ Click **View > Zoom > Zoom Out**.
- ▼ **To select objects and focus on a portion of the topology diagram**
 1. Click **View > Zoom > Overview Window**.

A copy of the topology diagram appears in a secondary window.
 2. Use the mouse to select desired objects or portions of objects in the configuration. The selected objects will be the focus of the main topology pane, allowing you to focus on areas of the topology diagram.
- ▼ **To size the topology diagram to the size of the current pane**
 - ❖ Click **View > Zoom > Fit to Window**.
- ▼ **To change the screen display refresh rate**

The refresh rate specifies how often the Device Monitor will query device hosts for new drive status information.

 1. Click **View > Options. > Device Monitor**.
 2. Set the desired refresh rate.

Allowable Media Manager Characters

The following set of characters can be used in user-defined names, such as drive comments and drive names that you enter when creating these entities. These characters must be used even when specifying these items in foreign languages.



Do not use a minus as the first character. Spaces are only allowed in a comment for a drive.

- ◆ Alphabetic (A-Z a-z)
- ◆ Numeric (0-9)
- ◆ Period (.)
- ◆ Plus (+)
- ◆ Minus (-)
- ◆ Underscore (_)

Controlling the NetBackup Device Manager Service

The NetBackup Device Manager service must be running on the host being monitored or the lists in the Device Monitor detail panes will be blank.

▼ To manage this service

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. Click **Actions > Stop/Restart Device Manager Service**.
3. *The following step applies only to NetBackup Enterprise Server.*
Select a device host. The dialog also shows the current status of this service.
4. The dialog allows you to start, stop, or stop/restart the service on the host. Select the action you want to perform.
5. Click **OK** or **Apply**.
You may find it useful to select **Stop** and click **Apply**, and then select **Start** and click **Apply**.

Monitoring Devices on Other Servers

Initially, you can monitor devices on the server where you are running the Device Monitor. The name of this server and its connection status is shown in the status bar (on the lower right side) of the window, for example Master Server: spain Connected.

You can also change from the current server to a different master or media server. If you change from a NetBackup Enterprise Server to a NetBackup Server, the functionality available on the new server is limited to the functionality supported by NetBackup Server.

If you change from a NetBackup Server to a NetBackup Enterprise Server, complete functionality is available on the new server.

▼ **To change to a different master or media server**

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.

2. Click **File > Change Server**.

(You can also click the **arrow** to the right of the **Change Server** icon on the toolbar and select one of the servers shown in the list.)

3. In the dialog that appears, do one of the following to specify the server that you want to monitor.

- ◆ Enter the name of the server.
- ◆ Select a server from the servers shown in the list.
- ◆ Click **Browse** and select a server.
- ◆ Login to the current server using a different user name.
- ◆ Login to a different server using a different user name.

You can also click **Remove** to delete a server from the list.

4. Click **OK**.

The name of the new server appears and the panes in the Device Monitor window change to show device information for the new device host. This information is taken from the global device database for the new server.

The NetBackup Device Manager service must be running on the server that you are going to monitor, or the lists in the detail panes will be blank. If it is not running when you attempt to connect, a message box prompts you to start the service. Click **OK** in this box.

In addition to using **File > Change Server** to monitor devices on other servers, you can use **File > Login as New User**. See “Menus and Commands” on page 213.



Changing the Operating Mode of a Drive

It is usually not necessary to change the operating mode of a drive. Drives are set to the UP in AVR mode (the default mode) when you add drives to your configuration, and usually can be left at that setting. Other operating mode settings are used for special purposes.

For RSM robots, Media Manager does not scan the RSM library to update the status for devices. Therefore any physical device status changes done in the Microsoft RSM application should also be updated in the Device Monitor.

For example, if drive 2 is down in the RSM library, you must deactivate the drive in both the RSM application *and* Device Monitor. However if drive 2 is functional but you do not want NetBackup to assign it, then only the RSM application interface need be updated.

See the **Actions** menu in “Menus and Commands” on page 213 for an explanation of the operating mode commands.

▼ To change the mode of a drive

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Drives status pane, select a drive or drives.
3. From the **Actions** menu, choose the command for the new operating mode you want (**Up Drive**, **Down Drive**, or **Up Drive, Operator control**).
4. *This step applies only to NetBackup Enterprise Server.*


If the drive is a shared drive (SSO option), the dialog contains a list of the hosts that are sharing the selected drive. You can choose any number of hosts where the mode change will apply.

Changing Mode Example

This example shows the results of changing the operating mode of a drive from AVR to DOWN. See the table in “Drives Status Pane” on page 220 for an explanation of the columns in the drive status display.

Note Some columns of the drive status list are not shown in this example.

The following display shows the Drives status pane *before* changing the drive mode. Notice that the Control column contains AVR and the Ready column contains Yes.

Drive Name	Type	Control	Recorded Media ID	External Media ID	Ready	Writable	Request ID
 STK9840A-FC-1	HCART	AVR	000084	000084	Yes	Yes	0

The following display shows the Drives status pane *after* using **Actions > Down Drive** to change the operating mode of the drive to DOWN. Notice that the Control column contains DOWN and the Ready column now contains No.

Drive Name	Type	Control	Recorded Media ID	External Media ID	Ready	Writable	Request ID
 STK9840A-FC-1	HCART	DOWN			No	-	-

Resetting a Drive

Caution Do not reset an assigned drive unless directed by site policy or the system administrator. Terminating an active job can destroy user data.

Resetting a drive changes the state of the drive. The actions that result from resetting a drive depend on the original state of the drive as follows:

Original Drive State	Reset Action
DOWN	Media Manager attempts to unload the drive. This occurs for standalone drives, as well as drives in a robot.
UP state, not assigned to a user or application, and in a ready state	Media Manager attempts to unload the drive. If the drive is not ready, no action occurs.
UP state and assigned to a user or application	Media Manager removes the tape. This takes control away from the user.

Use the reset capability with caution. A situation where resetting a drive might be necessary is if a system problem causes the drive to remain assigned after a job is complete. In this case, the drive cannot be used for another request and the only way to regain control of the drive is to reset it.

Note Resetting a drive does not perform any SCSI bus or SCSI device resets.



▼ To reset a drive

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Drives status pane, select a drive or drives.
3. Click **Actions > Reset Drive**.
4. Verify that the assignment was terminated by checking that the User and Request ID columns are blank for the drive number you selected.

Drive Cleaning Functions

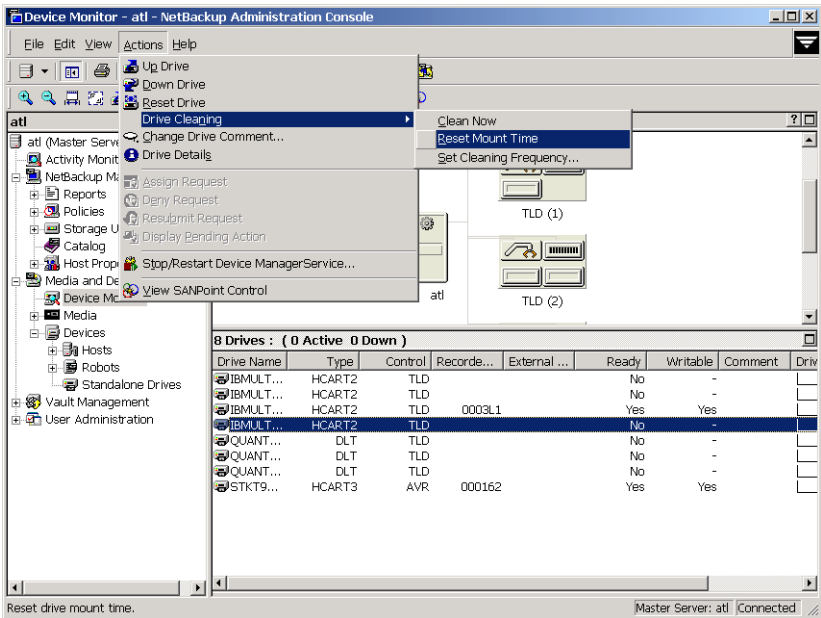
See “Drive Cleaning” on page 309 for background information on types of drive cleaning and cleaning tapes.

Note You can also perform drive cleaning functions from the Devices node. If you are managing the cleaning frequency from the Devices node, `ltid` must be stopped and restarted for any changes to take effect. This action also stops and restarts any robotic processes. For the functions available from the Devices node, see “Drive Cleaning Functions” on page 73.

▼ To perform drive cleaning functions

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Drives status pane, select a drive.

3. Select Actions > Drive Cleaning.



The sub-menu choices allow you to perform the following functions:

Select	To	Note
Clean Now	Start an operator-initiated cleaning of the selected drive, regardless of the cleaning frequency or accumulated mount time. If the drive is a standalone drive, it must contain a cleaning tape and a mount request will be issued. Clean Now resets the mount time to zero, but the cleaning frequency value remains the same.	
	For a shared drive (SSO option), the dialog contains a list of the hosts that are sharing the selected drive. You can choose only one host where Clean Now will apply.	Applies only to NetBackup Enterprise Server.
Reset Mount Time	Reset the mount time for the selected drive to zero. Use Reset Mount Time to reset the mount time after doing a manual cleaning of a drive.	



Select	To	Note
	For a shared drive (SSO option), the dialog contains a list of the hosts that are sharing the selected drive. You can choose any number of hosts where Reset Mount Time will apply.	Applies only to NetBackup Enterprise Server.
Set Cleaning Frequency	Set the desired number of mount hours between each drive cleaning. Set Cleaning Frequency is not available for robots that do not support frequency-based cleaning. Set Cleaning Frequency is not available for a shared drive (SSO option).	Applies to NetBackup Enterprise Server

4. Updated drive cleaning information is presented in the Drive Details dialog.

Note The **Clean Now** function may take several minutes to complete, so the cleaning information in the Drive Details dialog may not be updated immediately.

Adding or Changing a Drive Comment

▼ **To change a drive comment**

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Drives status pane, select the drive.
3. Click **Actions > Change Drive Comment**.
The dialog shows the current comment (if any).
4. *This step applies only to NetBackup Enterprise Server.*
If the drive is a shared drive (SSO option), the dialog contains a list of hosts that are sharing the selected drive and the current drive comment for each host. You can choose the hosts where a drive comment will apply.
5. Enter a comment or change the comment.



6. Click OK.

Handling Pending Requests and Pending Actions

In normal operating situations, NetBackup is able to resolve most requests automatically and quickly. For example if the requested volume is labeled and in a robotic library, Media Manager resolves the request as soon as the volume and a drive are available; and then removes the request and also the Pending Requests pane. In these normal cases, the pending request may not even be apparent to the operator.

The following special situations can occur:

- ◆ NetBackup needs a volume to complete a tape mount. NetBackup then displays a pending request in the Pending Requests pane.
See “Pending Requests” on page 237.
- ◆ NetBackup needs a volume to complete a tape mount and encounters problems. NetBackup then displays a pending action in the Pending Requests pane.
See “Pending Actions” on page 238.

Pending Requests

NetBackup sometimes needs operator assistance to complete a tape mount request for standalone drives or for drives in a robot that are not working (indicated by AVR in the Control column of the drive status pane).

In these cases, NetBackup is unable to automatically complete the request and is not certain what is causing the issue, since there may be multiple valid explanations for the problem.


The request remains in the Pending Requests pane until resolved. In any of the following cases, proceed as explained in “Resolving Pending Requests” on page 238.

- ◆ The required drive is up and is in operator control mode (OPR mode) and standalone drive extensions were disabled by using a `DISABLE_STANDALONE_DRIVE_EXTENSIONS` entry in the `bp.conf` file on UNIX servers or in the registry on Windows servers.
- ◆ The volume in a drive is unlabeled (and the volume being mounted is not known to be a Backup Exec volume that you are managing).
- ◆ NetBackup issues a write request for an unlabeled volume in a standalone drive and the standalone drive extensions were disabled.

The following figure shows a typical pending request.



Note Some columns of the pending requests pane are not shown in this figure.

horseradish : 1 Pending Request.									
Request ID	Recorded Media ID	External Media ID	User	Density	Mode	Time	Barcode	Volume Group	
 0	000084	000084	root	hcart	R	2/4/2003 3:49:32 PM	-----	---	

See the table in “Pending Requests Pane” on page 224 for an explanation of the columns in a pending request display.


Pending Actions

Media Manager also needs operator assistance to complete a tape mount request if the mount request encounters an error. These types of pending requests are known as pending actions and usually occur with drives in robotic libraries.

A pending action is similar to a pending request and is identified by an asterisk to the left of the request ID.

In these cases, NetBackup is certain what can be causing the issue and can issue instructions to the operator needed to resolve the action. Pending actions must be resolved before proceeding. See “Resolving Pending Actions” on page 241.

Note The following figure shows a typical pending action on a Windows server. Some columns of the pending requests pane are not shown in this example.

ainew2k : 1 Pending Request.									
Request ID	Recorded Media ID	External Media ID	User	Density	Mode	Time	Barcode	Volume Group	
 *0	000062	000062	NetBackup	hcart	R	2/5/2003 1:01:23 PM	000062	00_000_TLD	

See the table in “Pending Requests Pane” on page 224 for an explanation of the columns in a pending action (or pending request) display.

Resolving Pending Requests

Note *This note applies only to NetBackup Enterprise Server.*
You can also assign drives to a request by using the mouse to select and drag and drop items between the drive status and pending requests panes. This mouse action is valid only when the drive and request are on the same host.

▼ To assign a drive to a pending request

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Pending Requests pane, select the request. Also, note the contents of the following columns of the request:

Check this Column	To Determine
Density	The recording density that is required.
External Media ID	The ID of the media that is required.
Mode	Whether the volume should be write-enabled.

3. In the Drives status pane do the following:
 - a. Find a drive type that matches the density for the pending request.
See the table in “Pending Requests Pane” on page 224 for a list of the densities that each drive type supports.
 - b. Check that the drive is up and not assigned to another request.
 - c. Select the drive.

Note *This note applies only to NetBackup Enterprise Server.*

Ensure that the drive and the pending request are on the same host.

4. If necessary, get the media, write-enable it, and insert it into the drive.
5. Wait for the drive to become ready, as explained in the vendor’s drive equipment manual.
6. Click **Actions > Assign Request**.
Verify that the request is cleared from the Pending Requests pane.
7. In the Drives status pane, verify that the job request ID appears in the Request ID column for the drive *and* that the User column is not blank.



Resolving a Pending Request Example (Drive in AVR mode)


In this example, the drive is up under Automatic Volume Recognition control mode (the drive is a standalone drive or is a drive in a robot that is not working) as indicated by AVR in the Control column.

In this case, Media Manager can assign a drive automatically (which it does when the drive is in AVR mode, providing the recorded media ID on the volume header matches the media ID for the request). Since the volume is labeled, you *do not* have to assign the drive using **Actions > Assign Request**.

See the tables in “Drives Status Pane” on page 220 and “Pending Requests Pane” on page 224 for an explanation of each column in the drive status and the pending requests panes.


Note Some columns of the drive status and pending requests panes are not shown in this example.

1. The following pending request is displayed:

horseradish : 1 Pending Request.								
Request ID	Recorded Media ID	External Media ID	User	Density	Mode	Time	Barcode	Volume Group
 0	000084	000084	root	hcart	R	2/4/2003 3:49:32 PM	-----	---

The first task is to find an available tape drive for the request. The request specifies a recording density of hcart. This means that you need a 1/2 inch cartridge tape drive.

2. Check the Drives status pane for an appropriate tape drive.


1 Drive : (0 Active 0 Down)								
Drive Name	Type	Control	Recorded Media ID	External Media ID	Ready	Writable	Request ID	User
 STK9840A-FC-1	HCART	AVR			Yes	Yes	-	

STK9840A-FC-1 is a 1/2 inch cartridge drive and is available, since the control mode is not down and there is not a request number in the Request ID column.

3. Locate the volume with the external media ID of 000084. Depending on your site’s use of the Volume Group column, the volume group name may give an indication of where this media is located.
4. Insert the volume into the drive. Assume that the tape drive is on and ready to receive the volume. Also, assume that when you insert the volume, the tape drive loads and positions the tape to the load point.



5. Check the Drives status pane again to verify that the drive has been assigned to request ID 0. The following display shows that STK9840A-FC-1 is now assigned to request 0, which is the request to write information on the labeled volume 000084.

1 Drive : (1 Active 0 Down)									
Drive Name	Type	Control	Recorded Media ID	External Media ID	Ready	Writable	Request ID	User	
 STK9840A-FC-1	HCART	AVR	000084	000084	Yes	Yes	0	root	


The write operation will now proceed and the pending request will be removed. When the operation is complete, NetBackup or the `tpunmount` command will request Media Manager to release the drive and the drive will be available for other requests.

Resolving Pending Actions

▼ To resolve a pending action

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Pending Requests pane, select the pending action.

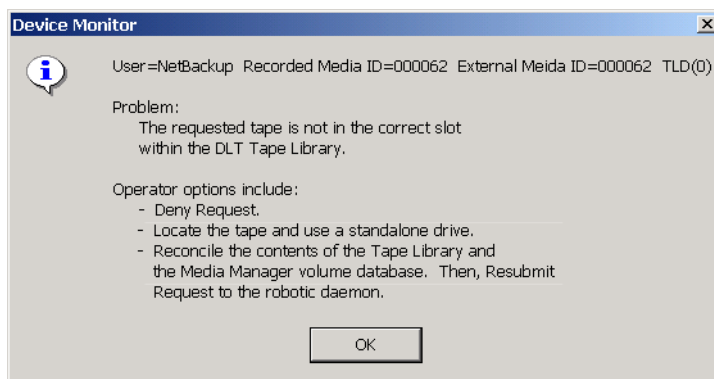
Note The following figure shows a pending action on a Windows server.

ainew2k : 1 Pending Request.								
Request ID	Recorded Media ID	External Media ID	User	Density	Mode	Time	Barcode	Volume Group
 *0 000062	000062	000062	NetBackup	hcart	R	2/5/2003 1:01:23 PM	000062	00_000_TLD

3. Click **Actions > Display Pending Action**.



This opens a message box with a description of the problem and a list of possible actions to correct the problem. The message box also shows other information, such as user name, recorded media ID, external media IDs, and drive number.



Click **OK** after viewing the information about the pending action.

4. In most cases, you can do either of the following actions to resolve the action:
 - a. Correct the error condition and resubmit the request. See “Resubmitting Requests” on page 242.
 - or
 - b. Click **Actions > Deny Request** to deny the request. See “Denying Requests” on page 243.

Resubmitting Requests

▼ To resubmit a request

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. Correct the problem identified by the pending action message.
3. In the Pending Requests pane, select the request.
4. Click **Actions > Resubmit Request**.

The pending action message is removed from the Pending Requests pane and the operation proceeds.

▼ **To resubmit a request for a missing volume**

For example, a volume was requested after being removed from a robotic library and the volume must be located.

1. Locate the missing volume.
2. Insert the volume in the robotic library.
3. Perform an Update Volume Configuration.

See “Updating the Volume Configuration for a Robot” on page 162 for complete instructions.

4. Resubmit the request.

Denying Requests

Some situations may require you to deny requests for service (for example, when drives are not available, you cannot find the volume, or the user is not authorized to use it). Denying a request returns an error message to the user.

▼ **To deny a request**

1. In the NetBackup Administration Console, click **Media and Device Management > Device Monitor**.
2. In the Pending Requests pane, select the request.
3. Click **Actions > Deny Request**.

The request is removed from the Pending Requests pane.



Shared Storage Option (SSO) Topics

6

Note *This chapter applies only to NetBackup Enterprise Server.*

The Shared Storage Option (SSO) is a separately licensed and priced VERITAS NetBackup software option, and is available only with NetBackup Enterprise Server. SSO runs on Windows and UNIX media servers (see “Supported Media Servers for SSO” on page 251) that has NetBackup is installed.

This software option is the Shared Drives option and the license key used to enable it is the Shared Storage Option key.

SSO requires appropriate hardware connectivity, such as, fibre channel hubs or switches, SCSI multiplexors, or SCSI-to-fibre bridges (see “Frequently Asked Questions About SSO” on page 263).

This chapter contains the following topics:

- ◆ “What is SSO?” on page 245
- ◆ “Configuring and Verifying Your SSO Hardware” on page 247
- ◆ “Installing the Shared Storage Option” on page 250
- ◆ “Configuring SSO in NetBackup” on page 253
- ◆ “Using Media Manager with SSO” on page 258
- ◆ “Troubleshooting SSO Issues” on page 260
- ◆ “SSO Reference Topics” on page 264

What is SSO?

SSO allows individual tape drives (stand-alone drives or drives in a robotic library) to be dynamically shared between multiple NetBackup servers licensed for SSO. Each media server can access any of the shared drives as needed and each server “owns” the drives it has active. The shared drives are automatically allocated and deallocated as backup and



restore operations dictate. This allows data to be backed up directly to tape drives in a SAN (Storage Area Network) configuration instead of moving data over the LAN—an important advantage of a SAN.

An Extension of Media Manager

SSO is an important extension to tape drive allocation and configuration for NetBackup Media Manager (see “SSO Components in Media Manager” on page 265). NetBackup and Storage Migrator use Media Manager for configuration, allocation, and control of tape drives and robotic libraries.

SSO is a software solution (in NetBackup and Media Manager). SSO does not load firmware in SAN devices or communicate with hub or switch APIs. SSO can communicate with hub or switch APIs if the `shared_drive_notify` script is used.

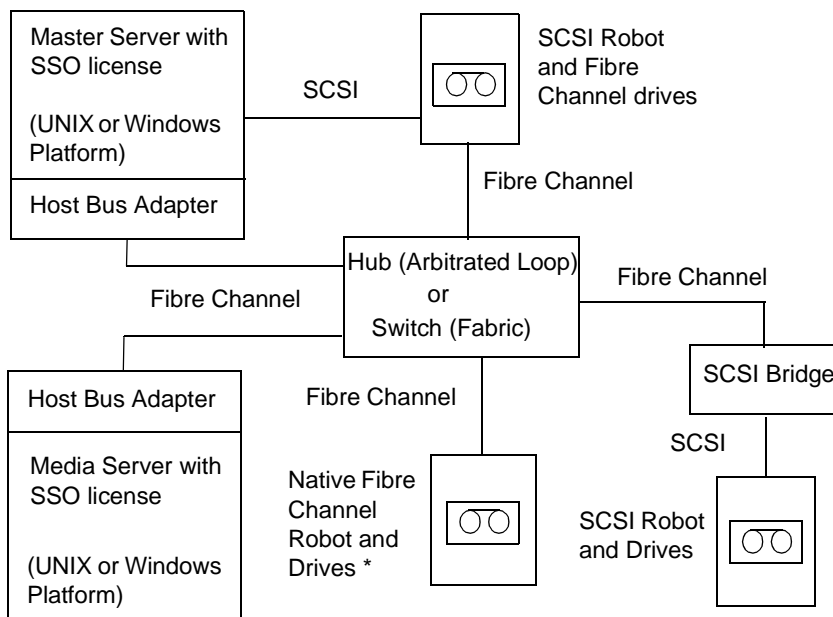
A SAN is not Required for SSO

SSO provides the management and coordination tools necessary to effectively share tape resources in a SAN. SSO was designed to work with fibre channel networks, but it can also be applied to environments that use SCSI switches or multi-initiator configurations. SAN fibre is not required to use SSO.

Sample SSO Configuration with SAN Components

The following figure shows typical SAN components in a shared drive configuration.

Example SSO Configuration



* Some robots have integrated bridges, but native fibre channel devices do not.

Configuring and Verifying Your SSO Hardware

Configuring your hardware for use with SSO includes the following general steps.

1. Configure your SAN environment.
2. Attach robots and drives.
3. Get all of the servers to recognize these shared devices.

On Windows servers, attaching devices and getting the system to recognize these devices is usually done by the operating system (in some instances you may have to install device drivers).

For UNIX servers, such as on Sun Solaris, hardware configuration may be more complicated, including modifying the sg driver configuration and other configuration files.

See “Making Changes to Your Hardware Configuration” on page 335 for information on replacing devices in an existing SSO configuration.



Using the Media Manager Device Configuration Guide

See the *NetBackup Media Manager Device Configuration Guide* for information on installing and configuring drivers, and modifying the appropriate system configuration files.

The configuration tasks explained in the device configuration guide are similar to the tasks required when configuring an SSO environment and in some cases specific fibre channel changes may be explained.

Configuration Tasks

Some of the following tasks may be optional depending on your particular hardware configuration.

- ◆ Determine the physical location of each drive within the robot. This is usually shown on the connectors to the drives or in the vendor documentation.

This task may not be needed if you use Media Manager device discovery (a part of the device configuration wizard).

- ◆ Make all drive and robot hardware connections.
- ◆ Install SAN connecting hardware (for example, bridges, switches, or hubs).
- ◆ If fibre is part of your configuration and you are using a SCSI-to-fibre bridge, determine the SCSI-to-fibre channel mapping for your tape devices.

Hard-wired SCSI IDs are converted to fibre channel LUNs that are presented to hosts involved in the configuration. Understanding which LUNs map to which physical SCSI IDs will ensure correct drive assignments.

Familiarity with the hardware and various vendor configuration tools will help you accomplish this task. See the vendor documentation for your bridge.

- ◆ Record the physical configuration.

When setting up an SSO configuration, it is helpful to record your hardware information. Record the adapter, SCSI addresses, WWNs, and fibre channel LUNs to which you connected each drive. It is also useful to record the version levels of firmware and drivers.

- ◆ Install and configure the appropriate drivers. See your vendor documentation for instructions.
- ◆ On UNIX servers, create any device files that are needed. Depending on the operating system, these files may be created automatically by using a reconfiguration boot (`boot -r`).

Create the device files for each drive based on the fibre channel LUNs of the drives and adapters. Add the name of the device file to your notes to complete the correlation between device files and physical drive location.

Use the device configuration guide and the man pages that are available with the operating system.

- ◆ On UNIX servers, customize the operating system by modifying the appropriate system configuration files. This task requires knowledge of the system files that use the SSO environment and their formats. For example on Sun Solaris systems, you may need to modify the sg, st, and HBA driver files.

Modify the HBA driver files to bind fibre channel devices (WWN) to a specific target ID. See your vendor documentation for specific syntax and more information.

- ◆ On Windows servers refer to the HBA documentation from the vendor for instructions on configuring the HBA.
- ◆ Use any available hardware configuration interface to configure and ensure that the configuration is what you expect. For example on Windows servers, you can use the HyperTerminal interface to configure SCSI-to-fibre bridges (click **Start > Programs > Accessories > HyperTerminal**).

Use the following general order when you configure and verify the hardware (start with the robot and shared drives and work back to the host):

- a. Robot and shared drives
 - b. Bridges
 - c. Hub or switches
 - d. Hosts
- ◆ If you experience errors during the installation and configuration of your SSO devices and you suspect the operating system, refer to the operating system logs as described in your operating system documentation.

Verifying Your Hardware is Connected and Working

Test your hardware configuration before proceeding with other configuration steps—this task is very important and is often overlooked. Note the following points:

- ◆ Verify that all of your servers (master and media) are able to communicate with one another. Perform a ping from each server to every other server. Be sure to ping by host name to verify that the name resolution methods are functioning properly.



- ◆ Use the NetBackup `bpcintcmd` utility to resolve IP addresses into host names. See the NetBackup troubleshooting guide and the NetBackup commands guide for more information.
- ◆ Use operating system and Media Manager commands and tools where available to verify the devices are configured correctly. Make sure you can "see" your devices on the SAN before you install and configure the SSO option.

For example on Solaris systems, use `mt -f /dev/rmt/0 status`). Note that if the configuration doesn't work in the operating system, it won't work for SSO.

- ◆ Make sure any dip switches on drives are set correctly (see "SSO Restrictions and Limitations" on page 252).
- ◆ See the appropriate chapter in the NetBackup Media Manager device configuration guide for more information and examples (the chapters in the configuration guide are organized by media server operating system type).

Installing the Shared Storage Option

See the following related topics:

- ◆ "System Requirements for SSO" on page 250
- ◆ "Volume Database Host (Device Allocation Host) Requirements" on page 251
- ◆ "Supported Robot Types for SSO" on page 251
- ◆ "Supported Media Servers for SSO" on page 251
- ◆ "SSO Restrictions and Limitations" on page 252
- ◆ "SSO Installation" on page 253

System Requirements for SSO

Because control messages used by the device allocator and many types of robot control are passed by a socket connection, all NetBackup and Storage Migrator servers must be LAN-connected.

See "NetBackup Mixed Server Configurations" on page 37 for information about mixed NetBackup server environments.

Volume Database Host (Device Allocation Host) Requirements

The host that is defined as the volume database host (usually the NetBackup master server) is also the device allocation host for SSO. If this system fails, not only will the SSO feature become non-operational, but all NetBackup backup and restore activity will fail. The following are requirements and recommendations for this host.

Host Requirements
It must be network-accessible from all hosts that are sharing drives managed by the device allocation host.
The volume database host, the global device database host, the vmd/DA host, and the master server must all be running the same level of NetBackup. The volume database host and the global device database host must be at the same or greater level of NetBackup as the media servers that they service.
VERITAS Host Recommendations
Use a common volume database host (the NetBackup master server is recommended) for your configuration.
Configure the common volume database host as a Highly Available host.
Use a relatively high-powered server for your volume database host.

Supported Robot Types for SSO

There is a difference between Media Manager supported robot types and Media Manager supported robot types for use with SSO.

SSO is supported *only* with the following Media Manager robot types. (The remaining Media Manager robot types are *not* supported for SSO.)

- ◆ ACS, TLH, and TLM (these are known as API robot types)
- ◆ TL8 and TLD

Supported Media Servers for SSO

The following list shows the media server platforms that are supported for use with SSO. See the NetBackup Media Manager device configuration guide and the NetBackup release notes for information on the supported operating system levels for these server platforms.

- ◆ Sun Solaris



- ◆ IBM RS6000 AIX
- ◆ HP HP9000 HP-UX
- ◆ HP Alpha Tru64 UNIX
- ◆ SGI IRIX
- ◆ RedHat Linux
- ◆ Suse Linux
- ◆ Microsoft Windows

SSO Restrictions and Limitations

- ◆ SSO cannot be used to share drives with an NDMP server. For example, a Network Appliance or an Auspex file server cannot share a tape drive with a NetBackup media server.
- ◆ SSO cannot be used to share drives with VERITAS Backup Exec. There is no interoperability between NetBackup and Backup Exec SSO, and they cannot share the same drives or robotics because of the different methods of drive arbitration that are used.
- ◆ SSO cannot be used to share drives with other applications running on a system, including system commands that access shared drives. This can interfere with device control and may lead to data loss.
- ◆ SSO cannot be used with certain types of tape robots. See “Supported Robot Types for SSO” on page 251 for the robot types that are supported.
- ◆ SSO is configured with Media Manager interfaces that are provided with NetBackup. If you intend to utilize SSO with VERITAS Storage Migrator you also must have NetBackup installed.
- ◆ Frequency-based drive cleaning is not supported for SSO drives because of issues tracking drive usage among multiple hosts. TapeAlert should be used.

See “Frequency-Based Cleaning” on page 312 for information on replacing devices in an existing SSO configuration.

Also see “Frequently Asked Questions About SSO” on page 263.

- ◆ NetBackup does not share media between media servers for shared (or non-shared) drives. When media is first used in a backup, NetBackup notes the media server (or NetBackup SAN media server) where the media is written and does not allow the media to be used by other servers.
- ◆ In some configurations, individual host power failure or reboots can affect data transfers on other hosts that share connectivity on a SAN.

- ◆ Older Sony AIT tape drives *may* require specific dip switch settings for proper SSO configuration and these settings can be different on various hosts. This is a limitation in their use in a SSO configuration. A Sony AIT drive that requires dip switch settings cannot be connected to multiple hosts that require different switch settings. In homogeneous configurations these drives work correctly; for example, in a configuration with multiple Windows hosts or multiple Solaris hosts.

SSO Installation

When you install NetBackup on a server you enter a key for NetBackup Enterprise Server. When NetBackup software is installed, Media Manager and the Shared Storage Option software are also installed.

SSO is a separately licensed feature and although the SSO software is already installed, you need a key to enable it. Check the license keys that were included with your software order to ensure that you have the Shared Storage Option key.

On the server you are prompted to enter license keys for any other software options that you purchased and want to enable. For more information on administering licenses for optional software, see the NetBackup system administrator's guide.

You can check keys by using the license key GUI available from the NetBackup help menu on Windows and UNIX servers (**Help > License Keys**). You can also use the `get_license_key` command on UNIX servers.

SSO must be enabled (by entering the Shared Storage Option key) on every server where shared drives will be configured and used.

▼ To enable SSO on all servers

1. Enable SSO on your master server.
2. Enable SSO on all of your media servers (or NetBackup SAN media servers).

Configuring SSO in NetBackup

Before using NetBackup, you must configure your shared drives for Media Manager usage (see “Configuring SSO Devices in Media Manager” on page 254), and also configure storage units and backup policies (see “Configuring NetBackup Storage Units and Backup Policies” on page 255).



Configuring SSO Devices in Media Manager

Using the Device Configuration or the Shared Drive Media Manager wizards is recommended and is the easiest method for configuring shared drives. Each of these wizards guides you through the steps involved in configuring drives that will be shared.

See “Why You Should Use the Media Manager Wizards” on page 43 and “Adding Shared Drives” on page 57.

There are also alternate ways to configuring SSO. See “Using Alternate Interfaces to Configure Shared Drives” on page 59.

Device Configuration Wizard Limitations

When using the Device Configuration wizard for shared drives, the limitations are different than in a configuration without shared drives. The following limitations apply when using this wizard in an SSO configuration.

Also see “The Device Configuration Wizard” on page 44 for more information about this wizard.

- ◆ You can use this wizard to configure devices only on the media servers listed in “Supported Media Servers for SSO” on page 251.
- ◆ In an SSO environment, this wizard does not support the complete configuring of ACS or TLM robots.

Some manual configuration is also involved. See “Configuring Shared ACS Drives” on page 382 and “Configuring Shared TLM Drives” on page 417.

- ◆ This wizard also does not support LMF or RSM robots, but these two robot types are *not* supported for SSO. The wizard will configure any drives found in these robots as standalone drives.
- ◆ This wizard can discover robots and drives attached to NDMP hosts, but using shared drives with NDMP is *not* supported for SSO.

Shared Drive Wizard Limitations

The Shared Drive wizard can be used to configure shared drives in ACS, TL8, TLD, TLH, or TLM robots; to configure shared standalone drives, or to change an existing shared drive.

This wizard has limited usage and

- ◆ Does not configure robots.
- ◆ Does not use device serialization and requires prior configuration details from you about your configuration before starting.

- ◆ Configures only one drive at a time.

Configuring NetBackup Storage Units and Backup Policies

On the master server you need to configure storage units and policies for your shared drives. If the device configuration wizard was used, storage units may have already been configured by the wizard.

See the NetBackup system administrator's guide for more detailed information.

Configuring Storage Units for Each Media Server

In each storage unit definition, you logically define the robot and the shared drives for that media server. For the number of drives to be used for backup (**Maximum concurrent drives used for backup**), you should specify the total number of all shared drives in the robot.

Configuring a Backup Policy for Each Media Server

Defining a policy for a media server depends on your VERITAS media server license, as follows. A license for a regular media server provides the greatest flexibility in configuring policies. A license for a NetBackup SAN media server is more restrictive.

- ◆ If you are defining a policy for a media server that is using SSO, then the policy can contain the media server (itself) as a client and any other network clients that you want to back up across the SAN to this media server.
- ◆ If you are defining a policy for a NetBackup SAN media server, then the policy will have just one client—the SAN media server—and will use the specific storage unit.

If you are defining a policy for network clients that you want to back up anywhere in your configuration, you can list all of the clients and choose **Any_available** (on NetBackup UNIX servers) or **Any_available** (on NetBackup Windows servers) as the policy storage unit or use the storage unit groups (prioritized storage units).

Verifying Your SSO Configuration

In an SSO configuration, a drive that is shared among multiple media servers must have the same logical name (drive name) on all of the NetBackup media servers. If the drive resides within a robotic library, it must also be correctly located (using the driver number) within the library. This section describes some tools that can be used to verify your configuration.



Verifying that your SSO configuration is set up correctly depends on your devices and how you configured SSO as follows:

- ◆ If you have serialized devices in your SSO configuration, VERITAS recommends using the Device Configuration wizard. The wizard will verify your configuration.
- ◆ If you have non-serialized devices in your SSO configuration, see the VERITAS support site for a tech note with instructions on verifying your configuration. The headline for the tech note is “Verifying an SSO Configuration with Non-Serialized Devices”.
- ◆ If you have serialized devices in your SSO configuration but you did *not* use the Device Configuration wizard, use the following procedure to verify your configuration.

▼ To verify a manually-configured SSO configuration

On all servers in your SSO configuration that are sharing a drive, you execute `scan` and `tpconfig -d` to verify that the robot drive number shown in the output of `tpconfig` matches the drive number that the robot reports in the output of `scan`. These commands are located in the NetBackup Media Manager directory `\Volmgr\bin`.

In the following example the ADIC robotic library has six drives, but only drives 5 and 6 are configured on this particular host.

Note The `scan` utility is not officially supported by VERITAS.

1. Execute `tpconfig -d` or `tpconfig -dl` and `scan`.
2. The output from `tpconfig -d` shows the logical drive names as assigned by Media Manager (QUANTUMDLT70000 and QUANTUMDLT70001) and the drive numbers for each drive.

Index	DriveName	DrivePath	Type	Shared	Status
0	QUANTUMDLT70000	/dev/st/nh3c0t5l0	dlt	No	UP
	TLD(0) Definition	DRIVE=5			
1	QUANTUMDLT70001	/dev/st/nh3c0t1l0	dlt	No	UP
	TLD(0) Definition	DRIVE=6			

Currently defined robotics are:

```
TLD(0)      robotic path = /dev/sg/h3c0t0l0,
            volume database host = norway
```

3. The output from the robot section of `scan` shows the same address for the robot (`/dev/sg/h3c0t0l0`), drive numbers (5 and 6), and serial numbers (PXA37S3261 and PXA50S2276) of these drives in the robot:

```

*****
***** SDT_TAPE *****
***** SDT_CHANGER *****
***** SDT_OPTICAL *****
*****
Device Name   : "/dev/sg/h3c0t010"
Passthru Name: "/dev/sg/h3c0t010"
Volume Header: ""
Port: -1; Bus: -1; Target: -1; LUN: -1
Inquiry      : "ADIC      Scalar 100      3.10"
Vendor ID    : "ADIC      "
Product ID   : "Scalar 100      "
Product Rev: "3.10"
Serial Number: "ADIC009K0340314"
WWN          : ""
WWN Id Type  : 0
Device Identifier: ""
Device Type   : SDT_CHANGER
NetBackup Robot Type: 6
Removable     : Yes
Device Supports: SCSI-2
Number of Drives : 6
Number of Slots : 50
Number of Media Access Ports: 10
Drive 1 Serial Number      : "PXB03S0979"
Drive 2 Serial Number      : "PXB03S0913"
Drive 3 Serial Number      : "CXA04S2051"
Drive 4 Serial Number      : "PXA31S1787"
Drive 5 Serial Number      : "PXA37S3261"
Drive 6 Serial Number      : "PXA50S2276"
Flags : 0x0
Reason: 0x0

```

4. Using the drive paths (/dev/st/nh3c0t510 and /dev/st/nh3c0t110) from the output of `tpconfig`, match the drive paths in the drives section output of `scan` to locate the serial numbers for each drive (PXA37S3261) and (PXA50S2276).

```

-----
Device Name   : "/dev/st/nh3c0t510"
Passthru Name: "/dev/sg/h3c0t510"
Volume Header: ""
Port: -1; Bus: -1; Target: -1; LUN: -1
Inquiry      : "QUANTUM DLT7000      2561"
Vendor ID    : "QUANTUM  "
Product ID   : "DLT7000      "
Product Rev: "2561"
Serial Number: "PXA37S3261"

```



```
WWN          : ""
WWN Id Type   : 0
Device Identifier: ""
Device Type    : SDT_TAPE
NetBackup Drive Type: 9
Removable      : Yes
Device Supports: SCSI-2
Flags : 0x4
Reason: 0x0
-----
Device Name    : "/dev/st/nh3c0t1l0"
Passthru Name  : "/dev/sg/h3c0t1l0"
Volume Header: ""
Port: -1; Bus: -1; Target: -1; LUN: -1
Inquiry       : "QUANTUM DLT7000          296B"
Vendor ID     : "QUANTUM "
Product ID    : "DLT7000          "
Product Rev   : "296B"
Serial Number : "PXA50S2276"
WWN          : ""
WWN Id Type   : 0
Device Identifier: ""
Device Type    : SDT_TAPE
NetBackup Drive Type: 9
Removable      : Yes
Device Supports: SCSI-2
Flags : 0x4
Reason: 0x0
```

5. Verify that the serial numbers for each drive (PXA37S3261) and (PXA50S2276) match the serial numbers in the output from the robot section of `scan` (see step 3).
6. Repeat these steps on all of the servers in your configuration. Ensure that each shared drive has the same logical Media Manager drive name on each media server that is sharing the drive.

Using Media Manager with SSO

You can use the Device Monitor to obtain information about your SSO configuration and manage your shared drives. See “Using the Device Monitor with SSO” on page 259.

You can also fine tune your configuration by adding SSO-related options in the Media Manager configuration file. See “Adding SSO Configuration Options” on page 260.

Using the Device Monitor with SSO

The Drive Status Pane

This display contains columns that are of note for shared drives. For example, **Control** and **Drive Index**.

See “Drives Status Pane” on page 220 for more details.

Changing the Operating Mode for a Shared Drive

The change mode dialog contains a list of the hosts that are sharing the selected drive. You can choose any number of hosts where the mode change will apply.

See “Changing the Operating Mode of a Drive” on page 232 for more details.

Adding or Changing a Comment for a Shared Drive

The change drive comment dialog contains a list of the hosts that are sharing the selected drive. You can choose any number of hosts where the change will apply.

See “Adding or Changing a Drive Comment” on page 236 for more details.

Performing Drive Cleaning Functions for a Shared Drive

See the following table for the available drive cleaning functions and their use with shared drives.

Drive Cleaning Function	Shared Drive Usage
Clean Now	In the list of hosts sharing the drive, you can choose only one host where the function will apply.
Reset Mount Time	In the list of hosts sharing the drive, you can choose any number of hosts where the function will apply.
Set Cleaning Frequency	This function is not available for shared drives.

See “Drive Cleaning Functions” on page 234 for more details.



Adding SSO Configuration Options

You can fine tune your configuration by adding SSO options to the Media Manager configuration file.

See “The Media Manager Configuration File (vm.conf)” on page 355 for descriptions of all of the available `vm.conf` entries.

Troubleshooting SSO Issues

This section includes the following:

- ◆ Lists of guidelines (“Hardware Configuration Guidelines” on page 260 and “Media Manager Configuration Guidelines” on page 261).
- ◆ Operating system references (“Operating System Help” on page 262).
- ◆ Common problems (“Common Configuration Issues with SSO” on page 262)
- ◆ FAQs that may help you resolve any SSO issues (“Frequently Asked Questions About SSO” on page 263).

Hardware Configuration Guidelines

- ◆ Mixing SAN components can introduce problems. Always use a SAN configuration and firmware levels that are supported by the hardware vendors.
- ◆ Consult SAN device, HBA, and operating system documentation to determine how to configure operating system tape drivers and passthru drivers to detect your SAN devices.
- ◆ Check your hub timer settings.
- ◆ Using hard arbitrated loop physical addresses, rather than soft addresses, usually works best. It is important to check with hardware suppliers to verify the recommended usage of their products.
- ◆ Check the firmware levels of all your fibre-channel hardware (for example, bridges) and make sure you are using the most recent level that is known to inter-operate with other SAN hardware devices. Firmware levels change very rapidly.
- ◆ Try to duplicate SAN issues and problems using commands and utilities on the host operating system.
- ◆ Test both backup and restore capabilities. It is possible to complete backups, but have unrecoverable images (for example, caused by incorrect switch settings).
- ◆ Ensure your hardware and SAN configuration is working and stable before adding SSO software.

Test backup and restore capabilities with dedicated tape drives before configuring them as shared drives.

- ◆ When building a large configuration, start drive sharing with a small number of tape drives and a small number (two or three) of media servers (or NetBackup SAN media servers).
- ◆ Configuration and troubleshooting of SSO is much easier when done on a smaller scale. If possible, create multiple and independent SSO configurations with subsets of servers sharing subsets of SAN-attached drives.
- ◆ Use the correct boot order for your fibre-channel hardware, as follows. Some devices take a while to completely boot. Watch for any indicator lights to become green.
 - a. Robots or drives
 - b. Bridges
 - c. Hubs or switches (wait 3 or 4 minutes)
 - d. Hosts

Media Manager Configuration Guidelines

Because of the great potential for creating incorrectly identified devices within an SSO configuration, it is recommended that you follow these practices:

- ◆ Use the Media Manager wizards to configure SSO. In particular, use the Device Configuration wizard rather than the Shared Drive wizard where possible.
- ◆ If you are using the Device Configuration wizard, you should configure all shared drives from *one* host (this is usually the master server). Launch the wizard only once with the current host set to the master server. You then indicate a list of media servers or NetBackup SAN media servers (in the Device Hosts screen). The wizard will configure devices on all of the media servers you selected and these hosts will receive the shared configuration information.
- ◆ Whether you have single or multiple master servers, define only one server to contain the volume database.

If you are using the Device Configuration wizard on a new installation, the volume database host is set by default to be the master server (unless you did not accept the default settings during NetBackup installation).



Operating System Help

If errors occur during the installation or configuration of your SSO devices and you suspect problems with the operating system, refer to the following:

- ◆ Operating system logs, as described in the operating system documents.
- ◆ NetBackup logs.
- ◆ Operating system man pages (UNIX servers only).
- ◆ The NetBackup Media Manager device configuration guide.

Common Configuration Issues with SSO

- ◆ Using incompatible or outdated firmware or drivers in a hub, switch, HBA, or bridge.
- ◆ Did not set the JNI HBA fail-over value to a value of zero to avoid I/O hangs (this is a bridge/HBA vendor fix).
- ◆ Using a HBA with SCSI-3 protocol, and the HBA is not compatible with the operating system drivers.
- ◆ Using cluster configurations when they were not supported.
- ◆ Using vendor peripherals that only work on a fibre-channel arbitrated loop.
- ◆ Did not verify that SSO has been enabled on *each* server (you enable SSO using the Shared Drive license key).
- ◆ Did not verify that SSO has been installed correctly. You can check keys by using the license key GUI available from the NetBackup **Help** menu on Windows and UNIX servers.
- ◆ Did not configure all of SSO from the master server. All configuration should be done from the master server, not from a media server (or SAN media server).
- ◆ Did not configure the same robotic path on every host. Remember that except for ACS and TLM robot types, only one host controls the robot.
- ◆ When using the Device Configuration wizard, did not select the appropriate device hosts, including the host with robotic control.
- ◆ Created inconsistent configurations by using `tpconfig` to configure SSO rather than the configuration wizards. These wizards have the added benefit of coordinating configurations across all hosts that are sharing the drives.
- ◆ Drives and robots that are connected by fibre channel cause increased complexity in a Media Manager device configuration. On some operating systems, the use of SCSI-to-fibre bridges may result in inconsistencies in the device paths when rebooting the host. After a reboot of the host, the device configuration should be verified.

- ◆ Using a name that is not consistent across all systems sharing drives.
- ◆ Did not test the drive paths on every media server.
- ◆ Did not define NetBackup storage units for each media server.
- ◆ Interrupting the data path while backup data is being transferred will cause the NetBackup job to fail. It can fail with a media write error or it may hang and have to be terminated manually.
- ◆ Did not use Berkeley-style close on the tape path (UNIX servers only)
- ◆ See the Sun chapter of the NetBackup Media Manager device configuration guide for more information on the following configuration tasks.

Forgot to add tape configuration list entries in `/kernel/drv/st.conf` (if needed).

Did not define configuration entries for expanded targets and LUNs in `sg.links` and `sg.conf` files. If you see problems with the entries in the `/etc/devlink.tab` file (created from `sg.links`). Check the following:

- ◆ The first entry uses hexadecimal notation for the target and LUN. The second entry uses decimal notation for the target and LUN.
- ◆ Use a single tab character between the entries, not a space or a space and a tab.

Did not configure the operating system to force load the `sg/st/fcaw` drivers.

Frequently Asked Questions About SSO

What combinations of SAN hardware components are supported for SSO?

SSO works with many hardware combinations. VERITAS has an open policy on hardware support for SSO. It is important to check with hardware suppliers to verify the interoperability of their products.

A list of SAN components that have been tested with NetBackup is available on the support web site (<http://support.veritas.com>).

I assume that once a server picks a tape drive and writes media, that media can only be written to again by that server. With existing NetBackup media servers today, a tape “belongs” to a media server until it expires or is deleted. Is this right?

Yes. Assigned media is still dedicated to a single server (see “SSO Restrictions and Limitations” on page 252). Be sure to define only one volume database host.



If I allocate four drives to a server and after an hour the server is finished with two of the drives and another server is requesting drives, will the two available drives be reallocated? Or does NetBackup wait until the backup schedule using the four drives is completely finished before reallocating the drives?

The two available drives will be reallocated and used. The NetBackup tape manager component is aware of drive status and notifies the NetBackup scheduler of drive availability.

Does the NetBackup SSO use IP protocol or SCSI protocol?

SSO uses IP protocol to pass control messages among peers.

Is it possible to set up drive cleaning for shared drives? I realize you can't use frequency-based cleaning, but can TapeAlert be used?

Yes. Using TapeAlert without frequency-based cleaning means that the tape will be cleaned only when the drive firmware (TapeAlert) requests a cleaning.

TapeAlert is not available for some types of drives, and some host platforms and adaptor connections. Since TapeAlert provides the same type of cleaning as library-based cleaning (robotic cleaning or auto cleaning), it is recommended that you disable library-based cleaning if using TapeAlert (for most vendor's robots).

SSO Reference Topics

SSO-Related Terms and Concepts

Shared Drive

When the Shared Storage Option is installed, a tape drive that is shared among hosts is termed a shared drive.

Backup Exec Shared Storage Option

The VERITAS NetBackup Shared Storage Option is not the same as the VERITAS Backup Exec Shared Storage Option. The Backup Exec implementation of drive sharing does not include support for UNIX servers and uses a different method for drive arbitration.

Library Sharing or Robot Sharing

Media Manager also manages distributed access from multiple servers to robotic tape libraries (library sharing or robot sharing). This capability is not related to SSO and should not be confused with SSO.

Media Servers and NetBackup SAN Media Servers

VERITAS licenses media servers that can back up their own data or data from other network clients as well. VERITAS also licenses NetBackup SAN media servers that can only back up their own data to shared drives—no backing up of data residing on other clients is allowed.

SSO Components in Media Manager

SSO utilizes the basic NetBackup and Media Manager processes and daemons to perform its tasks. `vmd` is the Media Manager volume daemon on UNIX hosts and the NetBackup Volume Manager service on Windows hosts. A major function of `vmd` is to manage media information. An additional function that `vmd` can provide is to be the device allocator (DA) for shared drives. In this case, `vmd` is known as `vmd/DA`.

vmd/DA

To coordinate network-wide allocation of tape drives, `vmd/DA` acts as a central clearing agent for all NetBackup and Storage Migrator shared tape requests in a storage area network. `vmd/DA` responds to requests from multiple instances of NetBackup master servers, media servers, NetBackup SAN media servers, or Storage Migrator (the versions of Media Manager that are installed must be compatible).

For shared drive configurations, the host that is configured as the volume database host for a drive in a robot or a standalone drive is also known as the device allocation host (see “Device Allocation Host” on page 268). This is the host where `vmd/DA` resides. Other hosts in the configuration have `vmd` without device allocator functionality being utilized.

`vmd/DA` maintains shared drive and host information, such as a list of hosts that are registered to share a drive and which host currently has the drive reserved. Shared drive information is

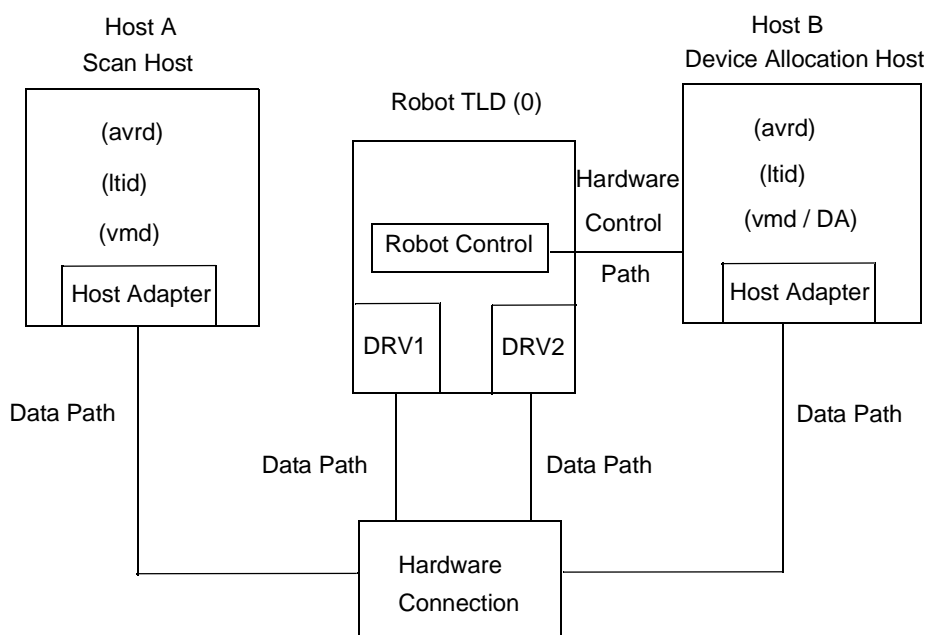
- ◆ Modified by requests from `ltid` (the Media Manager device daemon on UNIX and the NetBackup Device Manager service on Windows).
- ◆ Dynamic, since it is built and maintained at runtime, rather than being stored on the device allocation host.



When `ltid` initializes on a device host, it calls `vmd/DA` with a list of shared drives. `vmd/DA` adds these drives and the host name to its configuration if necessary. Since `ltid` passes a complete list of drives each time, `vmd/DA` deletes references to drives for that host when a change in configuration removes them from that host's shared drive list. This deletion occurs when `ltid` is shut down gracefully or after it is restarted.

Example SSO Configuration Showing Media Manager Components

The following figure shows an example of a shared drive configuration with Media Manager components. See the NetBackup troubleshooting guide for a process flow diagram of SSO components.



In this figure, Host A is

- ◆ Connected to drives `DRV1` and `DRV2` through enabling hardware.
- ◆ The host where `ltid` was started first and called `vmd/DA` on the device allocation host (Host B) to register a shared drive. This action identifies Host A as the initial scan host (see “Scan Host” on page 267) for the drives.

In this figure, Host B

- ◆ Is connected to drives `DRV1` and `DRV2` through enabling hardware.

- ◆ Is configured to be the volume database host for the robot TLD (0) and therefore is also the device allocation host (see “Device Allocation Host” on page 268). `vmd/DA` is active on this host.
- ◆ Controls the robotics (except for ACS or TLM robot types, there is only one robot control host for each robot).
- ◆ Could be optionally configured as a Highly Available (HA) server.

Scan Host

Each shared drive has a host that is identified as the scan host. A *scan host* is the host where `avrd` (the automatic volume recognition daemon/process) is scanning the drive when there is no other activity on that drive. A scan host must have data-path access to the drive.

Instances of `ltid` on hosts that are *not* scan hosts create `rdevmi` (remote device management interface) processes on the scan hosts. These processes communicate with the other hosts sharing the drive, and run on the scan hosts as slave processes of the non-scan hosts `ltid`. These processes receive drive status information held in shared memory on the scan host. This status information is used to maintain the shared drive information on all of the hosts sharing the drive.

Each time an `rdevmi` process starts up, it is logged in the daemon log. Also, each host that is identified as a scan host in the output of the `vmdareq` command will show `rdevmi` processes running for each host it is sharing a drive with. For example if there are 12 hosts sharing a drive, the host that is the scan host will have 11 `rdevmi` processes running on it.

How the Scan Host is Determined

Scan hosts are determined by `vmd/DA` and may be different for each shared drive. The first device host (with a scan ability factor of non-zero, see “Adding SSO Configuration Options” on page 260) that registers each shared drive with `vmd/DA` becomes the initial scan host for that drive. This host does not change as other hosts register.

All device hosts that register with `vmd/DA` pass a list of shared drives. The name of the currently assigned scan host for each drive is then returned to each registering host.

The Scan Host Can Change

A scan host is assigned for a shared drive until some interruption occurs. For example, one of the following occurs:

- ◆ The socket connection, the host, the drive, or the network goes down.
- ◆ The drive is logically placed in the Down mode.



A new scan host is then chosen. If a scan host is declared unavailable, `vmd/DA` assigns a new scan host so that the requesting host can resume as soon as the previous scan host relinquishes its use of the drive.

The scan host temporarily changes to hosts that are requesting tape mounts while the mount is in progress. This happens so only one host at a time has access to the drive path.

A scan host for a drive needs to periodically re-register with `vmd/DA` to ensure that it remains the scan host. A host that is not identified as a scan host does not need to re-register until some disruptive event occurs (for example, a restart of `ltid` or a failure to get drive status data from the scan host for one or more drives).

Re-registering with `vmd/DA` keeps `vmd/DA` and the host that is registering in coordination within a dynamic shared drive configuration.

Device Allocation Host

The device allocation host is another name for the volume database host, when the volume database host performs tasks in support of SSO. This host is also the host where `vmd/DA` runs and manages the following:

- ◆ Reservations for shared drives on a host-by-host basis.
- ◆ A list of shared drives.
- ◆ A list of hosts that have registered to share a drive and where the drive is currently assigned.

How the Device Allocation Host is Determined

For SSO, the current volume database host for the drive is always the device allocation host for that drive.

If you follow the recommendations (see “Volume Database Host (Device Allocation Host) Requirements” on page 251) and configure one volume database host for a site, one device allocation host can manage multiple robotics connected to many media or master servers.

Media Manager Reference Topics

A

You may find the following Media Manager reference and conceptual topics useful:

- ◆ “NetBackup Media Manager Best Practices” on page 270
- ◆ “NetBackup and Media Manager Databases” on page 274
- ◆ “Robot Overview” on page 276
- ◆ “Frequently Asked Questions About Device Discovery” on page 295
- ◆ “How NetBackup Uses SCSI Reserve/Release” on page 298
- ◆ “Correlating Device Files to Physical Drives When Adding Drives” on page 306
- ◆ “Drive Cleaning” on page 309
- ◆ “Volume Pools and Volume Groups” on page 314
- ◆ “Barcodes” on page 321
- ◆ “Using the Physical Inventory Utility for Non-Barcoded Media” on page 325
- ◆ “Making Changes to Your Hardware Configuration” on page 335
- ◆ “Labeling Media” on page 338
- ◆ “Mounting and Unmounting of Media” on page 338
- ◆ “Suspending Media Or Downing Devices” on page 339
- ◆ “How Media Manager Selects a Drive for a Robotic Mount Request” on page 339
- ◆ “How NetBackup Selects Media in Robots” on page 340
- ◆ “How NetBackup Selects Media in Standalone Drives” on page 342
- ◆ “Media Formats” on page 344
- ◆ “Media Manager Security” on page 347
- ◆ “Administrators Quick Reference” on page 352
- ◆ “The Media Manager Configuration File (vm.conf)” on page 355



NetBackup Media Manager Best Practices

The following are lists of best practices for NetBackup Media Manager. If you follow these recommendations, you will greatly reduce your chances of encountering problems. Many of these best practices are directly related to reducing the amount of effort needed to administer your configuration. Following these best practices should save you administration time.

- ◆ “General Practices” on page 270
- ◆ “Media and Device Management Domain Management” on page 271
- ◆ “Media Management” on page 271
- ◆ “Device Management” on page 272
- ◆ “Performance and Troubleshooting” on page 273
- ◆ “Other Best Practices” on page 274

Visit the VERITAS support web site (<http://www.support.veritas.com>) for a list of supported devices, server platforms, and the latest device mapping file.

See “Media Manager Terminology” on page 1 for definitions of the terms used in these topics.

General Practices

- ◆ Use only VERITAS documented and VERITAS supported options for NetBackup Media Manager commands.
- ◆ Refer to the NetBackup release notes to see if the methods you are currently using are being eliminated or going to be eliminated in future releases, as well as for information about all new functionality in each release.
- ◆ Use the documented methods for terminating the NetBackup Media Manager daemons and services.
- ◆ Periodic auditing of backups should be done using the verify command in the NetBackup administrator interface. Periodic restores should also be done.
- ◆ Always backup your media servers' databases, as well as your master server's databases.
- ◆ When restoring NetBackup databases, the backups must all be from the same point in time (this includes media databases).
- ◆ If you want to use devices with some other application and these devices are currently being controlled by Media Manager, you must down the drive if the drive is in the Media Manager UP state.



Media and Device Management Domain Management

- ◆ Users cannot share devices or volumes between MDM Domains.
- ◆ Media IDs must be unique within a given MDM Domain.
- ◆ Barcodes must be unique within a given MDM Domain.
- ◆ Drive Names must be unique within a given MDM Domain and should be descriptive.
- ◆ Robot Numbers must be unique within a given MDM Domain.
- ◆ Host names should be consistent throughout a MDM Domain. That is, everywhere within a configuration, a host should be referred to with the same name. Do not mix fully qualified and unqualified, or physical names with virtual host names.
- ◆ The MDM Domain server should be one of the NetBackup master servers and there should be only one MDM Domain server per site.
- ◆ All names and numbers for devices, and all media IDs and barcodes should remain unique across the entire enterprise.

The following applies only to NetBackup Enterprise Server.

- ◆ The volume database host, the global device database host, and the master server must all be running the same release level of NetBackup.
- ◆ There should be only one volume database host per global device database host and both of these key databases should be located on the same host (it is recommended that this host be the master server). This host is known as the Media and Device Management Domain (MDM Domain) server.

You can enforce this practice by adding a NOT_DATABASE_HOST entry in the Media Manager configuration file. See “Not Allowing a Host To Manage Databases” on page 368.

The `tpautoconf` command has options to preview and merge existing global device databases. Also, the `vmdb_merge` command can be used to merge volume, pool, and media databases. See the NetBackup commands guide for details.

Media Management

- ◆ Use the robot inventory update operation for media management.
- ◆ Use a scratch pool for unassigned media.
- ◆ Configure cleaning cartridges for your drives and use TapeAlert for automatic drive cleaning where possible.



- ◆ Replace old media, especially cleaning media, according to the life-span recommendations of the manufacturer.
- ◆ Do not use robotic libraries that do not have a barcode reader and use only barcode labels that are recommended by the robot vendor.
- ◆ Use barcode rules for proper media type assignment when inventorying multi-media libraries. Use barcode-naming conventions, such as naming prefixes, to differentiate between data and cleaning tapes as well as different physical media types.
- ◆ Only use only the NetBackup Administration Console or the `bpexpdate` command to unassign media. Never use the Media Manager command lines for this task.
- ◆ Before performing inject or eject commands, the media access port should be empty. Although NetBackup can handle a port that is not empty, some libraries may have problems.

Device Management

- ◆ Periodically monitor the NetBackup system log for device errors encountered.
- ◆ Periodically monitor devices using the NetBackup Device Monitor.
- ◆ Investigate the causes of all drives that are down.
- ◆ Do not use the robotic test utilities while running backup or restore jobs.
- ◆ Read the NetBackup device configuration guide before configuring devices on media servers (or SAN media servers).
- ◆ Use only tested robots. See the NetBackup hardware compatibility list.
- ◆ Use only tested tape drives and tape drivers. See the NetBackup hardware compatibility list on the VERITAS support site.
- ◆ Use only supported server platforms and hardware. See the NetBackup release notes and the VERITAS support site.
- ◆ Use only fully-serialized devices. A full-serialized SCSI library should report a serial number for the robot and also serial numbers for each drive in the robot.
- ◆ Always configure and use pass-through paths for robotic libraries and drives.
- ◆ When applicable, enable SCSI reserve/release in the operating system.
- ◆ Use persistent bindings for fibre-attached devices.
- ◆ When applicable, use the device configuration wizard to configure your devices for use with NetBackup.

Note Any devices that were manually configured are deleted and are reconfigured by this wizard.

- ◆ Download the latest device mapping file from the VERITAS support web site before running the device configuration wizard.
- ◆ Use consistent logical drive types for all physical drive types on all servers enterprise-wide. For example, all DLT7000 drives are configured in NetBackup as the logical drive type dlt.
- ◆ Do not use the Microsoft RSM Remote Storage Manager (RSM) unless your devices need to be shared with other applications. Sharing devices between NetBackup and other applications should be avoided.
- ◆ Do not load vendor medium-changer drivers on Microsoft Windows hosts. The default Microsoft medium-changer driver is acceptable (but is not required) for use with NetBackup.
- ◆ *The following applies only to NetBackup Enterprise Server.*

Shared devices (drives and robot libraries) must be configured on hosts that have access to each other.

See “Shared Storage Option (SSO) Topics” on page 245 for details.
- ◆ *The following applies only to NetBackup Enterprise Server.*

When setting up ACS robot configurations, use the following general sequence:

 - a. Use the device configuration wizard to add all drives as standalone drives on one host.
 - b. Manually add the ACS robot and update the drives with the correct robot coordinates.
 - c. Verify the drives using the procedures outlined in the NetBackup device configuration guide.
 - d. Propagate the configuration to other hosts using the device configuration wizard.

Performance and Troubleshooting

- ◆ Use the performance-tuning documents available on the VERITAS support web page.
- ◆ Use only dedicated backup servers (not application or file servers) for the volume database host and master servers. Plan periodic maintenance periods for all of your backup servers.



- ◆ Consult the NetBackup troubleshooting guide for all error conditions.
- ◆ Always install the latest NetBackup patches (feature and maintenance packs) available from VERITAS.
- ◆ Verify all SCSI-related operating system configuration files (for example, the Solaris `st.conf` file), when installing operating system patches.
- ◆ For device related problems, consult the vendor for firmware upgrades and consult the VERITAS hardware compatibility list for supported firmware levels.
- ◆ Do not use `DISABLE_RESOURCES_BUSY`.
- ◆ Do not disable `TCP_NODELAY` functionality.
- ◆ *The following applies only to NetBackup Enterprise Server.*

See “Shared Storage Option (SSO) Topics” on page 245 before installing and configuring SSO drives.

Other Best Practices

- ◆ Have a well-documented disaster recovery and storage management plan in place. This plan should include keeping catalog backup media IDs in multiple physical locations. See the NetBackup Vault administration guide.
- ◆ Maintain an independent and separate test environment for software and hardware upgrade testing and new device compatibility testing. This environment should be used to test any changes planned for your production system.
- ◆ See the recommended best practices for your NetBackup optional software in the guides for these products. For example, see the NetBackup Vault system administration guide for the best practices for NetBackup Vault.

NetBackup and Media Manager Databases

NetBackup and Media Manager use internal databases to keep information about the media and device configuration.

Caution Do not remove or edit the NetBackup or Media Manager databases. These files are for internal use only and altering them in any way can result in permanent loss of data.

See the following topics:

- ◆ “Media Manager Volume Database” on page 275
- ◆ “Media Catalog” on page 275



- ◆ “NetBackup Catalogs” on page 275
- ◆ “Device Databases” on page 276

Media Manager Volume Database

The volume database contains information about volumes that have been configured for use by Media Manager. When you add volumes they are recorded in the volume database. The volume database resides in the *install_path*\Volmgr\database folder (the default *install_path* is C:\Program Files\VERITAS).

When adding new volumes, you target the NetBackup server that has the volume database. A part of this process is assigning media IDs.

Media IDs must be unique and can consist of six or less alphanumeric characters. Optical disks each have two media IDs, one for side A and one for side B.

Media Catalog

NetBackup keeps a media catalog with information that correlates backups to the volumes where they are stored. Each NetBackup server maintains a media catalog for the storage units that are attached to that server.

During installation, the media catalog is created in the *install_path*\NetBackup\db\media folder. NetBackup refers to the media catalog when it needs a volume for a backup or restore. If the media catalog does not contain a suitable volume, NetBackup has Media Manager assign one. In this manner, the catalog is populated as NetBackup uses new volumes for backups.

When the retention period has ended for all backups on a volume, NetBackup deletes the volume from the media catalog. NetBackup then sends a request to Media Manager to unassign the volume so it is available for later reassignment.

NetBackup Catalogs

Volumes for backups of the NetBackup catalogs are a special case and do not appear in the media catalog.

You must track the media IDs for these volumes separately so you can find them in case the media catalog is damaged. However, they do appear in the Media Manager volume catalog and are listed as assigned to NetBackup (they are unassigned only if you delete them from your catalog backup settings).

Alternatively, you can locate media for catalog backups using the physical inventory utility. It may take significant time for each tape to be mounted so its recorded label can be read. See “Using the Physical Inventory Utility for Non-Barcoded Media” on page 325.



Device Databases

The device databases have information about the drives and robots that are in NetBackup storage units. When you configure drives and robots, Media Manager stores this information in its device databases. These databases are located under *install_path\Volmgr\database*.

Robot Overview

In Media Manager, a robot is a peripheral device that automates the mounting and dismounting of media in tape or optical disk drives. Media Manager software that controls robots is referred to as robotic control software.

See the following topics:

- ◆ “Media Manager Robot Types” on page 276
- ◆ “Media Manager Media Types” on page 277
- ◆ “Robot Attributes” on page 279

Media Manager Robot Types

Media Manager classifies robots by robot type, according to one of the following characteristics:

- ◆ The physical characteristics of the robot. Library usually refers to a larger robot, in terms of slot capacity or number of drives. Stacker usually refers to a robot with one drive and low media capacity (6 - 12 media slots).
- ◆ The media type commonly used by that class of robots. 4 MM and 8 MM are examples of media types.
- ◆ The communication methods used by the underlying robotics. SCSI-based and API robots are the two main methods.

The following table lists the Media Manager robot types, with drive and slot limits for each type. Check the Note column for any restrictions.

Visit the VERITAS support web site to determine which robot type applies to the model of robot that you are using.

Media Manager Robot Types

Robot Type	Description	Drive Limits	Slot Limits	Note
ACS	Automated Cartridge System	1680 (per the ACS Library Software host)	No limit	Applies only to NetBackup Enterprise Server.
LMF	Library Management Facility	256	No limit	Applies only to NetBackup Enterprise Server.
ODL	Optical Disk Library	12	490	
RSM	Removable Storage Manager	256	No limit	
TL4	Tape Library 4MM	2	15	
TL8	Tape Library 8MM	No limit	16000	
TLD	Tape Library DLT	No limit	16000	
TLH	Tape Library Half-inch	256	No limit	Applies only to NetBackup Enterprise Server.
TLM	Tape Library Multimedia	250	No limit	Applies only to NetBackup Enterprise Server.
TS8	Tape Stacker 8MM	2	21	
TSD	Tape Stacker DLT	1	14	
TSH	Tape Stacker Half-inch	1	10	

Media Manager Media Types

Media Manager uses media types to differentiate tape or optical media with different physical characteristics. Each Media Manager media type may represent a specific physical media type, for example Sony AIT media can have a Media Manager media type of 8MM, 8MM2, or 8MM3.



The following table lists the Media Manager media types and their description:

Media Type	Description
QCART	1/4 inch cartridge tape
HCART	1/2 inch cartridge tape
HCART2	1/2 inch cartridge tape 2
HCART3	1/2 inch cartridge tape 3
4MM	4MM cartridge tape
8MM	8MM cartridge tape
8MM2	8MM cartridge tape 2
8MM3	8MM cartridge tape 3
DLT	DLT cartridge tape
DLT2	DLT cartridge tape 2
DLT3	DLT cartridge tape 3
DTF	DTF cartridge tape
REWR_OPT	Rewritable optical disk
WORM_OPT	WORM optical disk
HC_CLN	1/2 inch cleaning tape
HC2_CLN	1/2 inch cleaning tape 2
HC3_CLN	1/2 inch cleaning tape 3
4MM_CLN	4MM cleaning tape
8MM_CLN	8MM cleaning tape
8MM2_CLN	8MM cleaning tape 2
8MM3_CLN	8MM cleaning tape 3

Media Type	Description
DLT_CLN	DLT cleaning tape
DLT2_CLN	DLT cleaning tape 2
DLT3_CLN	DLT cleaning tape 3
DTF_CLN	DTF cleaning tape

Alternate Media Types

Use the 8MM2, 8MM3, DLT2, DLT3, HCART2, or HCART3 alternate media types when you have more than one type of 8MM, DLT or 1/2 inch cartridge tape in the same robotic library and you want to differentiate between them.

For example if a robotic library has DLT7000 and DLT4000 drives, you do not want to accidentally load a tape that was written in a DLT7000 drive into a DLT4000 drive. In this case, you can specify the DLT media type for DLT7000 tapes and DLT2 for DLT4000 tapes, if the drive types were configured using the same convention.

Note In a robotic library, all of the volumes of a particular vendor media type *must* be the same Media Manager media type.

In the example that follows for a TLH robot type, the HCART2 media type is not valid. Both volumes must be HCART or both must be HCART2.

Volume	TLH Media Type	Media Manager Media Type
ABC123	3490E	HCART
ABC156	3490E	HCART2

Robot Attributes

Media Manager configures and controls a robotic device differently depending on the robot type. The following tables list the attributes that dictate how these robot types differ.

See the NetBackup release notes or visit the VERITAS support web site for more detailed information on supported peripherals, platforms, and firmware levels tested.



ACS Robot Attributes

Attribute	NetBackup Server (ACS robots are not supported)	NetBackup Enterprise Server
API Robot		Yes
SCSI Control		No
LAN Control		Yes
Remote Robot Control		No. Each host that has ACS drives attached has robotic control.
NDMP Support		Yes
Shared Drives Support		Yes
Drive Cleaning Support		No. Drive cleaning is managed by ACS library software.
Media Access Port Support		Yes, for eject only.
Media Manager Tracks Slots		No
Media Type Support		DLT, DLT2, DLT3, HCART, HCART2, and HCART3.
Hosts Supported		Windows (requires STK LibAttach software) and UNIX. Note: LibAttach for Windows is not available for servers running Windows 2003.
Barcode Support		Yes. Depends on ACS library software to obtain Media Manager media IDs. Barcodes must be the same as the media ID (1 to 6 characters).
Robot Examples		STK 97xx, STK L180, STK L700, and STK Powderhorn Silo.



ACS Robot Attributes (continued)

Attribute	NetBackup Server (ACS robots are not supported)	NetBackup Enterprise Server
For More Information		See the ACS appendix, “STK Automated Cartridge System (ACS)” on page 377.

LMF Robot Attributes

Attribute	NetBackup Server (LMF robots are not supported)	NetBackup Enterprise Server
API Robot		Yes
SCSI Control		No
LAN Control		Yes
Remote Robot Control		Yes
NDMP Support		No
Shared Drives Support		No
Drive Cleaning Support		No. Cleaning is managed by the robotic library.
Media Access Port Support		Yes
Media Manager Tracks Slots		No
Media Type Support		HCART, HCART2, and HCART3.
Hosts Supported		UNIX Solaris.
Barcode Support		Yes. Depends on LMF software to obtain the Media Manager media ID. Barcodes must be the same as the media ID (1 to 6 characters).



LMF Robot Attributes (continued)

Attribute	NetBackup Server (LMF robots are not supported)	NetBackup Enterprise Server
Robot Examples	Fujitsu F6458	

ODL Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes
LAN Control	No	No
Remote Robot Control	No	No
NDMP Support	No	No
Shared Drives Support	No	No
Drive Cleaning Support	No	No
Media Access Port Support	Yes	Yes
Media Manager Tracks Slots	Yes	Yes
Media Type Support	REWR_OPT and WORM_OPT. REWR_OPT and WORM_OPT.	
Hosts Supported	UNIX. Not all UNIX operating systems are supported, see the NetBackup support web site.	
Barcode Support	No, but the robot has inventory capability and can report if a slot in the robot contains media.	
Robot Examples	HP Optical Disk Libraries and HP SureStore Optical Libraries.	
For More Information	See the NetBackup Media Manager device configuration guide.	



RSM Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	Yes	Yes
SCSI Control	No	No
LAN Control	No	No
Remote Robot Control	No	No
NDMP Support	No	No
Shared Drives Support	No	No
Drive Cleaning Support	No. Drive cleaning is supported using the RSM administrative interface on the Microsoft Windows operating systems that support RSM robots.	
Media Access Port Support	Eject is supported. Inject is not supported, but you can use the RSM Inject wizard on the Microsoft Windows operating systems that support RSM.	
Media Manager Tracks Slots	No	No
Media Type Support	4MM, 8MM, 8MM2, 8MM3, DLT, DLT2, DLT3, HCART, HCART2, HCART3, and QIC.	
Hosts Supported	Microsoft Windows operating systems that support RSM.	
Barcode Support	Yes, if the robot supports barcodes. Barcodes must be the same as the Media Manager media ID (1 to 6 characters).	
Robot Examples	Exabyte 210 and Quantum DLTStor.	
For More Information	See the RSM appendix, "Microsoft Removable Storage Manager (RSM)" on page 391.	



TL4 Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes
LAN Control	Not Applicable	No
Remote Robot Control	Not Applicable	No
NDMP Support	No	No
Shared Drives Support	Not Applicable	No
Drive Cleaning Support	Yes	Yes
Media Access Port Support	No	No
Media Manager Tracks Slots	Yes	Yes
Media Type Support	4MM	4MM
Hosts Supported	Windows and UNIX.	Windows and UNIX.
Barcode Support	No, but the robot has inventory capability and can report whether a slot in the robot contains media.	
Robot Examples	ADIC 4mm DAT Autochanger and HP DAT Autoloader.	
For More Information	See the NetBackup Media Manager device configuration guide.	

TL8 Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes



TL8 Robot Attributes (continued)

Attribute	NetBackup Server	NetBackup Enterprise Server
LAN Control	Not Applicable	No
Remote Robot Control	Not Applicable	Yes
NDMP Support	Yes	Yes
Shared Drives Support	Not Applicable	Yes
Drive Cleaning Support	Yes	Yes
Media Access Port Support	Yes	Yes
Media Manager Tracks Slots	Yes	Yes
Media Type Support	8MM, 8MM2, and 8MM3.	8MM, 8MM2, and 8MM3.
Hosts Supported	Windows and UNIX.	Windows and UNIX.
Barcode Support	Yes. Barcodes can be from 1 to 16 characters. Note: the Media Manager media ID will be six or less characters.	
Robot Examples	IBM 7331, Qualstar 46120, ADIC Scalar 100 AIT, ADIC Scalar 1000 AIT, Overland Data LoaderXpress, and Exabyte X200.	
For More Information	See the NetBackup Media Manager device configuration guide.	

TLD Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes
LAN Control	Not Applicable	No
Remote Robot Control	Not Applicable	Yes



TLD Robot Attributes (continued)

Attribute	NetBackup Server	NetBackup Enterprise Server
NDMP Support	Yes	Yes
Shared Drives Support	Not Applicable	Yes
Drive Cleaning Support	Yes	Yes
Media Access Port Support	Yes	Yes
Media Manager Tracks Slots	Yes	Yes
Hosts Supported	Windows and UNIX.	Windows and UNIX.
Media Type Support	DLT, DLT2, DLT3, DTF, 8MM, 8MM2, 8MM3, QIC, HCART, HCART2, and HCART3.	
Barcode Support	Yes. Barcodes can be from 1 to 16 characters in length. Note: the Media Manager media ID will be six or less characters.	
Robot Examples	ADIC Scalar 1000 DLT, ATL D7000, STK L Series, and Overland Data Neo series	
For More Information	See the NetBackup Media Manager device configuration guide.	

TLH Robot Attributes

Attribute	NetBackup Server (TLH robots are not supported)	NetBackup Enterprise Server
API Robot		Yes
SCSI Control		No
LAN Control		Yes
Remote Robot Control		Yes
NDMP Support		Yes



TLH Robot Attributes (continued)

Attribute	NetBackup Server (TLH robots are not supported)	NetBackup Enterprise Server
Shared Drives Support		Yes
Drive Cleaning Support		No. Cleaning is managed by the robotic library.
Media Access Port Support		Yes
Media Manager Tracks Slots		No
Media Type Support		HCART, HCART2, and HCART3.
Hosts Supported		Windows and UNIX.
Barcode Support		Yes. Depends on IBM ATL software to obtain the Media Manager media ID. Barcodes must be the same as the media ID (1 to 6 characters).
Robot Examples		IBM 3494 and IBM VTS
For More Information		See the TLH appendix, "IBM Automated Tape Library (ATL)" on page 399.

TLM Robot Attributes

Attribute	NetBackup Server (TLM robots are not supported)	NetBackup Enterprise Server
API Robot		Yes
SCSI Control		No
LAN Control		Yes



TLM Robot Attributes (continued)

Attribute	NetBackup Server (TLM robots are not supported)	NetBackup Enterprise Server
Remote Robot Control		No. Each server that has TLM drives attached has robotic control.
NDMP Support		No
Shared Drives Support		Yes
Drive Cleaning Support		Yes
Media Access Port Support		Yes
Media Manager Tracks Slots		No
Media Type Support		4MM, 8MM, 8MM2, 8MM3, DLT, DLT2, DLT3, DTF, HCART, HCART2, HCART3, REWR_OPT (HP9000-800 only), and WORM_OPT (HP9000-800 only).
Hosts Supported		Windows and UNIX.
Barcode Support		Yes. Depends on DAS/SDLC software to obtain the Media Manager media ID. Barcodes must be the same as the media ID (1 to 6 characters).
Robot Examples		ADIC AML/J, ADIC AML/S, and ADIC Scalar 10000.
For More Information		See the TLM appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 411.



TS8 Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes
LAN Control	Not Applicable	No
Remote Robot Control	Not Applicable	No
NDMP Support	No	No
Shared Drives Support	Not Applicable	No
Drive Cleaning Support	Yes	Yes
Media Access Port Support	No	No
Media Manager Tracks Slots	Yes	Yes
Media Type Support	8MM, 8MM2, 8MM3.	8MM, 8MM2, 8MM3.
Hosts Supported	Windows and UNIX.	Windows and UNIX.
Barcode Support	Yes. Barcodes can be from 1 to 16 characters in length. Note: the Media Manager media ID will be six or less characters.	
Robot Examples	Exabyte 10x and Exabyte 210. Exabyte 10x and Exabyte 210.	
For More Information	See the NetBackup Media Manager device configuration guide.	

TSD Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes



TSD Robot Attributes (continued)

Attribute	NetBackup Server	NetBackup Enterprise Server
LAN Control	Not Applicable	No
Remote Robot Control	Not Applicable	No
NDMP Support	Yes	Yes
Shared Drives Support	Not Applicable	No
Drive Cleaning Support	Yes	Yes
Media Access Port Support	No	No
Media Manager Tracks Slots	Yes	Yes
Media Type Support	DLT, DLT2, and DLT3.	DLT, DLT2, and DLT3.
Hosts Supported	Windows and UNIX.	Windows and UNIX.
Barcode Support	No, but the robot has inventory capability and can report whether a slot in the robot contains media.	
Robot Examples	Sun StorEdge L280 and Quantum DLTStor.	
For More Information	See the NetBackup Media Manager device configuration guide.	

TSH Robot Attributes

Attribute	NetBackup Server	NetBackup Enterprise Server
API Robot	No	No
SCSI Control	Yes	Yes
LAN Control	Not Applicable	No
Remote Robot Control	Not Applicable	No
NDMP Support	No	No



TSH Robot Attributes (continued)

Attribute	NetBackup Server	NetBackup Enterprise Server
Shared Drives Support	Not Applicable	No
Drive Cleaning Support	Yes	Yes
Media Access Port Support	Yes	Yes
Media Manager Tracks Slots	Yes	Yes
Media Type Support	HCART, HCART2, and HCART3.	
Hosts Supported	UNIX. Not all operating UNIX systems are supported, see the NetBackup support web site.	
Barcode Support	No, but the robot has inventory capability and can report whether a slot in a robot contains media.	
Robot Examples	IBM 3590 B11 Autoloader. IBM 3590 E11.	
For More Information	See the NetBackup Media Manager device configuration guide.	

Table-Driven Robotics

Table-driven robotics provides support for some new robotic library devices without the need to modify any library control binaries. This feature uses the device mapping file for supported robots and drives.

This means that support for your new or upgraded devices may be accomplished without waiting for a maintenance patch from VERITAS. Since the device mapping file includes pertinent information relating to the operation and control of libraries, support for some new devices may only require that you download an updated mapping file when any device changes are made to your configuration.

See “The Device Mapping File” on page 36 for information on how to download the latest mapping file for your devices.



Robotic Test Utilities

You can use the robotic test utilities for configured robots by executing `install_path\volmgr\bin\robtest.exe` and selecting the desired type of robotic library.

From each test utility, you can obtain a list of available test commands by entering a question mark (?).

The following point applies only to NetBackup Enterprise Server.

Use the `drstat` command to determine the drive addressing parameters for ACS, LMF, TLH, and TLM robot types. This command is available in the robotic test utilities for these robot types. For most robot types, the drive addressing parameter is the robot drive number. For ACS robot types, drives are addressed by ACS, LSM, Panel, and Drive number. For TLH robot types, drives are addressed by the IBM device number. For TLM robot types, drives are addressed by the DAS/SDLC drive name.

Robotic Processes

A Media Manager robotic and possibly a robotic control process exist for each robotic library that you install on a Windows media server (or SAN media server).

Every Media server that has a drive in a robotic library has a robotic process for that robotic library. The robotic process receives requests from the NetBackup Device Manager and sends necessary information directly to the robotics or to a robotic control process.

Robotic control processes exist only for robot types that support library sharing (or robot sharing).

Starting the NetBackup Device Manager service on a media server (or SAN media server) starts the robotic and robotic control processes for all robots configured on that host. Stopping this service stops these processes.

The Services tab of the NetBackup Activity Monitor has commands for starting and stopping all services, including the NetBackup Device Manager service. You can also start and stop this service through commands on the Device Monitor **Actions** menu or the Media and Device Management **Actions** menu. In addition, the NetBackup Commands for Windows manual describes commands for controlling robotic processes that run on Windows media servers (or SAN media servers).

When a robotic or robotic control process is running, the NetBackup Activity monitor processes tab shows it in the UP or DOWN state. When a connection is made to the appropriate robotic library, the corresponding process is in the UP state and can mount or unmount tapes (or platters). If the connection cannot be made or errors exist, the process changes to the DOWN state. In the DOWN state the process is still running and returns to the UP state when the connection is made or problems no longer exist.

Process Example

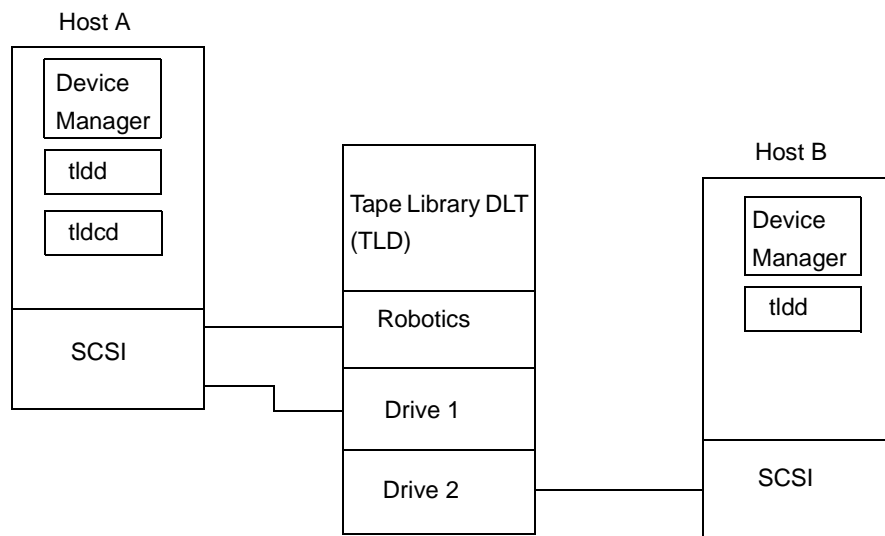
This is a NetBackup Enterprise Server topic.

For example, each drive in a Tape Library DLT (TLD) robot can be attached to a different host and each host would have a `tldd` process. The robotics, however, are controlled by a single host and only that host has the robotic control process, `tlcdc`. When it is necessary to mount a tape, the robotic process (`tldd`), on the host with the drive, sends control information to the robotic control process (`tlcdc`) on the host controlling the robotics.

The following figure shows the processes and where they run for a Tape Library DLT (TLD) robot. In this diagram

- ◆ Each host connects to one drive and has a robotic process, `tldd`.
- ◆ The robotic control and therefore the robotic control process, `tlcdc`, is on Host A.

The NetBackup Device Manager services on host A and B start `tldd`. The `tldd` process on Host A also starts `tlcdc`. Requests to mount tapes from host B go to `tldd` on Host B, which then sends the robotic command to `tlcdc` on Host A.



Processes by Robot Type

The following table lists the robotic and robotic control processes for each robot type that are supported on Windows media servers. Review the Note column for any restrictions.

Robotic and Robotic Control Processes

Robot Type	Process	Description	Note
Automated Cartridge System (ACS)	acsd	acsd runs on the NetBackup server and communicates mount and unmount requests to the host that controls the ACS robotics.	Applies only to NetBackup Enterprise Server.
Tape Library DLT (TLD)	tldd tlcdc	tldd, runs on a NetBackup server that has a drive in the Tape Library DLT. This process receives NetBackup Device Manager requests to mount and unmount volumes, and sends these requests to the robotic-control process, tlcdc. tlcdc communicates with the Tape Library DLT robotics through a SCSI interface. For library sharing, tlcdc runs on the NetBackup server that has the robotic control.	Applies only to NetBackup Enterprise Server.
Tape Library 4MM (TL4)	tl4d	tl4d runs on the host that has a Tape Library 4MM. This process receives NetBackup Device Manager requests to mount and unmount volumes and communicates these requests to the robotics through a SCSI interface.	
Tape Library 8MM (TL8)	tl8d tl8cd	tl8d, runs on a NetBackup server that has a drive in the Tape Library 8MM. This process receives NetBackup Device Manager requests to mount and unmount volumes, and sends these requests to the robotic-control process, tl8cd. tl8cd communicates with the TL8 robotics through a SCSI interface. For library sharing, tl8cd runs on the NetBackup server that has the robotic control.	Applies only to NetBackup Enterprise Server.



Robotic and Robotic Control Processes (continued)

Robot Type	Process	Description	Note
Tape Library Half-inch (TLH)	tlhd tlhcd	tlhd, runs on each NetBackup server that has a drive in the Tape Library Half-inch. This process receives NetBackup Device Manager requests to mount and unmount volumes and sends these requests to the robotic-control process. tlhcd runs on the NetBackup server that has the robotic control and communicates with the TLH robotics through a SCSI interface	Applies only to NetBackup Enterprise Server.
Tape Library Multimedia (TLM)	tlmd	tlmd runs on the NetBackup server and communicates mount and unmount requests to the host that controls the TLM robotics.	Applies only to NetBackup Enterprise Server.
Tape Stacker 8MM (TS8)	ts8d	ts8d runs on the NetBackup server that has a Tape Stacker 8MM attached. This process receives NetBackup Device Manager requests to mount and unmount volumes and communicates these requests to the robotics through a SCSI interface.	
Tape Stacker DLT (TSD)	tsdd	tsdd runs on the NetBackup server that has a Tape Stacker DLT attached. This process receives NetBackup Device Manager requests to mount and unmount volumes and communicates these requests to the robotics through a SCSI interface.	
Removable Storage Manager (RSM)	rsmd	rsmd runs on a Windows 2000 (and later supported releases) NetBackup server. rsmd interfaces with NetBackup Device Manager to mount and unmount tapes that are under Microsoft RSM control.	

Frequently Asked Questions About Device Discovery

NetBackup provides device discovery and auto-configuration on all supported operating system server platforms (except NetWare servers) and for supported peripherals. The following sections cover frequently asked questions about device discovery and auto device configuration in NetBackup.



What is device discovery?

Device discovery is an exploratory method used by Media Manager to determine which peripheral devices are visible from a given host. Visibility depends on physical attachment (SCSI, Fibre, and so on), device state (on and responding, or off and not responding), and host-based system device-layer configuration.

Discovery is done by sending SCSI commands through operating system device files (on UNIX) or APIs (on Windows servers) which support SCSI pass-through. Note that if there is no pass-through path to access a device, the device is not discovered or recognized.

What is the goal of device discovery?

The goal is to provide information to enable fully automated or partially-automated configuration of peripherals for use with NetBackup.

Device discovery must be accurate, timely, and provide coverage for typical NetBackup configurations.

Device discovery returns data needed to correlate devices that may be interconnected across multiple hosts or even multiple host bus adapters on the same host.

What is device serialization?

Serialization means that devices are uniquely identified by a serial number. Device relationships can be determined based on comparing serial numbers from multiple sources referring to the same device. If both a robotic library and a drive fully support serialization, the drive's position (or address) in the robotic library can be determined.

What types of devices can be auto-discovered by NetBackup?

The following types of devices can be discovered:

- ◆ SCSI-based robotic libraries (for example, changers, autoloaders, stackers).
- ◆ SCSI-based tape drives.
- ◆ Native parallel SCSI, fibre channel fabric (FCP) and FC-AL (loop) connections.
- ◆ SCSI over IP (reported).
- ◆ Devices that are attached to certain NDMP filers.

How does device discovery fit into the NetBackup architecture?

This is a NetBackup Enterprise Server topic.

NetBackup is based on a static configuration of devices. These configurations are persistent for robotic libraries, and tape or optical drives in device databases on each NetBackup media server (or SAN media server). These databases have data structures that are managed by the following:

- ◆ The NetBackup GUIs

- ◆ Device configuration wizards
- ◆ The `tpconfig` command.
- ◆ An internal API

A subset of device configuration information plus extra discovered attributes is managed in a central database called the global device database. The global device database host is defined at installation time and should be unique for all media servers (or SAN media servers) sharing devices in a multiple server configuration. See “Media and Device Management Domain Management” on page 271.

When `ltid` (the Media Manager device daemon on UNIX or the NetBackup Device Manager service on Windows servers) starts up, it reads the local device database into a shared memory segment. Components on the same host communicate using shared memory IPC or socket protocols. Socket protocols are used between components across multiple hosts. Command line interfaces are available to obtain run-time (shared memory) information and static device configuration information.

How does the Device Configuration wizard use device discovery?

Device discovery is initiated by the Device Configuration Wizard. This wizard is activated as part of the NetBackup Getting Started Wizard. From a list of hosts to be discovered, the wizard issues device discovery queries to all the hosts and correlates the data returned. A tree view of the devices is presented in the wizard, which allows drives to be dragged and dropped between specific addresses in a robotic library and the group of standalone (non-robotic) drives if required.

If the devices are fully serialized, no dragging and dropping is required. Device configuration changes are made as needed across all hosts where device discovery was requested. `ltid` is stopped and restarted to activate the latest device configuration.

The device configuration wizard can be used again if the physical device configuration has changed or if it needs to be verified. However, `ltid` cannot be stopped and restarted while NetBackup activity is in progress, which means that jobs should not be running when the device configuration wizard is invoked.

Does NetBackup require all of its devices to be discoverable?

No. Using device discovery and the Device Configuration wizard is the recommended and easiest-to-use method for creating and updating your device configurations. In addition, NetBackup supports a varied set of devices that are not currently auto-discovered, as well as some devices that are currently undiscoverable (for example, ACS, TLM, LMF, and RSM robots) without some user intervention. The Media Manager manual-based device configuration interfaces are still used in these cases.

How can the device configuration be viewed and verified?

You can view and check your device configuration by using one of the following device configuration interfaces available in NetBackup:



- ◆ Media and Device Management for UNIX
- ◆ Media and Device Management for Windows
- ◆ Menu-based device configuration interface (`tpconfig` on UNIX)
- ◆ Command line interface for device configuration (`tpconfig -d` command)

Your device configuration can be verified by using one of the following. Some details of a device configuration cannot be validated without attempting tape mounts. Robotic test utilities (using `robtest`) are available for extended device and configuration testing.

- ◆ Re-run the Device Configuration wizard.
- ◆ Use the Configuration Analyzer that is available from Media and Device Management for UNIX.

Why doesn't NetBackup detect whether drives are available from all hosts?

This is a NetBackup Enterprise Server topic.

NetBackup polls locally-attached non-shared drives on the hosts where they are configured when they are in the UP state and are not in use. However for shared drives, polling is done only on the Scan Host until a mount request is received from NetBackup. During a mount request, polling is transferred to the host requesting the mount once a drive has been selected.

This design enables NetBackup to support Dynamic Loop Switching or SAN zoning. Every drive needs to be visible only from a single-host perspective. Each drive can potentially have its own Scan Host that switches dynamically for error handling and continued availability. A central device arbitrating component (`vmd/DA`) manages scan host assignments for shared drives. `vmd/DA` also handles a network drive reservation system so that multiple media servers (or SAN media servers) can efficiently share a drive.

Polling a shared drive from a single host is not a complete solution. It allows dynamic loop switching and reduces the number of device accesses and associated CPU time, but it does not allow for breakages in device connectivity (for example, discontinuity in the fibre channel fabric) to be detected until the device is actually used for I/O.

How NetBackup Uses SCSI Reserve/Release

The following topics explain how SCSI reserve/release is used by NetBackup in SSO and non-SSO environments:

- ◆ “Background Topics” on page 299
- ◆ “How NetBackup Uses SCSI Reserve/Release Commands” on page 300
- ◆ “Issuing Reset Commands to Break a Reservation” on page 304

- ◆ “Controlling SCSI Reserve/Release” on page 305
- ◆ “SCSI Reserve/Release Requirements and Limitations” on page 306

Background Topics

The following topics explain a major change in the implementation of NetBackup SSO and an overview of the SCSI reserve/release functionality.

NetBackup Releases Prior to NetBackup 4.5

In previous releases of NetBackup, Media Manager used a network protocol for drive reservations. In some situations, this allowed any program outside the local NetBackup realm to access drives without NetBackup being aware of the fact (this was true for drives in SSO and SAN configurations, and also for non-SSO locally attached drives).

In SAN configurations, NetBackup could have a drive open for read or write operations on one host and the device could be accessed by another host. This situation could occur since there was no single tape driver controlling access to the device. If an external program moved the tape for any reason during a NetBackup operation, data corruption could be the result, since NetBackup assumed the tape position was unchanged from the last command NetBackup had issued to the drive.

NetBackup 4.5 and Later Releases

In multiple-initiator (multiple HBA) environments (such as SSO configurations), some form of device-level protection is required to avoid unintended sharing of tape devices and possible data loss problems. The only widely available technique for this purpose is to use SCSI reserve/release functionality.

Starting with release 4.5, NetBackup uses SCSI reserve/release commands to improve data integrity. SCSI reserve/release operates at the SCSI target level and depends on the fibre-to-SCSI bridge or the native fibre device hardware working correctly.

SCSI Reserve/Release Commands

When a device receives a SCSI reserve command, it will no longer process commands from any other HBA until the reserving HBA issues the SCSI release command. If an application sends a command to a reserved device, the device will fail the command by returning a status of RESERVATION CONFLICT. The only exceptions to this action are the Inquiry, Log Sense, Report LUNs, and Request Sense commands, which will return the requested information.

A device stays reserved until one of the following actions occurs. The device is



- ◆ Released by the HBA that reserved it.
- ◆ Released by some sort of TARGET or LOGICAL UNIT RESET. These resets are protocol dependent, and differ between parallel SCSI and FCP (SCSI on fibre channel). These resets may be issued from any HBA.
- ◆ Power cycled.
- ◆ Released by fibre channel LOGO/PLOGO/PRLI/PRLO/TPRLO or failed discovery (link actions).

A negative effect of SCSI reserve can occur if the reserving HBA stops working (for example, due to a system crash or hardware failure). All devices reserved by the HBA stay reserved until the reservation is removed or broken. The reservation can only be removed by the original HBA, which means the system must be available. In the case of a hardware failure, this is not possible.

To break a reservation the device must be reset. This can be done by any of the following:

- ◆ SCSI reset
- ◆ Bus device reset
- ◆ LUN device reset
- ◆ Power cycle
- ◆ Fibre channel link actions may break reservations.

SCSI reserve and SCSI release commands are mandatory for all SCSI-2 and SCSI-3 devices. See the SCSI 2 standard for a detailed description of SCSI reserve command operation and behavior.

How NetBackup Uses SCSI Reserve/Release Commands

The following topics explain how NetBackup uses SCSI reserve/release commands in an SSO environment (or any other multiple-initiator environment). The same basic operations are performed by other VERITAS applications (for example, VERITAS Storage Migrator components).

Issuing the Reserve

This topic applies to HP-UX, IRIX, Solaris, AIX, TRU64, Linux, and Windows servers.

The NetBackup processes (bptm, bprecover, and bpbbackupdb) that read or write tape media issue a SCSI reserve command to the tape device that contains the media in use (during the open process). Once the reservation is established, all other HBAs are locked out of this tape device. This reservation prevents other HBAs from issuing commands that can cause data loss.

This reservation *does not* prevent other applications from using the same device on the server with the reservation and causing data loss (for example, someone issuing a UNIX `mt` command).

Checking for Data Loss

This topic applies to HP-UX, Solaris, AIX, TRU64, Linux, and Windows servers.

The `bptm` process detects data loss by reading the tape position and then checking the actual position against the expected position. If the actual position is less than the expected position (at the end of the backup process), the following will occur:

- ◆ The tape is frozen.
- ◆ The backup fails.
- ◆ The following error message entry is placed in the error log:

```
FREEZING media id xxxxxx, External event caused rewind during
write, all data on media is lost
```

Possible Causes

If the SCSI reserve/release feature is not enabled on your servers, data loss can be caused by configuration errors, incorrect paths, multiple master servers, incorrect SSO configurations and third-party or operating system utilities. If the SCSI reserve/release feature is enabled on all servers, then the cause could be third-party or operating system utilities running on the server that is also running the backup operation.

Unfortunately data loss cannot be prevented, just recognized after the fact. The NetBackup catalog is not cleaned up to remove information on prior backup sessions that were lost. The `bpexptdate` command must be run on the media id to clean up the catalog.

Disabling the Position Check

VERITAS recommends that the check for data loss *not be* disabled.

▼ To disable the position check on UNIX servers

- ❖ Create the following file:
`/usr/opensv/netbackup/db/config/NO_POSITION_CHECK`

▼ To disable the position check on Windows servers

- ❖ Create the following file:
`install_path\netbackup\db\config\NO_POSITION_CHECK`



Checking for Tape/Driver Configuration Errors

This topic applies to HP-UX, Solaris, AIX, TRU64, Linux, and Windows servers.

The `bptm` process detects data loss by reading the tape position and then checking the actual position against the expected position. Any configuration problem that causes the actual position to be greater than the expected position (at the end of the backup process), causes the following to occur:

- ◆ The tape is frozen.
- ◆ The backup fails.
- ◆ The following error message entry is placed in the error log:

```
FREEZING media id xxxxxx, too many data blocks written, check  
tape/driver block size configuration
```

The backup data may be usable, in which case the image will need to be imported before restores can be done (using the `bpimport` command).

Possible Causes

The source of the configuration problem needs to be identified and corrected. The most common configuration error is the failure to configure the driver for variable length blocks.

A second source of the error could be in the tape driver's configuration data. On Solaris, this could be in `/kernel/drv/st.conf`. Review the NetBackup Media Manager device configuration guide for the operating system you are using.

Disabling the Position Check

VERITAS recommends that the check for data loss *not be* disabled.

▼ To disable the position check on UNIX servers

- ❖ Create the following file:
`/usr/opensv/netbackup/db/config/NO_POSITION_CHECK`

▼ To disable the position check on Windows servers

- ❖ Create the following file:
`install_path\netbackup\db\config\NO_POSITION_CHECK`

Issuing the Release

After a NetBackup process has finished with the media, a SCSI release is issued as part of the unmount operation. This release frees the device for access by another HBA.

Also, at the beginning of the startup process `avrd` issues a SCSI release to all configured tape devices that are currently in the Up state. This is done to release devices that were reserved at the time of a system re-boot or crash. The SCSI release command will return tape devices to general availability after a system crash.

Error Recovery

To recover a device that is reserved by an HBA that crashes or otherwise was unable to issue the SCSI release command, you can use the following option for the Media Manager `vmopr cmd` command:

```
vmopr cmd -crawlreleasebyname drive_name
```

This option requests all hosts that are registered to use the drive to release the drive (using the SCSI release command).

Issue the `vmopr cmd` command on the host that is the device allocator (DA host) or use the `-h` option on the command to specify the DA host.

Caution You can use this command after a PEND status has been displayed in **Device Monitor** in the NetBackup Administration Console, but do not issue this command during backups.

See the NetBackup commands for UNIX or Windows for the complete syntax and more information on using the `vmopr cmd` command.

SCSI Reserve/Release Logging and Conflict Notification

The `bptm` process logs all SCSI reserve/release commands. The `bptm` log should be checked on all hosts to ensure the SCSI reserve operation is being logged (look for SCSI RESERVE in the log).

The `avrd` process monitors all tape devices. NetBackup manages access to tape devices, such that a properly configured system will not receive the RESERVATION CONFLICT status from a tape device.

Reservation Conflict

If `avrd` gets a RESERVATION CONFLICT status, `avrd` changes the status of the device to PEND and writes the following message in the system log:

```
Reservation Conflict status from DRIVENAME (device NUMBER)
```



When the conflict is resolved, the following message will be written to the log:

```
Reservation Conflict status cleared from DRIVENAME (device NUMBER)
```

If this conflict occurs, some sort of mis-configuration is present (for example, the tape drive is reserved, but should not be) and the configuration problem should be corrected. A possible cause of this conflict is if an operating system crashes or a hardware failure has left a device reserved (see “Issuing the Release” on page 303).

Also in the **Device Monitor** or the output from the `vmopr cmd` command, PEND in the Control column means that a reservation conflict has occurred.

Server Operating System Limitations

This topic applies to HP-UX, TRU64, and Windows servers.

These operating systems cannot distinguish between a reserved device and a busy device. For these systems PEND will be reported in the Device Monitor, if another application is using the device. This indicates a mis-configuration, as NetBackup cannot share tape devices with other applications. If you are using other applications, you should use the `tpreq` command or Down the drive before using the drive.

These operating systems also may report PEND if the drive reports Busy when a volume is unmounted. You can use the AVRD_PEND_DELAY entry in the Media Manager configuration file to filter out these extraneous reports.

Server Operating System Limitations

This topic applies to IRIX servers.

This operating system cannot detect that a device is reserved. If the SSO scan host is running on an IRIX system, no indication of this configuration problem will occur.

Issuing Reset Commands to Break a Reservation

On the following operating systems, you can try to reset a reservation conflict by using the associated reset commands.

Caution The reset operation may reset other devices in your configuration. Loss of data is also possible. Alternate methods of breaking the reservation on a device (using switch and bridge hardware) should be tried first.

▼ **To reset a reservation on Sun Solaris**

1. Issue `mt -f drive_path_name forcereserve.`
2. Issue `mt -f drive_path_name release.`

See the `mt (1)` man page for more information.

▼ **To reset a reservation on HP-UX**

- ❖ Issue `st -f drive_path_name -r.`

See the `st (1m)` man page for more information.

▼ **To reset a reservation on IBM AIX**

- ❖ Issue `tctl -f drive_path_name reset.`

See the `tctl` man page (in the IBM AIX Commands Reference) for more information.

▼ **To reset a reservation on SGI IRIX**

Issue either of the following commands:

- ❖ `scsiha -r bus_number`
- ❖ `scsiha -L target_number bus_number`

See the `scsiha (1m)` man page for more information.

Controlling SCSI Reserve/Release

In NetBackup 4.5 and later releases, using SCSI reserve for data integrity is on by default. SCSI reserve can be disabled by using an entry in the UNIX `bp.conf` file or in the registry on Windows servers.

The `bp.conf` file can be modified to contain a `DISABLE_SCSI_RESERVE` entry, which will turn off the use of SCSI reserve to all tape devices from this host.

The NetBackup UNIX and Windows GUIs have a checkbox to add or remove this entry in the `bp.conf` file or the registry. Select **NetBackup Management > Host Properties**. Select a master or media server (or SAN media server) in the right pane and then **Properties > Media > Disable SCSI Reserve**.



SCSI Reserve/Release Requirements and Limitations

The requirements are as follows:

- ◆ There must be passthru driver access to all shared drives. The passthru driver must be installed and all required paths must be created.

See the NetBackup Media Manager device configuration guide for information on configuring and using the passthru driver for various UNIX operating systems.

- ◆ Host operating systems must be properly coordinated with the requirements of the NetBackup use of SCSI reserve/release.
- ◆ Users of Solaris 7 must install a ST driver patch to avoid a problem that keeps the device reserved when it should not be. For Solaris 7, the minimum patch level required is 107460-06.
- ◆ Users of HP-UX must disable the operating system's use of SCSI reserve/release.

See the topic, Enabling SCSI Reserve/Release in the HP 9000 chapter of the NetBackup Media Manager device configuration guide for instructions.

This VERITAS implementation using SCSI reserve/release has the following limitations:

- ◆ SCSI reserve/release is not applicable for NDMP drives (no reserve command is available).
- ◆ Third-party copy configurations must be configured correctly. To retain reservation of a tape device when doing a third-party copy backup, refer to the description of the `mover.conf` file in the *NetBackup ServerFree Agent System Administrator's Guide for UNIX*.
- ◆ Cluster environments or multi-path environments with fail-over capability may leave devices reserved when fail-over occurs. If the fail-over does not break the device reservations, then the NetBackup use of SCSI reserve/release must be disabled.
- ◆ Cluster environments or multi-path environments with dynamic path sharing (TRU64 systems, for example) will cause backup and restore failures if the path changes. If path sharing cannot be eliminated, then the NetBackup use of SCSI reserve/release must be disabled.

Correlating Device Files to Physical Drives When Adding Drives

The following two topics may not be necessary if you used the Device Configuration Wizard to configure your drives and the drives and robotic libraries both support device serialization.

The following point applies only to NetBackup Enterprise Server.



If you are configuring shared drives, see “Shared Storage Option (SSO) Topics” on page 245 for more information.

On Windows Hosts

When selecting the drive address (for example, robot drive number) for a tape drive, match the logical device name with the drives in the physical drive layout as follows:

▼ To correlate device files

1. Note the SCSI target of the drive and check the Windows Tape Devices display to determine which device name (for example, Tape0) was assigned to the drive.
2. Correlate the SCSI target to the drive address using the robot's interface panel or checking the indicators on the rear panel of the tape drive.
3. Determine the physical drive address (for example, number) by checking labels on the robot.
4. Configure the robot and then add the drives.

When you add the drives, check your notes to ensure that you are assigning the correct drive address to each device path.

5. Optionally, use the appropriate robotic test utility to verify the configuration.
 - a. Stop the NetBackup Device Manager service (`ltid`).
 - b. Start `ltid` to start the Automatic Volume Recognition process (`avrd`). You must stop and restart `ltid` to ensure that the current device configuration has been activated.

The following point applies only to NetBackup Enterprise Server.

Also start the remote robotic control process, if robotic control is not local to this host.

- c. Use the robotic test utility to mount a tape on a drive.
- d. Use the Device Monitor to verify the tape was mounted on the correct robot drive.

For example, assume you have the following drives in a TLD robot and have the device names configured as follows:

Drive 1: Tape0

Drive 2: Tape1



Drive 3: Tape2

Also assume that in step c you requested that the tape be mounted on Drive 1. If the device name for the drive is correctly configured, the Device Monitor shows the tape mounted on Drive 1. Unload and unmount the tape from Drive 1 using the robotic test utility. Repeat the test for each drive.

During your testing, if the Device Monitor shows the tape mounted on a drive other than the drive you specified in the test utility, the device name for that drive is not correctly configured. For instance, if you mounted a tape on Drive 2 and the Device Monitor shows the tape mounted on Drive 3, the device name for Drive 2 is incorrect. Replace the Drive 2 device name (Tape1) with the correct device name (Tape2) for Drive 3. You may need to use a temporary device name while making these changes. In this case, you also know that the device name for Drive 3 is incorrect. Possibly, the device names were swapped during configuration.

The following point applies only to NetBackup Enterprise Server.

It may be necessary to unload the drive with a command from another host or from the drive's front panel, if the true data path to the drive where the tape was mounted is not on the host with direct robotic control.

On UNIX Hosts

Establish device file to physical drive correlation during installation when you create the device files for each drive. The following is a general procedure:

▼ To correlate device files

1. Determine the physical location of each drive within the robotic library. This is usually shown on the connectors to the drives or in the vendor's documentation.
2. Physically connect the drives to SCSI adapters in your host.
3. Record the adapter and SCSI addresses to which you connected each drive.
4. Create device files for each drive based on the SCSI addresses of the drives and adapters. Add the device file using your notes from step 3 to complete the correlation between device files and physical drive location.
5. Configure the robot and then add the drives.

When you add the drives, check your notes to ensure that you are assigning the correct drive address (for example, robot drive number) to each device path.

6. Optionally, you can use the appropriate robotic test utility to verify the configuration.

- a. Stop the device daemon (`ltid`).
- b. Start `ltid` to start the Automatic Volume Recognition daemon (`avrd`). You must stop and restart `ltid` to ensure that the current device configuration has been activated.

The following point applies only to NetBackup Enterprise Server.

Also start the remote robotic control daemon, if robotic control is not local to this host.

- c. Use the robotic test utility to mount a tape on a drive.
- d. Use the Device Monitor to verify the tape was mounted on the correct robot drive.

For example, assume you have the following drives in a TLD robot and have the device paths configured as follows:

Drive 1: `/dev/rmt/0cbn`

Drive 2: `/dev/rmt/1cbn`

Drive 3: `/dev/rmt/3cbn`

Also assume that in step c you requested that the tape be mounted on Drive 1. If the device path for the drive is correctly configured, the Device Monitor shows the tape mounted on Drive 1. Unload and unmount the tape from Drive 1 using the robotic test utility. Repeat the test for each drive.

During your testing, if the Device Monitor shows the tape mounted on a drive other than the drive you specified in the test utility, the device path for that drive is not correctly configured. For instance, if you mounted a tape on Drive 2 and the Device Monitor shows the tape mounted on Drive 3, the device path for Drive 2 is incorrect. Replace the Drive 2 device path (`/dev/rmt/1cbn`) with the correct device path (`/dev/rmt/3cbn`) for Drive 3. You may need to use a temporary device path while making these changes. In this case, you also know that the device path for Drive 3 is incorrect. Possibly, the device paths were swapped during configuration.

The following point applies only to NetBackup Enterprise Server.

It may be necessary to unload the drive with a command from another host or from the drive's front panel, if the true data path to the drive where the tape was mounted is not on the host with direct robotic control.

Drive Cleaning

This section covers the following topics:

- ◆ “Available Types of Cleaning” on page 310



- ◆ “Reactive Cleaning (TapeAlert)” on page 310
- ◆ “Library-Based Cleaning” on page 312
- ◆ “Frequency-Based Cleaning” on page 312
- ◆ “Operator-Initiated Cleaning” on page 313
- ◆ “Using a Cleaning Tape” on page 314

Available Types of Cleaning

Media Manager has the following types of drive cleaning available:

- ◆ Reactive cleaning (also known as on-demand cleaning or TapeAlert cleaning).
This type of cleaning is the recommended practice. See “Reactive Cleaning (TapeAlert)” on page 310.
- ◆ Library-based cleaning (also known as robotic cleaning or auto cleaning).
This type of cleaning is not supported by Media Manager for most robots, since robotic library and operating systems vendors have implemented this cleaning in many different ways. These different methods often interfere with Media Manager robotic control operations. See “Library-Based Cleaning” on page 312.
- ◆ Frequency-based cleaning.
This type of cleaning occurs when the accumulated mount time exceeds the time you specified for cleaning frequency. See “Frequency-Based Cleaning” on page 312.
- ◆ Operator-initiated cleaning.
This type of cleaning can be performed regardless of the specified cleaning frequency or accumulated mount time. See “Operator-Initiated Cleaning” on page 313.

Reactive Cleaning (TapeAlert)

Reactive cleaning using TapeAlert is mainly a function of the tape drive. The drive determines and initiates the cleaning when needed. If a drive supports the TapeAlert capability and it is enabled on the drive, Media Manager polls the drive for status from TapeAlert.

TapeAlert allows reactive cleaning for most drive types. Not all platforms, robots, and drives, at all firmware levels, support this type of reactive cleaning.

In the cases where TapeAlert is not supported on a particular drive, frequency-based cleaning may be utilized (see “Frequency-Based Cleaning” on page 312 and “TapeAlert and Frequency-Based Cleaning” on page 311).

See the following topics:

- ◆ “Requirements for Using TapeAlert with Media Manager” on page 311
- ◆ “TapeAlert and Media Manager” on page 311
- ◆ “TapeAlert and Frequency-Based Cleaning” on page 311

Requirements for Using TapeAlert with Media Manager

To use TapeAlert, all of the following conditions must be true. No additional configuration is needed.

- ◆ VERITAS must support TapeAlert on the device host platform where the drive is connected.
- ◆ The drive must support the TapeAlert capability and the TapeAlert must be enabled on the drive.

To determine if drives support TapeAlert, see the VERITAS support site for information on drive support for TapeAlert.

- ◆ A cleaning tape is configured and available in Media Manager for the robotic library.
- ◆ The cleaning tape being used has cleanings remaining.
- ◆ Passthru device files must be configured on UNIX media servers (see the Media Manager device configuration guide).

TapeAlert and Media Manager

A drive with TapeAlert capability tracks how many read and write errors it has encountered within a certain time period. Although these errors are recoverable, once a threshold is reached a CLEAN_NOW or CLEAN_PERIODIC flag is set by TapeAlert.

If Media Manager detects that either of these flags is set, it performs a cleaning at *one* of the following times:

- ◆ At the end of a backup or restore to the drive.
- ◆ Prior to the next backup or restore to the drive.

TapeAlert and Frequency-Based Cleaning

Using TapeAlert *with* frequency-based cleaning ensures that a drive will get cleaned at least every *x* hours, depending on the setting for the cleaning frequency. In addition, the drive may be cleaned sooner, if the CLEAN_NOW or CLEAN_PERIODIC TapeAlert flags are set by the drive.



When using TapeAlert *without* frequency-based cleaning, a drive will be cleaned only when the drive sets its CLEAN_NOW or CLEAN_PERIODIC flags.

Library-Based Cleaning

Cleaning media used for library-based cleaning is hidden from Media Manager (that is, cleaning media is not defined in the Media Manager volume database and the media is managed by the robotic library).

Since TapeAlert provides the same type of cleaning as library-based cleaning, VERITAS recommends that you disable library-based cleaning when using TapeAlert.

Frequency-Based Cleaning

When you add a drive or make changes to a drive, you can specify the number of hours (cleaning frequency) that a drive will be used between drive cleanings. Media Manager updates the mount time for the drive each time a tape is unmounted.

If the following conditions are met, drive cleaning occurs when the accumulated mount time exceeds the time you specified for cleaning frequency:

- ◆ The drive is in a robotic library that supports drive cleaning (see “Robot Attributes” on page 279).
- ◆ A cleaning tape is configured and available in Media Manager for the robotic library.
- ◆ The cleaning tape has cleanings remaining.

Media Manager cleans the drive immediately after a tape is unmounted. Drive cleaning never causes an unmount in the middle of an active backup. The mount time is reset after the drive is cleaned. The cleaning frequency value remains the same.

A cleaning can occur within a backup if you are spanning tapes. For example, if cleaning is due after the first tape is full, Media Manager cleans the drive before proceeding to the next tape.

Leaving media in a drive for extended periods does not affect cleaning frequency because Media Manager increments the mount time only when the media is actually assigned to a process.

See the following topics:

- ◆ “Frequency-Based Cleaning Limitations” on page 313
- ◆ “Managing Frequency-Based Cleaning” on page 313

Frequency-Based Cleaning Limitations

Frequency-based cleaning is *not* supported for the following devices.

- ◆ Drives in RSM libraries that are under API robotic control. On Windows operating systems that support RSM robots, the system software controls the drive cleaning. To manage drive cleaning, use the Windows RSM administrative interface.
- ◆ *The following applies only to NetBackup Enterprise Server.*
Drives in ACS, LMF, or TLH libraries that are under API robotic control. The robotic library software controls the drive cleaning. To manage drive cleaning for these robots, use the robot vendor interfaces.
- ◆ *The following applies only to NetBackup Enterprise Server.*
Shared drives, since there is no single device path where tape mounts can be accurately counted.

Check the Drive Cleaning Support Attribute of the tables in “Robot Attributes” on page 279.

Managing Frequency-Based Cleaning

The following procedures use the NetBackup Administration Console to manage drive cleaning. You can also use the `tpclean` command.

- ▼ **To change the cleaning frequency value**
 - ❖ See “Dialog Entries for Adding (or Changing Drives)” on page 62.
- ▼ **To perform an operator-initiated drive cleaning or to reset the mount time for a drive**
 - ❖ See “Drive Cleaning Functions” on page 73.
- ▼ **To change the number of cleanings allowed for a cleaning tape**
 - ❖ See “Changing the Attributes for a Volume” on page 144 for configuration information.

Operator-Initiated Cleaning

You can perform an operator-initiated cleaning of a drive regardless of the cleaning frequency or accumulated mount time of the drive. You can clean standalone drives or robotic drives if a cleaning tape of the correct media type and residence for the drive has been added to the appropriate volume database.



If either of the following conditions are true

- ◆ The value for the mount time is greater than the cleaning frequency.
- ◆ The TapeAlert CLEAN_NOW flag is set.

and either of the following conditions are true

- ◆ The drive is a standalone drive and a cleaning tape is not defined.
- ◆ The drive is a standalone drive and no cleaning tape has any cleanings remaining.

then the message, NEEDS CLEANING, appears in the following displays:

- ◆ The Tape Cleaning Comment column of the Drive List in the **Devices** node of the NetBackup Administration Console.
- ◆ The comment field of the output from the `tpclean -L` command.

▼ To perform an operator-initiated cleaning

- ❖ See “Managing Frequency-Based Cleaning” on page 313.

Using a Cleaning Tape

Note Media Manager has no control over cleaning tapes that are used by library-based cleaning.

You can specify the number of cleanings that are allowed for a cleaning tape. This number is decremented with each cleaning, and when the number of cleanings is zero Media Manager stops using the cleaning tape. At this point, you can use a new cleaning tape or increase the number of cleanings allowed for the tape.

VERITAS suggests following the recommendations from cleaning tape vendors for the amount of tape usage. Using a cleaning tape past its recommended life can cause delays in the cleaning operation (due to excessive tape positioning) and potentially lead to downed drives.

You can change the number of cleanings at any time. See “Managing Frequency-Based Cleaning” on page 313.

Volume Pools and Volume Groups

A volume pool is used to identify a logical set of volumes by usage.

A volume group is a logical grouping that identifies a set of volumes that reside at the same physical location. Volume groups are convenient for updating a configuration when moving volumes (for example, from robotic to standalone).

Volume pools and volume groups are specified when you add the volume to the Media Manager configuration.

See the following topics:

- ◆ “Volume Pools” on page 315
- ◆ “Volume Groups” on page 315
- ◆ “Volume Pool and Volume Group Example” on page 316
- ◆ “Scratch Volume Pools” on page 318
- ◆ “Moving Volumes” on page 320

Volume Pools

The volume pool concept is relevant only for NetBackup storage units managed by Media Manager and does not apply to disk storage units.

Associating volumes with a volume pool protects them from access by unauthorized applications. You can create volume pools for applications or other reasons, and as you add volumes, associate them with the appropriate pool. You can also move unassigned volumes to a different pool later.

With the exception of the NetBackup and DataStore special volume pools, you must create a volume pool before you can add volumes to it. By default, Media Manager creates volume pools, named NetBackup and DataStore.

During initial configuration, it is easiest to create all of your volume pools first if you want to use volume pools other than the NetBackup volume pool. Then as you add volumes, you can assign them to these volume pools.

You can also configure a scratch volume pool (see “Scratch Volume Pools” on page 318).

Volume Groups

Volume groups are an administration tool for logically moving multiple volumes (where a logical move means to change the volume attributes to show the new location).

Using a volume group lets you move a set of volumes between a robotic library and a standalone location, or delete them from the configuration by specifying the group name, rather than each individual media ID of each volume. Volume groups are also convenient for tracking the location of volumes, such as the case when a group is moved off site.



Rules for Assigning Volume Groups

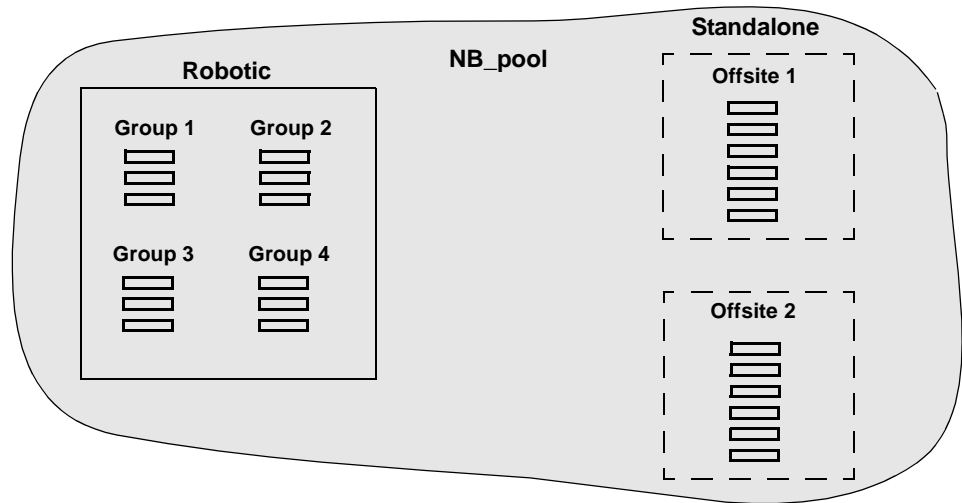
The following are the rules for assigning volume groups:

- ◆ All volumes in a group must be the same media type.
However, a media type and its corresponding cleaning media type are allowed in the same volume group (for example, DLT and DLT_CLN).
- ◆ All volumes in a robotic library *must* belong to a volume group. You cannot add volumes to a robotic library without specifying a group or having Media Manager generate a name for the group.
- ◆ The only way to clear a volume group name is to move the volume to standalone and not specify a volume group.
- ◆ More than one volume group can share the same location. For example, a robotic library can contain volumes from more than one volume group and you can have more than one standalone volume group.
- ◆ All volumes in a group must be in the same robotic library or be standalone. That is, Media Manager will not let you add a group (or part of a group) to a robotic library, if it already exists in another robotic library.

Volume Pool and Volume Group Example

The following figure shows an example with one volume pool (named NB_pool) and several volume groups. In this example, volumes can be moved between the groups in the robotic library and any groups that are off site. All volumes, however, remain in the same pool.

Volume Pool With Multiple Volume Groups

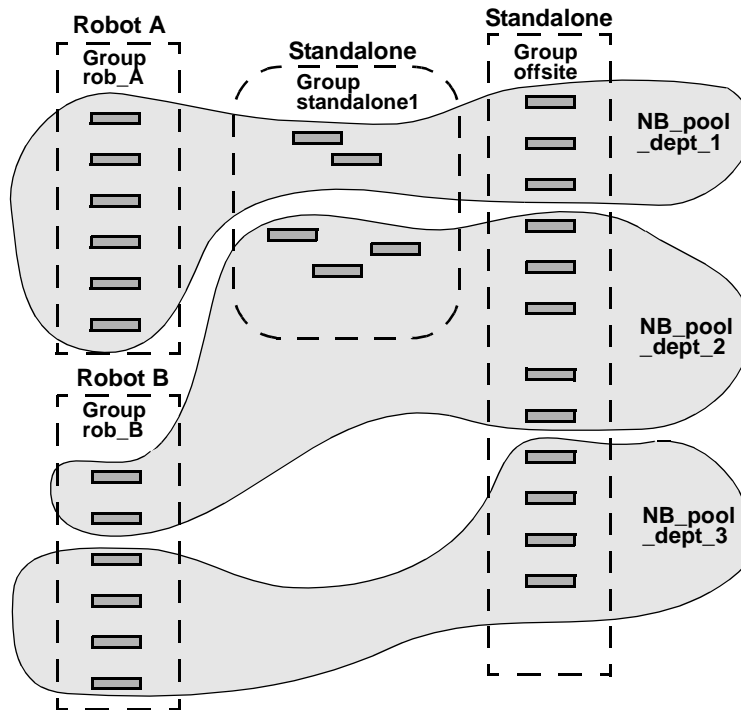


In the following figure, members of the same volume pools are in different volume groups. The important thing to notice in this example is that the data intended for use by different departments is kept on separate volumes by assigning different volume pools. The volumes in a pool can be in more than one physical location and in more than one volume group.

In this example, the volumes in the pool `NB_pool_dept_1` are spread among the `rob_A`, `standalone1`, and `offsite` volume groups. These groups also have volumes from more than one pool (though the volumes in each group must all be the same type).



Volume Groups With Multiple Volume Pools



It is also possible to configure a scratch pool from which Media Manager can transfer volumes when another volume pool has no media available (see “Scratch Volume Pools” on page 318).

Scratch Volume Pools

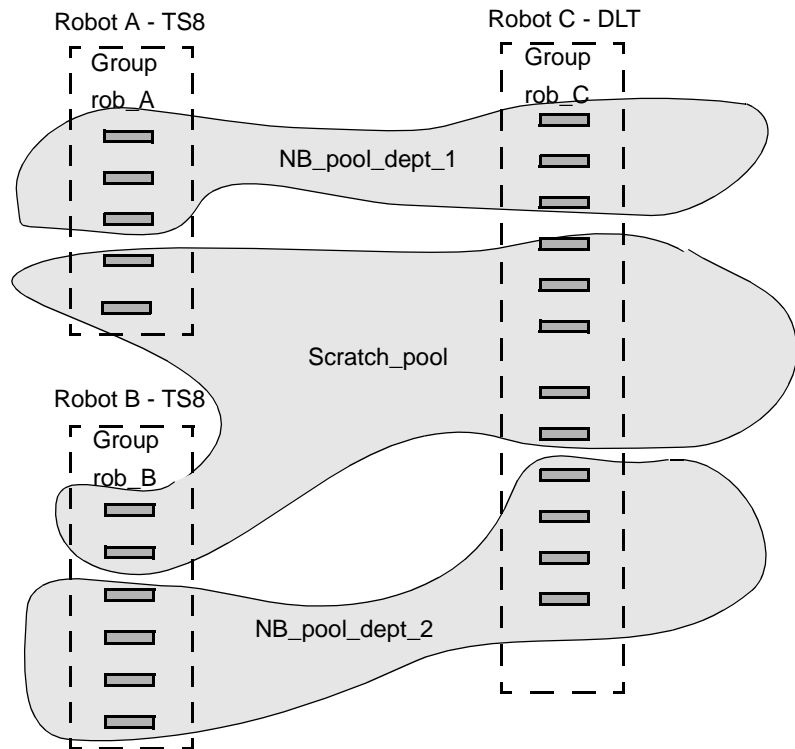
The scratch pool is an optional volume pool that you can configure. Each media server (or SAN media server) in your configuration can have one scratch pool defined. If a scratch pool is configured, Media Manager moves volumes from that scratch pool to other pools that have do not have volumes available.

See “Adding a New Volume Pool or Scratch Volume Pool” on page 109 for configuration information.

Scratch Pool Example

In the following figure, the scratch pool is named `Scratch_pool` and the three robots contain volumes from that pool in addition to those from other pools. Assume the following sequence of events:

- ◆ NetBackup requires a DLT volume, so Media Manager attempts to assign one from NB_pool_dept_1 in Robot C.
- ◆ Robot C has no unassigned volumes available in the NB_pool_dept_1 pool.
- ◆ Media Manager searches the scratch pool for an unassigned DLT volume in Robot C. If there is an available volume, Media Manager moves it to NB_pool_dept_1 and assigns it to NetBackup. Otherwise, a media unavailable status is logged.



Scratch Pool Usage

The following list contains important notes about scratch pool usage:

- ◆ If the scratch pool contains assigned volumes, these volumes remain in the scratch pool. Media Manager does not move assigned volumes to other pools as it does with unassigned volumes.
- ◆ Media Manager will not assign volumes while they are in a scratch pool. For example if a NetBackup policy or schedule specifies the scratch pool, all requests for those volumes are denied.
- ◆ Media Manager returns expired media to the scratch volume pool automatically (media that is returned must have been originally in the same scratch pool).



If this logical move is not desired, you can specify an entry in `vm.conf` to disable this behavior (see “Return Media to the Scratch Pool” on page 371). If this entry is used, the move must be done using **Media and Device Management** from the NetBackup Administration Console.

- ◆ To have Media Manager manage the allocation of your volumes to your volume pools, do the following:
 - a. Create volume pools as required, but do not add any volumes to the pools.
 - b. Define a scratch pool and add all of your volumes to it. Media Manager will move volumes to the other pools as they are needed.

Moving Volumes

Common instances when you move volumes are as follows:

- ◆ Replacing full volumes in a robotic library. When a volume is full and there are no more empty slots in the robotic library, you move the full volume to standalone and configure a volume for the empty slot, or move a volume into that slot. Use the same process to replace a defective volume.
- ◆ Moving volumes from a robotic library to an offsite location or from an offsite location into a robotic library. When you move tapes to an offsite location, you move them to standalone.
- ◆ Moving volumes from one robotic library to another (for example, if a robotic library is down).
- ◆ Changing the volume group for a volume or volumes.

Move Operations

In one move operation, you can move a single volume, multiple volumes, or combinations of single and multiple volumes. You are limited only in that you cannot move volumes to an invalid location (for example, DLT media to an 8 mm robot).

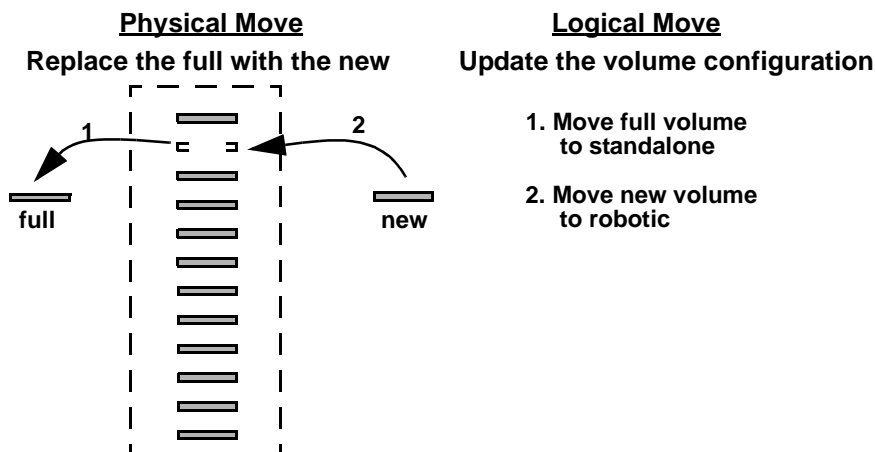
The best practice is to keep your moves simple by selecting and moving only one type of media at a time to a single destination. For example, if you have to move 8 mm and 4 mm cartridge tapes, do it in separate moves.

Physical and Logical Moves

When you move volumes in or out of a robotic library or from one robotic library to another, you must physically and logically move the volume, as follows:

- ◆ The physical part of the move is done when you insert or remove the volume. For some robot types, you can use Media Manager to physically move the volume (using Inject/Eject options).
- ◆ The logical part of the move is done when you use Media Manager to move volumes. Media Manager updates the volume database to show the volume at the *new* location.

The following figure shows an example of replacing a full volume with a new volume.



Barcodes

Reading barcodes on media is a function of the robotic library hardware. When a robotic library has a barcode reader, it scans the media for barcodes and saves the results. The results associate the slot number and the barcode with the media in that slot. Media Manager obtains this association from the robotic library.

See the following topics:

- ◆ “Barcode Advantages” on page 321
- ◆ “Barcode Best Practices” on page 322
- ◆ “Barcode Rules” on page 323
- ◆ “Media ID Generation Rules” on page 325

Barcode Advantages

VERITAS suggests that you use media with barcodes in robots that can read barcodes. Barcodes offer the following advantages:



- ◆ Automatic media ID assignment.

When you add new media to a robot, Media Manager is able to assign media IDs according to the criteria that you specify.

- ◆ More accurate tracking of volume location.

A Robot Inventory Update Volume Configuration operation can determine which volumes are in a robot.

- ◆ Increased performance.

Media Manager functions well whether or not barcodes are used. However, not using barcodes can adversely affect performance for some robots.

A robot that reads barcodes will perform a scan each time it moves a tape. This is normal and is done in order to store the correct barcode in memory or to verify a previously saved barcode. However, if a barcode is missing, the robot will retry the scan multiple times, degrading performance.

Barcode Best Practices

When selecting barcodes for your volumes consider the following important points:

- ◆ Barcodes usually appear on labels that you attach to the outside of tape volumes.
Barcodes are not generally used on optical disks and Media Manager does not support barcodes for optical disk libraries (ODL robots).
- ◆ The maximum barcode lengths that are supported by Media Manager depend on the type of robot. See the Barcode Support attribute of the tables listed in “Robot Attributes” on page 279.
- ◆ When you purchase barcode labels for use with Media Manager, always follow the robotic library vendor’s recommendations. Ensure that the barcodes have the correct number of characters.
- ◆ Barcodes can represent any combination of alpha and numeric characters, but different robots support different lengths of barcodes. See the robot vendor’s documentation to determine the requirements for a specific robot type.
- ◆ Use barcodes without spaces (leading spaces, trailing spaces, or spaces between any characters). Otherwise, the robot or Media Manager can have difficulty interpreting them.
- ◆ Volumes in an API robot have a real or a logical barcode. This volume identifier is used as the Media Manager media ID. This volume identifier is the volume serial number in ACS, LMF, TLH, and TLM robots.

For RSM robots, the last six characters of the media name are used as the volume identifier. If these characters contain spaces, only the characters back to the first space are used.

- ◆ For API robots, the barcode for a volume must be identical to the Media Manager media ID.

You can match barcodes to media IDs by getting custom labels in the same series as your media IDs. For example, to match a set of media IDs from AA0000 to ZZ9999, get barcode labels in that series.

- ◆ When a robotic library can contain more than one media type, a good strategy for assigning barcodes is to assign specific characters in the barcode to different media types using media ID generation rules (see “Media ID Generation Rules” on page 325). Also recommended is to use barcodes to differentiate between data tapes and cleaning tapes, or to differentiate between volume pools.

Barcode Rules

A barcode rule specifies criteria for assigning attributes to new robotic volumes. These attributes are assigned by Media Manager using the barcode for the volume that is returned by the robotic library and your barcode rules.

In Media Manager, you choose whether to use barcode rules when you set up the robot inventory update operation. The barcode rules that are actually used by Media Manager are the rules that are stored on the volume database host that is the target of the robot inventory update operation.

Media Manager Actions for Barcodes

When a robot inventory update operation uses Media Manager barcode rules and a new barcode is detected in a slot, Media Manager searches the list of rules starting at the top and checks for a barcode tag that matches the new barcode. If a tag matches, the media type associated for the rule is checked to ensure that it is compatible with the type you specified for the robot update.

If the media type also matches, Media Manager uses the media type, volume pool, maximum number of mounts (or number of cleanings), and description in the rule when it assigns attributes in the volume database.

Note Media Manager will not use barcode rules for barcodes that are being used by existing volumes.



Example Barcode Rules

The following table shows some sample barcode rules. Rules are sorted first according to the number of characters in the barcode tag and then by the order you add them. Two exceptions are the <NONE> and <DEFAULT> rules, which are always located at the end of the list.

Sample Barcode Rules

Barcode Tag	Media Type	Volume Pool	Max Mounts/ Cleanings	Description
0080	8MM	b_pool	55	new 008 volumes
DLT	DLT	d_pool	200	dlt backup
CLD	DLT_CLN	None	30	dlt cleaning
CLT	8MM_CLN	None	20	8 mm cleaning
TS8	8MM	t_pool	0	8 mm backup
TS	8MM	None	0	8 mm no pool
<NONE>	DEFAULT	None	0	no barcode
<DEFAULT>	DEFAULT	NetBackup	0	other barcodes

Refer to the previous table showing sample barcode rules for the following examples.

Assume that you select the following media settings (update options) for the update operation for a new 8-mm volume in a TS8 robot:

Media Type = 8MM

Volume Group = 00_000_TS8

Use Barcode Rules = YES

Volume Pool = DEFAULT

If a new volume in this robotic library has a barcode of TS800001, Media Manager uses the rule with the barcode tag of TS8 and assigns the following attributes for the volume:

Media ID = 800001 (last six characters of barcode)

Volume Group = 00_000_TS8

Volume Pool = t_pool



Max Mounts = 0 (no maximum)

If a new volume has a barcode of TS000001, Media Manager uses the rule with the barcode tag of TS and assigns the following attributes for the volume:

Media ID = 000001 (last six characters of barcode)

Volume Group = 00_000_TS8

Volume Pool = None

Max Mounts = 0 (no maximum)

Media ID Generation Rules

Note To use media ID generation rules, the robot must support barcodes and the robot cannot be an API robot. Media ID generation rules are saved in the Media Manager configuration file (`vm.conf`).

Using media ID generation rules allows you to override the default media ID naming method used by Media Manager. The default method uses the last six characters of the barcode returned by the robot to generate the Media Manager media ID.

For example, two eight-character barcodes might be S00006L1 and 000006L1. If you do not specify any media ID generation rules, Media Manager uses the last six characters of the barcode to generate its media IDs. In this example, the same media ID for the two barcodes would be created (0006L1).

You can control how media IDs are created by defining media ID generation rules that specify which characters of a barcode on tape will be used in the media ID. You also can specify that alphanumeric characters are to be inserted into the ID.

Rules can be defined with respect to a robot and barcode lengths. Multiple barcode creation entries can be specified, allowing the ID generation to be specific for each robot; or for each barcode format having different numbers of characters in the barcode. This allows flexibility for multi-media.

Using the Physical Inventory Utility for Non-Barcoded Media

A Media Manager robot inventory update is the automated operation of determining the location/slot of all media in the robotic library and updating the Media Manager volume database to synchronize it with the contents of the robotic library. A robotic inventory update, when invoked in any of the Media Manager interfaces, utilizes the `vmupdate` command to perform its functions.



`vmupdate` connects to the robotic control daemon and obtains a list of media known to the library. For robotic libraries having barcode readers and containing bar-coded media, the robotic inventory information is used for tracking the location of media, as `vmupdate` queries the volume database for its media information, and appropriately updates the volume database to match its contents to that of the robotic library.

See the following topics:

- ◆ “Why Use `vmphyinv`?” on page 326
- ◆ “When to Use `vmphyinv`” on page 327
- ◆ “How `vmphyinv` Performs a Physical Inventory” on page 328

Why Use `vmphyinv`?

For robotic libraries without barcode readers or libraries containing non-bar-coded media, only the presence of media in a robotic library slot is obtained. This information alone is not sufficient to perform automated media management. More information must be obtained. For non-barcoded media, it is necessary to mount the tape, read the tape header and determine which tape is in each slot.

The physical inventory utility, `vmphyinv`, performs a physical inventory on non-barcoded tape libraries by mounting the tape, reading the tape header, identifying the tape in each slot, and updating the Media Manager volume database.

For the complete syntax for the `vmphyinv` command, see `vmphyinv` in the NetBackup commands for UNIX or the NetBackup commands for Windows reference guides.

Features

`vmphyinv` has the following features:

- ◆ Can be invoked from any master or media server (or SAN media server).
- ◆ Can be used with barcoded tape libraries, because of the utility’s value in verifying the contents of the media.
- ◆ Recognizes NetBackup, Backup Exec, and Storage Migrator (VSM) tape formats.
- ◆ Supports remote administration. You do not need to invoke `vmphyinv` from the host where the drives are attached.
- ◆ Tries to use multiple drives in a robot, even if the drives are attached to different hosts.
- ◆ *The following applies only to NetBackup Enterprise Server.*
Works with shared drives (Shared Storage Option).
- ◆ Supports all SCSI-based robot types (except optical disk libraries).

- ◆ Can be used to inventory a single piece of media, in a standalone drive. The drive can be selected for inventory by specifying the `-u device_number` or `-n drive_name` option. The drive must contain media and it must be ready.

Requirements and Restrictions

`vmphyinv` has the following requirements and restrictions:

- ◆ At least one master or media server (host where the drives are attached) must be running NetBackup 4.5 FP3 or higher.

If the master server is at NetBackup 4.5 FP3 or higher and one or more media servers are at 4.5, the utility detects the version of all media servers and only performs inventories on hosts that are at the 4.5 FP3 or higher level. If some of the drives are attached to servers that are not at the 4.5 FP3 or higher level, those drives are not used for mounting media.

If none of the media servers are at the required level, the utility will not be able to perform the inventory operation and an error message is displayed.
- ◆ If the master or media server (or SAN media server) for a robot that is being inventoried is at NetBackup 4.5 FP3 or higher, then the volume database host for that robot must also be at 4.5 FP3 or higher.
- ◆ The Media Manager Global Device Database must be current before running the physical inventory utility.
- ◆ There is no way to distinguish between volume records based on the application type.
- ◆ When moving the media from robotic to standalone drives there is no option to move the media to a specific volume group.
- ◆ API robot types and optical disk library (ODL) robot types are not supported.

When to Use `vmphyinv`

This utility can be used to update the Media Manager volume database for NetBackup, Backup Exec, and Storage Migrator media. You can use `vmphyinv` in the following typical cases:

- ◆ You inserted new media into the robotic library and there are no Media Manager volume records corresponding to the media. Do one of the following actions.

It is not recommended to use a robot inventory update action for non-barcoded media unless it is the initial population of the volume database. For non-barcoded media, the second action is the recommended way to inventory the robot.



- a. Add volume records to the Media Manager volume database. This can be done using the Add Volumes or Robot Inventory Update interfaces. After the volume records are added, you can use `vmphyinv` to physically inventory the robot specifying only the robot number.

or

- b. Use the slot range or list option of `vmphyinv` to perform the inventory operation. You do not need to add volume records to the Media Manager volume database.
- ◆ Some of the media are misplaced and the Media Manager volume database does not reflect the correct physical location of these media.

In these cases, you can inventory the whole robot or choose to inventory a subset of media in the robot with options in `vmphyinv`.

- ◆ Media with unknown media IDs or GUIDs are inserted into the robot.

For example, you insert 10 media from a different tape library in slots 11 to 20 and you do not know the media IDs on the tapes. One method to inventory only these 10 media follows:

- a. Add volume records to the Media Manager volume database for these slots (you can use any media ID in this case).
- b. Move all the media to a separate volume pool, for example, `inv_pool`
- c. Run `vmphyinv` specifying the pool name as `inv_pool`. Only the 10 media belonging to this volume pool are inventoried.

A better way to inventory these 10 media is to specify a slot list/range in `vmphyinv`. When used with a slot list/range option, `vmphyinv` mounts the media using the slot information. When the tape header is read, the media ID can be determined. This media ID is used to add a Media Manager volume record. This method avoids unnecessary proliferation of media IDs like those added in step a.

How `vmphyinv` Performs a Physical Inventory

For a physical inventory, this utility performs the following sequence of operations:

1. Obtaining a List of Drives Used to Mount the Media
2. Obtaining a List of Media to be Mounted
3. Mounting Media and Reading the Tape Header
4. Updating the Media Manager Volume Database

Obtaining a List of Drives Used to Mount the Media

The drives obtained need not be locally configured. The list of drives is obtained from the global device database. If the device host is specified using the `-h` option, then that device host is used to obtain the global device database. If the `-h` option is not specified, then the current host is used to obtain the database.

You can control the number of drives used by the utility by specifying the `-drv_cnt` *drive_count* option. Though the specific drives to be used for physical inventory cannot be identified, the maximum number of drives that can be used for physical inventory can be specified. This allows you to reserve drives for NetBackup back up or restore operations.

Obtaining a List of Media to be Mounted

`vmphyinv` allows the following choices for specifying the media to be mounted:

- ◆ Specify a Media Manager robot number

Media Manager volume records must be present when using `vmphyinv` with this option. For example, if `vmphyinv` is called with `-rn robot_number`, there must be Media Manager records corresponding to the robot number in the Media Manager volume database for the robot. `vmphyinv` obtains a list of Media Manager volume records belonging to that robot and inventories each of the media in the list.

- ◆ Specify a Media Manager robot number with filtering options

Inventoring all the media in the robot may not be desired. You can specify a subset of all the media in the robot using filtering options like volume pool, volume group, or slot range. Media Manager volume records must be present when using `vmphyinv` with these options. The following are some examples:

Options Specified	Media Inventoried
<code>-rn 4 -pn bear</code>	Only media corresponding to robot 4 and in the volume pool bear.
<code>-rn 2 -v moon</code>	Media corresponding to robot 2 and in the volume group moon.
<code>-rn 1 -rc1 2 -number 3</code>	Only media corresponding to robot 1 and slot range 2 to 4.
<code>-rn 5 -pn NetBackup -v mars -rc1 2 -number 6</code>	Only media corresponding to robot 5, slot range 2 to 7, and also in volume group mars and the NetBackup volume pool.



- ◆ Specify a Media Manager robot number and a list of media belonging to a specific robot. Media Manager volume records must be present in the Media Manager volume database when specifying this option.

For example, if the `-rn robot_number` and `-ml A00001:A00002:A00003` options are specified, only the three media specified are inventoried. But if any of these media do not belong to the specified robot, the media is skipped and is not inventoried.

- ◆ Specify a Media Manager robot number and a slot range or list.
- Sometimes, media from a different robot or some other different source is moved to a robot and the media ID on the tape is unknown. In these cases, you can specify a slot range and/or list option. With these options, the Media Manager volume record does not need to be present in the volume database, but you must specify the density (using the `-d` option) when using these options.

Note For a robot that supports multi-media, you should carefully specify the density. If the wrong density is specified, `vmphyinv` cannot complete the mount and a wrong density can affect the physical drive (permanent hardware failure may occur).

The following table shows some examples:

Options Specified	Media Inventoried
<code>-rn 1 -slot_range 2 10 -d dlt</code>	Only media in the slot range 2 to 10 in robot 1.
<code>-rn 0 -slot_list 3:4:5 -d 8mm</code>	Only media in slots 3, 4, and 5 in robot 0.
<code>-rn 2 -slot_range 2 4 -slot_list 5:6:7 -d dlt</code>	Only media in slots 2, 3, 4, 5, 6, and 7 in robot 2.

Mounting Media and Reading the Tape Header

The following sequence of operations explains the mount process that is used:

1. `vmphyinv` contacts the Media Manager volume daemon or process, `vmd`, on the local host or remote host depending on where the drive is attached.
2. `vmd` starts `opr`.
3. `vmphyinv` communicates with `opr` and sends the mount request to `opr`. After receiving the request, `opr` issues a mount request to `ltid`.

Note The default mount timeout is 15 minutes, but it can be changed by specifying a different mount time in seconds using the `-mount_timeout` option.

Handling Media That is not Recognized

`vmphyinv` reads the tape header to determine the recorded media ID or GUID.

If the media is *not* NetBackup media, Backup Exec media, or Storage Migrator media, the media is unmounted and the next media is mounted. In these cases, `vmphyinv` will not generate a new record in the volume database. If you want to generate volume records for the media, you should run `vmupdate` to update the Media Manager volume database.

Handling Cleaning Media

If the following cases are *all* true, `vmphyinv` will not attempt to mount the media. The cleaning media is skipped and the next media in the list will be mounted.

- ◆ `vmphyinv` is *not* used with the slot range or list options.
- ◆ There is cleaning media in the robot.
- ◆ The media type is specified as cleaning media in the volume record (for example, `4mm_clean` or `dlt_clean`).

If there is cleaning media in the robot and *any* of the following cases are true, then the utility will try to determine if the media is cleaning media.

- ◆ `vmphyinv` is used with the slot range or list options, and the media type of the corresponding volume record that is found is not a cleaning media type.
- ◆ `vmphyinv` is used with the slot range or list options, and there is no volume record in the Media Manager volume database corresponding to the cleaning media.
- ◆ `vmphyinv` is *not* used with the slot range or list options, and the media type of the corresponding volume record that is found is not a cleaning media type.

`vmphyinv` tries to determine if the media is cleaning media based on the SCSI parameters (sense keys, tape alert flags, and physical (SCSI) media types) returned by the robot. If `vmphyinv` cannot determine if the media is cleaning media, it will continuously try to mount the media until the mount request times out.

Note It may not be possible for Media Manager to detect the presence of cleaning media for all drive types. Some drives do not report the presence of cleaning media in a manner usable by Media Manager.



Updating the Media Manager Volume Database

After all the media are mounted and the tape header is read, a list of recommended changes is generated and displayed. You can accept or reject the suggested changes. If you accept the changes, the changes are applied and the Media Manager volume database is updated. Until then the volume database remains unchanged.

Using the Verbose Option

You can specify the `-verbose` option to display summary information for the suggested changes. For example, how many drives are available, the contents of each tape, if the media is a catalog tape, and so on. (The media format column of the summary contains *NetBackup database* for NetBackup catalog tapes.)

This media format summary is written to `stderr`. You can redirect `stderr` to a file to obtain the media format summary.

Update Principles

`vmphyinv` updates databases depending on the media type found and based on the following principles:

- ◆ This utility never changes the volume pool, media type, and ADAMM_GUID of an assigned record.
- ◆ This utility conditionally changes the media type of an unassigned volume record. The media type is changed only if the new media type belongs to the same family of media types as the old media type. For example, the media type DLT can only be changed to DLT2 or DLT3.
- ◆ This utility never unassigns an assigned Media Manager record.
- ◆ This utility changes the residence and description field of any Media Manager record if required, regardless of whether it is assigned or not. The description field is changed only if the media is Backup Exec or Storage Migrator media.

Updating When the Media is Determined to be NetBackup Media

`vmphyinv` searches the Media Manager volume database checking if the media ID from the tape is present in the media ID field of any record of the Media Manager volume database.

Media ID Present?	Action
Yes	<code>vmphyinv</code> updates the Media Manager volume record having the media ID accordingly.

Media ID Present?	Action
No	<code>vmphyinv</code> creates a new Media Manager volume record corresponding to the NetBackup media.

Updating When the Media is Determined to be Backup Exec Media

`vmphyinv` searches the Media Manager volume database checking if the media GUID from the tape is present in the ADAMM_GUID field of any record of the Media Manager volume database.

Media GUID Present?	Action
Yes	<code>vmphyinv</code> updates the Media Manager record having the GUID accordingly.
No	<code>vmphyinv</code> creates a new Media Manager record corresponding to the Backup Exec media and updates the volume record. <code>vmphyinv</code> may use an existing record if the record does not correspond to any media in the tape library.

Note The NetBackup media database is updated only for Backup Exec media.

For each Media Manager volume record (updated or added), `vmphyinv` does the following operations:

- ◆ In the Media Manager record, the ADAMM_GUID field is updated with the GUID and the Description field is updated with the Backup Exec cartridge label read off the tape header.
- ◆ The media ID of the Media Manager record (added or updated) is added to the NetBackup media database (if not already present). Each record is assigned to NetBackup (if not already assigned) and its state is set to FROZEN in the NetBackup media database. (Each NetBackup master or media server has a media database that is distinctly separate from the Media Manager volume database.)

The volume pool of the unassigned Media Manager volume records associated with Backup Exec media is changed to the BackupExec pool. If the BackupExec pool is not present, it is created.

Note If a MEDIA_ID_PREFIX entry is not specified in the Media Manager configuration file (`vm.conf`), BE is the default prefix used for Backup Exec media.



Updating When the Media is Determined to be Storage Migrator for Windows Media

vmphyinv searches the Media Manager volume database checking if the media GUID from the tape is present in the ADAMM_GUID field of any record of the volume database.

Media GUID Present?	Action
Yes	vmphyinv updates the Media Manager record having the GUID accordingly.
No	vmphyinv creates a new Media Manager record corresponding to the Storage Migrator for Windows media and updates the volume record. vmphyinv may use an existing record if the record does not correspond to any media in the tape library.

For each Media Manager volume record (added or updated), vmphyinv does the following:

- ◆ In the Media Manager record, the ADAMM_GUID field is updated with the GUID and the Description field is updated with the Storage Migrator cartridge label read off the tape header.
- ◆ The volume pool of the unassigned Media Manager records associated with Storage Migrator for Windows media is changed to the StorageMigrator pool. If the StorageMigrator pool is not present, it is created.

Note If a MEDIA_ID_PREFIX entry is not specified in the Media Manager configuration file (vm.conf), RS is the default prefix used for Storage Migrator for Windows media.

The Storage Migrator database is not updated.

Handling Error Cases

vmphyinv may not be able to update the Media Manager volume database correctly in the following cases and these cases are reported as errors. If any of the following cases are encountered, manual intervention is required to proceed.

- ◆ Duplicate media IDs are found. Two or more media in the same robot have the same media ID.
- ◆ A Media Manager volume record belonging to a different robot is found, with the same media ID as the media ID read from the tape header.
- ◆ The media type, media GUID, or volume pool of an assigned volume record needs to be changed.

- ◆ The barcode of an existing volume record needs to be changed.

Making Changes to Your Hardware Configuration

The following are advanced topics for changing an existing NetBackup configuration:

- ◆ “Replacing Devices in a SSO Configuration” on page 335.
- ◆ “Decommissioning a Media Server” on page 336.

Replacing Devices in a SSO Configuration

This is a NetBackup Enterprise Server topic.

If you replace an existing device in your shared drive configuration with a new device, the serial number of the device will likely change. This change can lead to a wrong configuration in Media Manager of the global device database and also the local device databases on each server.

▼ To reconfigure the Media Manager device databases after replacing a device

Note The `tpautoconf` options used in this procedure are available only with NetBackup release 5.0 or later.
Media servers that are also robot control hosts, must be running NetBackup release 5.0 or later to use this procedure.

1. Configure the new device on all servers sharing the device. The device must be available through the operating system of each server.

This device configuration may require remapping, rediscovery, and possibly a reboot of the operating system (refer to the *NetBackup Media Manager Device Configuration Guide* for more information).

2. On a server running NetBackup release 5.0 or later, run `tpautoconf -report_disc` on one of the reconfigured servers to produce a list of new and missing hardware. This command will scan for new hardware, and produce a report showing the new and the replaced hardware.
3. Ensure that all servers that are sharing the new hardware are up and are running NetBackup services.



4. On a server running NetBackup release 5.0 or later, run `tpautoconf` with the `-replace_drive drive_name` or `-replace_robot robot_number` option. Also specify the `-path hardware_path` option. *hardware_path* is the new hardware path, as shown in the output of the report created in step 2.

The serial number is read from the new hardware device and the Media Manager global data base is updated. Also any servers (running NetBackup release 5.0 or later) sharing the new device will replace the serial number in their local databases.

5. If the new device is a drive, run the device configuration wizard on all servers that are sharing the drive.

If the new device is a robot, run the wizard on the server that is the robot control host and on all servers that are running any version of NetBackup 4.5.

Decommissioning a Media Server

This is a NetBackup Enterprise Server topic.

Several steps must be accomplished to decommission a media server and remove it from a NetBackup configuration. If all of the steps are not completed, any later restores will have to be performed by importing the tapes, which is a much longer process.

Note If you are using NetBackup Vault and plan to decommission a media server, it is recommended that you contact VERITAS Consulting for help with this task.

▼ To decommission a media server

In the following procedure the media server that is being decommissioned is referred to as the *old_server* and the new media server as *new_server*.

Refer to the NetBackup system administrator's guide for more information for the steps involving configuring NetBackup.

1. Run the `bpmedialist` command to determine which tapes on the *old_server* have NetBackup images that have not expired (the `-l` option produces one line of output per tape).

```
bpmedialist -mlist -l -h old_server
```

2. Select another server or the master server (*new_server*) to manage the tapes from the *old_server*.

Run the `bpmedia` command for each tape that has active images as identified in step 1. This updates the NetBackup media database files on the *old_server* and the *new_server*, and updates the images database on the master server. (Media database files are binary files that can only be updated by `bpmedialist`.)

```
bpmedia -movedb -ev media_ID -oldserver old_server
        -newserver new_server
```

3. Add the following command to the end of the `bp.conf` file on the master server to allow restores to occur from a media server other than the server that performed the original backups. *old_server* is the media server that performed the original backups and *new_server* is the server that will be used for future NetBackup restores (see step 2).

```
FORCE_RESTORE_MEDIA_SERVER = old_server new_server
```

4. Use the Media and Device Management GUI to move the tapes that are in robots attached to the *old_server* to non-robotic status (standalone). Select each robot attached to the *old_server*, highlight all of the tapes, and move them to standalone.

See “Moving Volumes” on page 130.

5. Use the Media and Device Management GUI to delete the drives and then the robots from the *old_server*.

See “Managing Your Device Configuration” on page 68.

6. Use the Storage Unit Management GUI to delete all storage units associated with robots that are associated with the *old_server*.

7. If any robots from the *old_server* will be reused on other media servers, do the following steps:

- a. Power down the affected servers and make any cabling changes required to physically attach the robots to the new media servers. Verify that the robots are recognized by the operating system on the new media servers.

- b. Use the Media and Device Management GUI to add the robots and drives to those media servers.

See “Adding Robots” on page 46 and “Adding Drives” on page 60.

- c. Use the Storage Unit Management GUI to create the appropriate NetBackup storage units.

- d. Use the Media and Device Management GUI to inventory the robots attached to the *new_server*. This will update the location of all tapes in these robots.

8. Modify any classes that explicitly specified any of the storage units on the *old_server*. These classes must be changed to point to any other defined storage units in the NetBackup configuration or to Any Available, as appropriate.



9. Update the `bp.conf` and `vm.conf` files (or their equivalent on Windows servers) on the master server and all media servers in the NetBackup configuration to remove any reference to the *old_server*.
10. Update the server list on all clients to no longer refer to the *old_server*. Restart the NetBackup daemons (or services) on any system where these files are modified.

Labeling Media

You normally do not have to label media.

For a robotic library, you select the media IDs when you configure the media in Media Manager and tape labeling is done automatically when NetBackup uses the media. For optical media, you have the option of formatting and labeling when you add the media to the robot. Or, you can do it manually with the Media Manager `tpformat` command.

For standalone drives, the standalone drive extension feature makes it unnecessary to label media in a standalone drive. You can, however, pre-label tapes by using the `bplabel` command.

Automatic labeling does not occur if the media was last used for NetBackup catalog backups. It also does not occur if the media contains data from a recognized non-NetBackup application and you are not using the NetBackup Media host property, **Allow Media Overwrite**. In either of these instances, you must label the media by using the `bplabel` command.

Pre-labeling of Media

It may be beneficial to pre-label your media for the following reasons:

- ◆ Writing a label validates that the media is usable, compatible, and is not write-protected.
- ◆ The recorded label may assist with media management in the cases where the media is misplaced, or the barcode or external label is missing or damaged.

Mounting and Unmounting of Media

For robots, Media Manager automatically mounts and unmounts the volume. Operator intervention is usually required only if the required volume is not in the robot.

For example, if a restore requires a volume that has been removed from a robot (or is offsite), the Device Monitor will display a mount request. The operator can then locate and insert the proper volume and resubmit the request using the Device Monitor.

Suspending Media Or Downing Devices

NetBackup can automatically suspend the use of volumes, or down a device if it suspects failures are due to the volume or the device. The reason for the action is logged in the NetBackup error catalog (viewable in the Media Logs report or the All Log Entries report). If Media Manager downs a device it is logged in the system log.

Repeated write failures are usually the cause for setting a volume to the SUSPENDED state or a device to DOWN. A volume is also set to SUSPENDED if the write failure occurs in such a way that could make future attempts at positioning unreliable. Write failures are frequently caused by a tape device with dirty write heads or deteriorating media.

▼ To reverse a suspend or down action

1. Use the `bpmmedia` command to unsuspend the volume.
2. Use the NetBackup Device Monitor to set the device to Up.

How Media Manager Selects a Drive for a Robotic Mount Request

When a robotic mount request is issued, `ltid` queries `vmd` on the volume database host(s) for the media ID that was specified. If the media ID is found, `vmd` returns the location of the media (which robotic library and the storage slot number, if applicable).

If a drive exists that meets the following criteria, the mount request is forwarded to the appropriate robotic process.

- ◆ The drive is configured.
- ◆ The drive is in the robotic library that contains the media.
- ◆ The drive allows the requested media density.

A robotic process manages the drives and requests for locally-attached or shared drives in the robotic library that contains the requested media. The process (for example, `tldd`) does the following:

1. Determines which of the drives are currently available. Is the drive
 - ◆ Configured as DOWN?
 - ◆ Already assigned?
 - ◆ Of a compatible type?
 - ◆ *The following applies only to NetBackup Enterprise Server.*



Reserved by another host?

2. Picks the drive that was used least recently.

The time stamp used by drive selection is contained in robotic process memory. This stamp is based on the dismount time, *not* the mount time. The first drive in the drive configuration as shown by `tpconfig -d` will be used first, then the second drive, and so on. If the robotic process is stopped and restarted, the drive time stamps are all reset.

The following point applies only to NetBackup Enterprise Server.

When selecting drives among a set of drives, and some of the drives are shared (SSO option) and some are not, a non-shared drive is chosen first (if one is available). This is so the shared drives can be used on other hosts that are sharing the drives.

Controlling Hardware Compression

NetBackup tries to turn on hardware compression on all tape drives that support compression. To disable compression, create a file named `install_path\Volmgr\NO_COMPRESSION`. If this file exists, NetBackup disables hardware compression for all tape drives that it uses.

How NetBackup Selects Media in Robots

When NetBackup selects a volume in a robot, it proceeds as follows:

1. NetBackup searches the media catalog for a volume that is already mounted in a drive and which meets the following criteria:
 - ◆ Configured to contain backups at the retention level required by the schedule (unless the NetBackup Media host property, **Allow Multiple Retentions per Media** is specified for the server).
 - ◆ In the volume pool required by the backup that is being performed.
 - ◆ Not in a FULL, FROZEN, IMPORTED, or SUSPENDED state.
 - ◆ Of the same density required by the requested backup and, in the case of a robotic storage unit, in the robot requested by the backup.
 - ◆ Not currently in use by another backup or a restore.
 - ◆ Not written in a protected format. This is detected after the volume is mounted. If the volume is in a protected format, it is unmounted and NetBackup resumes the search.

2. If NetBackup cannot find a mounted volume that satisfies all of the conditions in step 1, it checks its media catalog for any volume that is suitable.
3. If the media catalog does not have a suitable volume, NetBackup requests Media Manager to assign one. Also, if a volume is at EOM (end of media), NetBackup will request a new volume. This may happen even if the volume is not completely full (because NetBackup received an EOM message from the drive).

Media Manager assigns a volume to NetBackup that meets all of the following criteria:

- ◆ Is the correct media type.
 - ◆ Is for the correct robot type (if applicable).
 - ◆ Is located in the requested robotic peripheral (if applicable).
 - ◆ Resides on the requested host.
 - ◆ Is in the correct volume pool.
 - ◆ Is not currently assigned (not already allocated to NetBackup).
 - ◆ Is not expired (if an expiration date is defined in Media Manager).
 - ◆ Has not exceeded the maximum number of mounts allowed.
4. If more than one volume qualifies, Media Manager chooses the volume that was least recently used. NetBackup then adds it to the media catalog and assigns it the specified retention level.
 5. If there are no unassigned volumes of the requested type, the backup terminates with an error indicating that there was no available media.

Spanning Media

After an end of media (EOM) condition is reached, automatic media selection is a special case and depends on whether NetBackup is configured to allow backups to span media, as follows:

- ◆ NetBackup spans media if the NetBackup Media host property **Allow Backups to Span Media** is specified for the server. In this case, NetBackup uses another volume to start the next fragment and the resulting backup is composed of fragments on different volumes.
- ◆ NetBackup does *not* span media if **Allow Backups to Span Media** is not specified. In this case, the backup terminates abnormally and the operation is retried according to the NetBackup Global Attributes host property, **Schedule Backup Attempts**.



How NetBackup Selects Media in Standalone Drives

The section explains media selection and other aspects of standalone drive operations.

Media Selection Using Standalone Drive Extensions

When the standalone drive extensions capability is enabled, NetBackup tries to use any labeled or unlabeled media that is in a standalone drive. This capability is enabled by default during installation. The media selection process is as follows:

1. If a backup is requested and an appropriate standalone drive does not contain a volume, NetBackup selects a volume as explained in “How NetBackup Selects Media in Robots” on page 340.

The Device Monitor shows the mount request; and an operator must manually insert the volume and assign it to a drive.

2. If an appropriate drive contains a volume, NetBackup tries to select and use that volume.

A volume that has been previously used for backups must meet the following criteria:

- ◆ Not be FULL, FROZEN, or SUSPENDED.
- ◆ Be at the same retention level and in the same volume pool as the backup being performed, unless you specify the NetBackup property **Allow Multiple Retentions per Media** for the server.

Previously unused media is used by NetBackup. If the media is unlabeled, the following actions occur:

1. NetBackup labels the media.
2. Media Manager adds a media ID to the volume configuration, if necessary. If a media ID is added, the NetBackup media ID prefix is used as the first characters of the media ID.
3. If a media ID prefix is not specified, the default prefix is the letter A. For example, A00000.
4. Media Manager adds the requested volume pool to the volume configuration (if the backup policy specifies a volume pool).

If the unused media is unlabeled, you can label it by using the `bplabel` command. When using this command, you can specify the `-u` parameter in order to force assignment of a specific drive index. This eliminates the need to manually assign the drive.

Disabling Standalone Drive Extensions

You can disable the standalone drive extensions by clearing the NetBackup Media host property check box, **Enable Standalone Drive Extensions**, for the server. Clearing this property causes NetBackup to use the same method to select media for standalone drives as it uses for robotic drives.

Spanning Media

Media selection following an end of media condition is a special case and depends on whether NetBackup is configured to allow backups to span media, as follows:

- ◆ NetBackup spans media if the Media host property, **Allow Backups to Span Media**, is specified for the server. In this case, NetBackup selects another volume to begin the next fragment and the resulting backup has data fragments on more than one volume.
 - a. Following an end of media condition, NetBackup first attempts to use an unassigned volume rather than one that already has images on it, and requests Media Manager to assign one. Media Manager checks its volume database for a volume that is the correct media type, in the correct volume pool, and so on.
 - b. If Media Manager cannot find a suitable volume, NetBackup selects one from its media catalog.
 - c. In either case, the Device Monitor displays the mount request and an operator must manually insert the volume and assign it to the drive.
- ◆ NetBackup does not span media if **Allow Backups to Span Media** is not specified. In this case, the backup terminates abnormally when the end of media is reached and the operation is rescheduled according to the Global Attributes host property, **Schedule Backup Attempts**.

When spanning media and an end of media is encountered on a standalone drive that uses a gravity feed stacker (a stacker that is not controlled by software), you can direct NetBackup to continue on the next volume loaded by the stacker, rather than looking for another drive.

To do this, specify the Media host property, **Media Request Delay**, for the server. This property specifies the number of seconds for NetBackup to pause before looking for another drive. When using a standalone drive without a stacker, **Media Request Delay** can be set to allow enough time for the operator to insert the desired volume.



Keeping Standalone Drives in the Ready State

To leave standalone drives in a ready condition after a backup or restore completes, use the `DO_NOT_EJECT_STANDALONE` entry in the `vm.conf` file. See “The Media Manager Configuration File (`vm.conf`)” on page 355.

When NetBackup detects this entry, it prevents Media Manager from ejecting the tape after an operation completes. The tape is ejected if end of media (EOM) is reached.

It is possible for more than one standalone drive to be ready and contain suitable media. If this occurs, the drive selection occurs in logical drive index number order. For example, if drives 2 and 3 are the same type and both contain suitable media, NetBackup selects drive 2.

Media Formats

NetBackup writes media in a format that allows the position to be verified before appending new backups. The format for tape and optical media differ slightly due to characteristics of the media itself.

To determine the contents of tape or optical media, use the Media Contents report. For optical media, the offsets and sizes are shown, along with the backup ID. For tape media, the file number is shown.

The following symbols are used in the media format descriptions that follow.

Symbol	Description
MH	Media Header (1024 bytes).
*	Tape mark.
BH	Backup Header (1024 bytes).
BH1 ... BHn	Backup Headers (1024 bytes). One for each job that is part of the set of jobs being multiplexed
Image	Data from the backup.
EH	Empty Backup Header, used for position validation.

Non-QIC Tape Format

For all tape media except QIC, the format for backups that are not multiplexed is as follows:

MH * BH Image * BH Image * BH Image * EH *

When adding a new backup image, the tape is positioned to the EH and the position is verified. The EH is overwritten by a BH and the backup proceeds. When complete, a new EH is written for future positioning validation.

When NetBackup encounters the end of media during a write, it terminates the tape with two tape marks and does not write an EH.

QIC Tape Format

For QIC tape media, NetBackup does not write empty backup headers (EH). The format of nonmultiplexed backups is as follows:

MH * BH Image * BH Image * BH Image . . .

To append backup images to QIC media, NetBackup positions to the end of data (EOD) and then starts the next backup.

Optical Media Format

For optical media, the format is as follows:

MH BH Image EH BH Image EH BH Image EH

Note Optical disk media have no tape marks to delimit backups. The data on an optical disk is recorded in successive sectors. Since optical disks can seek to a random position, finding and verifying a position is a fast operation.

Fragmented Backups

For fragmented backups the media format is similar to the format described for QIC and non-QIC tapes, except that NetBackup breaks the backup image into fragments of the size that you specify when you configure the storage unit.

For example,

MH * BH Image (frag 1)* BH Image (frag 2)* BH Image (frag n) * EH *



Fragmentation is intended primarily for storing large backup images on a disk type storage unit. In these instances, fragmenting images allows you to avoid exceeding the two gigabyte size limit that applies to most UNIX file systems.

Another benefit of fragmenting backups on disk is increased performance when restoring from images that were migrated by Storage Migrator. For example, if a 500 megabyte backup is stored in 100 megabyte fragments, you can restore a file quicker because Storage Migrator has to retrieve only the specific fragment with the file rather than the entire 500 megabytes.

Fragmenting tape backups can also speed up restores because NetBackup can skip to the specific fragment before starting its search for a file.

Note If an error occurs in a backup, the entire backup is discarded and the backup restarts from the beginning, not from the fragment where the error occurred.

Multiplexing Format

The tape format for multiplexed backups is as follows. By default, the data image is in 64 kilobyte blocks. Each block also contains 512 bytes that are reserved for multiplexing control information and to identify the backup that the block corresponds to.

MH * BH1 ... BHn Image...

When a job ends or a new job is added to the multiplexing set, NetBackup writes a tape mark and starts multiplexing the revised set of jobs. The following is an example of this.

MH * BH1 BH2 BH3 Image* BH2 BH3 Image* BH2 BH3 BH4 Image. .

Spanning Tapes

By default, NetBackup spans a backup image to another tape if it encounters the end of media during a backup. The format is the same as described for fragmented backups, and the first fragment on the next tape begins with the buffer of data where the end of media occurred.

First tape: (NetBackup does not write an EH, and terminates the tape with two tape marks)

MH * ... *BHn Image (frag 1) **

Second tape:

MH * BHn Image (frag2)* ... * EH *

Media Manager Security

Media Manager security works in conjunction with NetBackup authentication/authorization security (see “NetBackup Authentication/Authorization” on page 347) to control user access to the following:

- ◆ `vmd` (the Media Manager volume daemon on UNIX and the NetBackup Volume Manager service on Windows).
- ◆ Media Manager robotic daemons and services.

Media Manager security consists of the following levels of security. Each successive level listed provides more security. These levels are explained in the following topics:

- ◆ “Media Manager Authentication/Authorization” on page 348.
- ◆ “Media Manager Security (Using SERVER Configuration Entries)” on page 349.
- ◆ “Possible NetBackup and Media Manager Conflicts” on page 350.
- ◆ “Media Manager Enhanced Authorization” on page 350.

NetBackup Authentication/Authorization

NetBackup authentication verifies NetBackup client to server access and also controls access to the services available on that host.

NetBackup authorization verifies if a NetBackup administration user has permission to use the services available on that host. Authorization provides additional security over the security provided by authentication.

The steps you use to set up security levels for your NetBackup master server apply generally to setting up security for Media Manager media servers (or SAN media servers). See the NetBackup system administrator's guide (for UNIX or for Windows servers) for more information including the following topics:

- ◆ Explanations of authentication and authorization.
- ◆ Explanations of Enhanced Authentication.
- ◆ Explanations of Enhanced Authorization.
- ◆ Definition of the NetBackup configuration file (`bp.conf`) on UNIX.
- ◆ Definitions of the `methods.txt`, `methods_allow.txt`, and `authorize.txt` files.
- ◆ Information on `bpauthsync(1M)`, `vopied(1M)`, and `vopie_util(1M)` man pages.



Media Manager Authentication/Authorization

Media Manager security works in conjunction with the following security components to control access to `vmcmd` and robotic functions.

- ◆ NetBackup authentication/authorization
- ◆ Media Manager server-based security
- ◆ Media Manager enhanced authorization (includes robot authorization)

The two matrices (“No `vm.conf` Entry Present” on page 348 and “`vm.conf` Entry is Present” on page 349) provide an overview of Media Manager security. Server Name, used in these matrices, refers to `SERVER` entries in the Media Manager configuration file.

See “The Media Manager Configuration File (`vm.conf`)” on page 355 for more information about the `SERVER`, `AUTHORIZATION_REQUIRED`, `ENABLE_ROBOT_AUTH`, and `PREFERRED_GROUP` entries.

No `vm.conf` Entry Present

The following matrix describes Media Manager security when there is *no* `AUTHORIZATION_REQUIRED` entry in the `vm.conf` file.

If authentication is not enabled (see the fourth row in the following matrix), the resulting security reduces to the level of Media Manager server-based security (see “Media Manager Security (Using `SERVER` Configuration Entries)” on page 349).

Media Manager Security Matrix - No `AUTHORIZATION_REQUIRED` Entry

Access to Media Manager functionality?	Server name is in <code>vm.conf</code>	No server names in <code>vm.conf</code> (or no <code>vm.conf</code> file)	Server name not in <code>vm.conf</code> (other server names are present)
Authentication failed	Denied	Denied	Denied
Authentication enabled and user is authorized	Allowed	Allowed	Allowed (overrides server-based security)
Authentication enabled and user is not authorized	Allowed (uses server-based security)	Allowed (uses server-based security)	Denied
Authentication not enabled	Allowed	Allowed	Denied

vm.conf Entry is Present

The following matrix describes Media Manager security when there *is* an `AUTHORIZATION_REQUIRED` entry in the `vm.conf` file.

Media Manager Security Matrix - `AUTHORIZATION_REQUIRED` Entry

Access to Media Manager functionality?	Server name is in <code>vm.conf</code>	No server names in <code>vm.conf</code>	Server name not in <code>vm.conf</code> (other server names are present)
Authentication failed	Denied	Denied	Denied
Authentication enabled and user is authorized	Allowed	Allowed	Allowed (overrides server-based security)
Authentication enabled and user is not authorized	Allowed (uses server-based security)	Denied (disables server-based security)	Denied
Authentication not enabled	Allowed	Denied	Denied

Your level of security is dependent upon your use of the following:

- ◆ Authentication
- ◆ Authorization
- ◆ `SERVER` entries in `vm.conf`

Media Manager Security (Using `SERVER` Configuration Entries)

`SERVER` entries in `vm.conf` are used for server-based Media Manager security.

If there are no `SERVER` entries and no `AUTHORIZATION_REQUIRED` entry present on a particular host, other hosts can perform media and device management on the host. You can add `SERVER` entries allowing only specific hosts to remotely access those capabilities.

The fourth row of the matrix in “No `vm.conf` Entry Present” on page 348 provides an overview of Media Manager server-based security level.

If a host's `vm.conf` file contains *any* `SERVER` entries, there must also be a `SERVER` entry for that host or it will not be able to manage its own devices.



Possible NetBackup and Media Manager Conflicts

Media Manager authentication/authorization may affect systems where NetBackup authentication/authorization has been enabled.

Connections to media and device management functionality on the host will fail if the following are all true:

- ◆ Authentication/authorization are enabled.
- ◆ An `AUTHORIZATION_REQUIRED` entry is present in `vm.conf`.
- ◆ The caller of the media and device management functions does not have the required permission to use those functions.

▼ To enable authentication/authorization in NetBackup (but not in Media Manager)

You can do either of the following:

- ❖ Add `SERVER` entries in `vm.conf`.
- ❖ Have no `SERVER` and no `AUTHORIZATION_REQUIRED` entries in `vm.conf`.

Media Manager Enhanced Authorization

The set of commands that Media Manager enhanced authorization allows users (other than administrators) to execute is limited. These commands interact with `vmd` or with the control functions for robotic services.

See the following topics:

- ◆ “Supported Commands and Daemons” on page 351.
- ◆ “Allowing Enhanced Authorization” on page 352.
- ◆ “Enabling Robot Authorization” on page 352.

Supported Commands and Daemons

The set of Media Manager commands and daemons (or services) that support enhanced authorization are shown in the following table. All other Media Manager commands that manipulate the Media Manager database or configuration files directly are restricted to administrators. Review the Note column for any restrictions.

Commands and Daemons (or Services)	Note	Commands and Daemons (or Services)	Note
acsd	Applies only to NetBackup Enterprise Server.	tshd	
lmfcd	Applies only to NetBackup Enterprise Server.	vmadd	
odld		vmchange	
rsmd		vmcheckxxx	
tl4d		vmdelete	
tl8cd		vmoprcmd	
tlbcd		vmphyinv	
tlhcd	Applies only to NetBackup Enterprise Server.	vmppool	
tlmd	Applies only to NetBackup Enterprise Server.	vmquery	
tpautoconf		vmrule	
ts8d		vmupdate	
tsdd			



Allowing Enhanced Authorization

If you want to control user access to administer Media Manager commands, see the NetBackup system administrator's guide for UNIX for instructions on using enhanced authentication and authorization.

Enabling Robot Authorization

Robot authorization extends the scope of Media Manager enhanced authorization to include the robot daemons (or services). The robot daemons (and services) authenticate and authorize incoming requests so that a subset of robot functions can be used by authorized users. By default robot authorization is disabled.

Since the use of reserved ports is only valid for privileged users, the Media Manager robot daemons (and services) no longer require reserved ports.

Note Connecting to a robotic control daemon using a reserved port is still allowed.

▼ To enable robot authorization

- ❖ Add an `ENABLE_ROBOT_AUTH` entry in `vm.conf` on the master server and the media server (or SAN media server).

Administrators Quick Reference

The tables (see “Media Manager Commands” on page 352 and “Media Manager Log Files” on page 355) provide a quick reference to commands and log files that you may require while using Media Manager. Check the Note column for any restrictions.

Media Manager Commands

See the NetBackup Commands for Windows reference guide for detailed information on the commands shown in the following tables. These commands listed are located in *install_path\volmgr\bin*.

Note Services should be started and stopped using the **Services** tool available in **Administrative Tools** in the Windows control panel. If they are started from the command line, some services will occupy that NetBackup Console session until they are stopped.

Administrative Utilities

Command	Description
robtest	Starts the robotic test utilities. NOTE: This utility is not officially supported.

Starting Services and Processes

Command	Description	Note
acsd	The Automated Cartridge System robotic process. This process is started by ltid.	Applies only to NetBackup Enterprise Server.
avrd	The Automatic Volume Recognition process. This process is started by ltid.	
ltid	Starts the NetBackup Device Manager service. Starting ltid also starts the robotic, robotic control, Media Manager volume, and automatic volume recognition daemons.	
rsmd	The Removable Storage Manager robotic process. This process is started by ltid.	
tl4d	The Tape Library 4MM robotic process. This process is started by ltid.	
tl8cd	Starts the Tape Library 8MM robotic-control process. This process is started by ltid.	
tl8d	The Tape Library 8MM robotic process. This process is started by ltid.	
tl8cd	Starts the Tape Library DLT robotic-control process. This process is started by ltid.	
tl8dd	The Tape Library DLT robotic process. This process is started by ltid.	



Starting Services and Processes (continued)

Command	Description	Note
tlhcd	Starts the Tape Library Half-inch robotic-control process. This process is started by ltid.	Applies only to NetBackup Enterprise Server.
tlhd	The Tape Library Half-inch robotic process. This process is started by ltid.	Applies only to NetBackup Enterprise Server.
tlmd	The Tape Library Multimedia process. This process is started by ltid.	Applies only to NetBackup Enterprise Server.
ts8d	The Tape Stacker 8MM robotic process. This process is started by ltid.	
tsdd	The Tape Stacker DLT robotic process. This process is started by ltid.	
vmd	The NetBackup Volume Manager service. This process is started by ltid.	

Stopping Services and Processes

Command	Description	Note
stopltid	Stops the device, robotic, and robotic-control services.	
tlbcd -t	Stops the Tape Library DLT robotic-control process.	
tl8cd -t	Stops the Tape Library 8MM robotic-control process.	
tlhcd -t	Stops the Tape Library Half-inch robotic-control process.	Applies only to NetBackup Enterprise Server.

Media Manager Log Files

The following table contains descriptions of important Media Manager log files.

Log Files

Log File	Description	Note
Event Viewer	Contains general Media Manager logging, including errors.	
daemon/ <i>ddmmyy</i> .log	Contains debug information for the NetBackup Volume Manager service (vmd) and its associated processes (opr and rdevmi). The path is <i>install_path</i> \volmgr\debug\daemon.	
reqlib/ <i>ddmmyy</i> .log	Contains debug information on the processes that request vmd. The path is <i>install_path</i> \volmgr\debug\reqlib.	
tpcommand/ <i>ddmmyy</i> .log	Contains debug information for device configuration. Includes information for tpconfig, tpautoconf, and the NetBackup GUIs. The path is <i>install_path</i> \volmgr\debug\tpcommand.	
ltid/ <i>ddmmyy</i> .log	Contains debug information for ltid, the NetBackup Device Manager service. The path is <i>install_path</i> \volmgr\debug\ltid.	
robots/ <i>ddmmyy</i> .log	Contains debug information for SCSI robotic processes. Includes information for tldcd, tl8cd, tl4d, rsmd, and tshd processes. The path is <i>install_path</i> \volmgr\debug\robots.	

The Media Manager Configuration File (vm.conf)

The *install_path*\volmgr\vm.conf file contains configuration entries for media and device management. This file is usually created by NetBackup, but if it does not exist you need to create it to add entries.



Entries in this configuration file are read and interpreted on the host where the NetBackup component (command, daemon, process, or utility) that is using a specific entry is running. This host may be a NetBackup administration client or a server where administration operations are requested.

See “Example vm.conf File” on page 375 for an example configuration file.

The entries that this file can contain are as follows.

- ◆ “ACS Media Mapping” on page 357
- ◆ “Adjacent LSM Specification for ACS Robots” on page 357
- ◆ “API Robot Barcode Rule Enable” on page 358
- ◆ “Authorization Required” on page 359
- ◆ “Automatically Empty Robot MAP” on page 359
- ◆ “AVRD Scan Delay” on page 359
- ◆ “AVRD Pending Status Delay” on page 360
- ◆ “Backup Exec - Mapping Media Types” on page 360
- ◆ “Backup Exec - Mapping Robots” on page 361
- ◆ “Cleaning Drives Timeout” on page 361
- ◆ “Client Port Range” on page 362
- ◆ “Connect to Firewall Options” on page 362
- ◆ “DAS Client Name” on page 363
- ◆ “Days To Keep Debug Logs” on page 363
- ◆ “Device Host Entries” on page 364
- ◆ “Disable Automatic Path Remapping” on page 364
- ◆ “Disallow Non-NDMP Request on NDMP Drive” on page 364
- ◆ “Do Not Eject Standalone Tapes” on page 365
- ◆ “Enable Robot Authorization” on page 365
- ◆ “Inventory Robot Filter” on page 365
- ◆ “Media Access Port Default for ACS Robots” on page 366
- ◆ “Media ID Generation” on page 367
- ◆ “Media ID Prefix” on page 368
- ◆ “Not Allowing a Host To Manage Databases” on page 368
- ◆ “Preferred Group” on page 368

- ◆ “Prevent Media Removal (for TL8 Robots)” on page 369
- ◆ “Random Port Numbers” on page 369
- ◆ “Cluster Name, Media Manager Name, Required Network Interface” on page 370
- ◆ “Return Media to the Scratch Pool” on page 371
- ◆ “RSM Media Mapping” on page 371
- ◆ “Scratch Pool Configuration” on page 371
- ◆ “Server Entry” on page 372
- ◆ “SSO DA Re-register Interval” on page 372
- ◆ “SSO DA Retry Time” on page 372
- ◆ “SSO Host Name” on page 373
- ◆ “SSO Scan Ability Factor” on page 373
- ◆ “TLH Media Mapping” on page 374
- ◆ “TLM Media Mapping” on page 374
- ◆ “Vault Media Description Reset” on page 374
- ◆ “Verbose Message Logging” on page 375

ACS Media Mapping

ACS_mediatype = Media_Manager_mediatype

This configuration entry applies only to NetBackup Enterprise Server

If this entry is specified in `vm.conf`, ACS (Automated Cartridge System) media types are mapped to Media Manager media types. This entry is read and interpreted on the host where `vmcheckxxx` and `vmupdate` are running as part of the robot inventory operation.

For more information, see the appendix, “STK Automated Cartridge System (ACS)” on page 377.

Adjacent LSM Specification for ACS Robots

ADJ_LSM = robot_num ACS_ID,LSM_ID ACS_ID,LSM_ID

This configuration entry applies only to NetBackup Enterprise Server.

In an ACS robot with multiple Library Storage Modules (LSMs), media to be ejected may have to travel through pass-through mechanisms from LSM to LSM to reach a Media Access Port (MAP). This travel time can be excessive when passing through several LSMs.



Use this entry to specify the physical orientation of the LSMs in an ACS robot. If this entry is specified in `vm.conf`, you do not need to know which MAP (or ACS CAP) to select for efficient ejects. Media Manager determines the appropriate MAP to complete the media eject using a nearest-MAP algorithm.

This nearest-MAP algorithm is based on the physical orientation of the LSMs that you define with this entry. This algorithm is only for the cases where more than one MAP has been requested to handle the eject. If this algorithm is being utilized, any `MAP_ID` entries in `vm.conf` are ignored.

Note The nearest-MAP capability is only available using the `vmchange` command with the `-map` option or the Vault administrative interface. It is not available in the NetBackup graphical administrative interfaces for Media Manager.

Without this entry present, Media Manager assumes that all LSMs are interconnected with pass-through ports, except for the first and last LSMs (the LSMs are interconnected in a line formation).

`robot_num` is the robot number. `ACS_ID` and `LSM_ID` are the coordinates of the LSM.

The following example specifies the physical layout of LSM interconnections for robot number 700. This robot has 4 LSMs that are connected by pass-through mechanisms in a circular configuration. LSMs 1 and 3 are also interconnected.

```
ADJ_LSM = 700 0,0 0,1
ADJ_LSM = 700 0,0 0,3
ADJ_LSM = 700 0,1 0,3
ADJ_LSM = 700 0,1 0,2
ADJ_LSM = 700 0,2 0,3
```

API Robot Barcode Rule Enable

`API_BARCODE_RULES`

This configuration entry applies only to NetBackup Enterprise Server.

If this entry is specified in `vm.conf`, barcode rule support for API robots is enabled.

Media Manager barcode rules allow you to override the default media mappings. Barcode rules are especially useful when the media used by multiple generations of the same tape drive is not differentiated by the vendor.

For example STK 9940A and STK 9940B drives use STK1R media, but write data at different densities. The drive must be configured as `hcart` or `hcart2`. You can specify a barcode rule for a series of barcodes to configure some of the media as `hcart2`. Other STK1R media not in this barcode range will be configured as `hcart` (the default for

STK1R). Without an `API_BARCODE_RULES` entry, a robot inventory operation would configure all media of type STK1R as either hcart or hcart2, depending on how the drive was configured.

Authorization Required

`AUTHORIZATION_REQUIRED`

If this entry is specified in `vm.conf`, Media Manager and NetBackup utilities must have authorization to connect to `vm`; or a `SERVER` entry must be present in the `vm.conf` file. This entry is recommended for maximum security, and is read and interpreted on the hosts where `vm` is running.

If this entry is not specified, Media Manager and NetBackup utilities may connect to `vm` without specific authorization, except in the case when a non-matching `SERVER` entry is present in `vm.conf`.

Automatically Empty Robot MAP

`AUTO_UPDATE_ROBOT`

If this entry is specified in the `vm.conf` file of the media server with a TL8 or TLD robotic control daemon, the Media Access Port (MAP) of the robot will be emptied into the robotic library and the volume database will be updated.

This entry only operates with TL8 or TLD robots that post a unit attention when their MAP has been opened. Since most robotic libraries with multiple partitions do not post a unit attention when the MAP has been accessed, using this entry is not recommended with partitioned libraries.

AVRD Scan Delay

`AVRD_SCAN_DELAY = number_of_seconds`

If this entry is specified in `vm.conf`, `avrd` will wait *number_of_seconds* between normal scan cycles. This entry is read and interpreted on the host where `avrd` is running.

You can use this entry to minimize tape mount times. Without this entry present, a mount request is delayed by an average of 7.5 seconds.

The minimum for *number_of_seconds* is 1. The maximum is 180. A value of zero is converted to 1 second. The default value is 15 seconds. Using a value greater than the default will delay mount requests and the displaying of drive status information in the Device Monitor.



Caution Setting *number_of_seconds* to a value that allows media to be changed within one scan cycle could cause NetBackup to be unaware of a media change and cause a loss of data.

AVRD Pending Status Delay

AVRD_PEND_DELAY = number_of_seconds

If this entry is specified in *vm.conf*, *avrd* will wait *number_of_seconds* before displaying a pending status (PEND) in the Device Monitor. This entry is read and interpreted on the host where *avrd* is running.

Some server operating systems (Windows, Tru64, and HP-UX) report PEND if the drive reports Busy when a volume is unmounted. You can use this entry to minimize the display of this misleading status.

The minimum for *number_of_seconds* is zero. The maximum is 255. The default value is 180 seconds.

Backup Exec - Mapping Media Types

backup_exec_media_type = netbackup_robot_number netbackup_media_type

If this entry is specified in *vm.conf*, you can map Backup Exec media types to NetBackup media types. This entry is used with the Backup Exec tape reader feature and can be used when a NetBackup robot has different drives of a similar type configured. This entry is read and interpreted on the host where *bephyinv* or *beconv* is running.

For example in a Backup Exec configuration, you have a robot with two DLT drives. Both drives are considered to be DLT and all media in this robot have a media type of BE_DLT. You plan to move your Backup Exec media to be used with NetBackup.

In your NetBackup configuration, you have a different robot (robot 1) with two DLT drives. One drive is configured as DLT (Drive0) and the other drive is DLT3 (Drive1). The Backup Exec DLT media type can map to DLT or DLT3.

If a *backup_exec_media_type* entry is *not* specified, the Backup Exec media type will be mapped to the media type of the drive with the lowest index. Based on information not shown for this example, Drive0 is determined to have the lowest drive index. Drive0 is DLT, so Backup Exec media type DLT will be mapped to the NetBackup media type DLT. (This is equivalent to specifying *BE_DLT = 1 DLT*.)

If you do not want this default mapping, you can add a *backup_exec_media_type* entry to specify that for this robot, the Backup Exec DLT media type maps to the NetBackup DLT3 media type (*BE_DLT = 1 DLT3*).



backup_exec_media_type is the Backup Exec media type.

netbackup_robot_number is the NetBackup robot number. For standalone drives, the robot number must be -1. For example, `BE_DLT = -1 DLT`

netbackup_media_type is the NetBackup media type (see “Media Manager Media Types” on page 277).

Allowable and default mappings are as follows:

Backup Exec Media Type	NetBackup Media Type	Default Mapping
BE_8MM	8MM, 8MM2, 8MM3	8MM
BE_DLT	DLT, DLT2, DLT3	Media type of the drive with the lowest index
BE_HALF_INCH	HCART, HCART2, HCART3	Media type of the drive with the lowest index

Backup Exec - Mapping Robots

`BE_CHANGER_NAME_name = netbackup_robot_number`

If this entry is specified in `vm.conf`, you can map robots used in Backup Exec to NetBackup robots. This entry is used with the Backup Exec tape reader feature and is required when a robot is not serialized. This entry is read and interpreted on the host where `bephyinv` or `beconv` is running.

`BE_CHANGER_NAME_name` is the Backup Exec changer (robot) name. There cannot be any spaces in this field. For example if the robot name is HP 1, this field would be `BE_CHANGER_NAME_HP1`.

netbackup_robot_number is the NetBackup robot number.

The following are some examples of entries:

```
BE_CHANGER_NAME_HP4 = 1
BE_CHANGER_NAME_EXABYTE1 = 2
```

Cleaning Drives Timeout

`CLEAN_REQUEST_TIMEOUT = minutes`



You can add this entry in `vm.conf` to specify how long Media Manager will wait for a drive to be cleaned before removing the cleaning request from the cleaning queue. The cleaning request is normally removed from the queue, if the request has not been processed after 30 minutes.

minutes can be from 1 to 144000 (100 days). The default value is 30 and a value of zero is converted to the default value of 30.

Client Port Range

```
CLIENT_PORT_WINDOW = start end
```

If this entry is specified in `vm.conf`, you can specify the range of non-reserved ports on this host that are used for connecting to `vmd` on other hosts. This entry is read and interpreted on the hosts where `vmd` is running.

For example, the following entry permits ports from 4800 through 5000:

```
CLIENT_PORT_WINDOW = 4800 5000
```

The operating system determines the non-reserved port to use in the following cases:

- ◆ You do not specify a `CLIENT_PORT_WINDOW` entry
- ◆ You specify a value of zero for *start*.

Connect to Firewall Options

```
CONNECT_OPTIONS = server_name 0 0 [0|1|2]
```

You can add this entry in `vm.conf` to specify options that are designed to enhance firewall efficiency with Media Manager. Server connection options can be any of the following: use `vnetd` or the daemon's port number, use only `vnetd`, or use only the daemon's port number.

You can specify `CONNECT_OPTIONS` entries for multiple servers and can also use a similar entry and add it to the NetBackup configuration file (`/usr/openv/netbackup/bp.conf`). See the NetBackup system administrator's guide for details.

server_name is the name of the media server (or SAN media server) to be connected to and the server must be at NetBackup level 4.5 for `vnetd` to operate correctly.

The first and second settings currently are not used. Specify zero for these settings.

The third setting indicates the connection method to use to connect to *server_name* as follows:

- ◆ A value of 0 specifies to connect to a daemon on the server using `vnetd` if possible, otherwise connect using the traditional port number of the daemon.
- ◆ A value of 1 specifies to connect to a daemon on the server using `vnetd` only.
- ◆ A value of 2 specifies to connect to a daemon on the server using the traditional port number of the daemon only (2 is the default value).

The following are some examples:

```
CONNECT_OPTIONS = shark 0 0 0
```

This entry specifies that connections to `vmd` and robotic daemons on the server named `shark` can use either `vnetd` or the daemon's port number.

```
CONNECT_OPTIONS = dolphin 0 0 1
```

This entry specifies that connections to `vmd` and robotic daemons on the server named `dolphin` must use `vnetd`.

```
CONNECT_OPTIONS = perch 0 0 2
```

This entry specifies that connections to `vmd` and robotic daemons on the server named `perch` must use the daemon's port number.

DAS Client Name

```
DAS_CLIENT = client_name
```

This configuration entry applies only to NetBackup Enterprise Server

If this entry is specified in `vm.conf`, you specify the DAS client name that the TLM robot uses for communications with the DAS/SDLC server. By default this client name is the host name of the Media Manager server. This entry is read and interpreted on the host where `tlmd` is running.

See the appendix, "ADIC Distributed AML Server/Scalar Distributed Library Controller" on page 411 for more information.

Days To Keep Debug Logs

```
DAYS_TO_KEEP_LOGS = days
```

If this entry is specified in `vm.conf`, you can specify the number of days to keep debug logs before `vmd` deletes them. This entry is read and interpreted on the hosts where `vmd` is running.

A value of zero means that the logs are not deleted. The default is zero.



Device Host Entries

```
DEVICE_HOST = host_name
```

This configuration entry applies only to NetBackup Enterprise Server

Note These entries are not used by the NetBackup Administration Console.

If this entry is specified in `vm.conf`, it specifies a host that is to be included when running the Media Manager configuration analyzer interface from the command line. This entry is read and interpreted on the host where the configuration analyzer is running.

Entries are also added when the NetBackup Volume Manager service restarts, based on robot host names appearing in volume groups.

Disable Automatic Path Remapping

```
DISABLE_AUTO_PATH_CORRECTION
```

If this entry is specified in `vm.conf`, automatic device path remapping is disabled. This entry is read and interpreted on the host where the NetBackup Device Manager service is running.

With this entry, the device configuration will remain unchanged when the NetBackup Device Manager service is started. This may result in the device configuration becoming out of sync with the host's view of devices following a reboot.

Disallow Non-NDMP Request on NDMP Drive

```
DISALLOW_NONNDMP_ON_NDMP_DRIVE
```

This entry is read and interpreted on the host where the robotic daemon or process is running.

In NetBackup, all read types of operations (restore, the read-portion of duplicates, import, and verify) and the write-portion of duplicates are not scheduled. Therefore, these operations compete for available drives.

NetBackup attempts to use an available drive based on the type of request as follows:

- ◆ For a NDMP backup or restore request, the drive must be a NDMP drive.
- ◆ For a non-NDMP request of any kind, NetBackup always tries to find an available non-NDMP drive. If a non-NDMP drive is not available, and a NDMP drive *is* available, the operation will be done using the slower NDMP drive.

If a `DISALLOW_NONNDMP_ON_NDMP_DRIVE` entry is specified in `vm.conf` on a given master or media server (or SAN media server), NetBackup will *not* assign a non-NDMP request to available NDMP drives.

Be aware when specifying this entry, that because some operations may have to wait for available non-NDMP drives to become available, the media mount timeout value may have to be increased. You can increase this value by using an entry in the `UNIX bp.conf` file or selecting **Host Properties > Master Server > Global NetBackup Attributes** on Windows.

Do Not Eject Standalone Tapes

`DO_NOT_EJECT_STANDALONE`

If this entry is specified in `vm.conf` on a given host, tapes in standalone drives will not be ejected when a backup has completed on that host (tapes will be ejected if end of media is reached during a backup). This entry is read and interpreted on the host where the standalone drives are defined.

This entry can be used in a NetBackup environment where it is desirable to keep a standalone drive ready after successful backups are performed.

The `NO_STANDALONE_UNLOAD` file is also used to control tape ejects in standalone drives. Refer to the NetBackup system administrator's guide for Windows servers for more information about this file.

Enable Robot Authorization

`ENABLE_ROBOT_AUTH`

Robot authorization extends the scope of Media Manager enhanced authorization to include the robot daemons (or services). If robot authorization is enabled, the robot daemons authenticate and authorize incoming requests so that a subset of robot functions can be used by authorized users.

If this entry is specified in `vm.conf` on the master and media servers (or SAN media servers), robot authorization is enabled.

By default robot authorization is disabled.

Inventory Robot Filter

`INVENTORY_FILTER = robot_type robot_number mode value1 [value2 ...]`

This configuration entry applies only to NetBackup Enterprise Server.



Used for robotic inventory filtering in ACS, TLH, or LMF robot types. This entry must be added to the configuration file (`vm.conf`) on the media server (or SAN media server) where you plan to do the robotic inventory. This entry is read and interpreted on the host where `vmcheckxxx` and `vmupdate` are running.

Note This entry is required if you are doing a robot inventory for an ACS robot and the ACS library software host is an STK Library Station.

robot_type can be ACS, TLH, or LMF.

robot_number is the number of the robot as was configured in Media Manager.

mode is `BY_ACS_POOL` for ACS, `BY_CATEGORY` for TLH, or `BY_PREFIX` for LMF robot types.

The following are some examples:

```
INVENTORY_FILTER = ACS 0 BY_ACS_POOL 4 5
INVENTORY_FILTER = TLH 0 BY_CATEGORY FFFA CDB0
INVENTORY_FILTER = LMF 0 BY_PREFIX zzz yy
```

See the appendices, “STK Automated Cartridge System (ACS)” on page 377 and “IBM Automated Tape Library (ATL)” on page 399 for more information.

Media Access Port Default for ACS Robots

```
MAP_ID = robot_num map_ID
```

This configuration entry applies only to NetBackup Enterprise Server.

This entry in `vm.conf` sets the Media Manager default for the Media Access Port that may be used for ejecting media from ACS (Automated Cartridge System) robots. This default is highlighted as a choice in the Media Manager and Vault administrative GUIs, but the user can also select other Media Access Ports for ejects.

If the access port specified by the MAP ID entry is not available or this entry is not present, the default media access port selection process will be used. This selection process matches the number of media specified to be ejected to the smallest access port that will hold that number of media, and uses that port.

If multiple MAPs are selected by the user, the MAP ID entry is not used and the nearest-MAP algorithm is used (see “Adjacent LSM Specification for ACS Robots” on page 357).

robot_num is the robot number. *map_ID* is in the format of an ACS CAP (Cartridge Access Port) ID and cannot contain any spaces.

The following example specifies the MAP ID for ACS robot number 700. The ACS CAP ID of 0,1,0 is used.




```
MAP_ID = 700 0,1,0
```

Media ID Generation

```
MEDIA_ID_BARCODE_CHARS = robot_num barcode_length media_ID_rule
```

Note To use this entry, the robot must support barcodes and the robot type cannot be one of the API robots.

If this entry is specified in `vm.conf`, it controls Media Manager media ID generation. This entry is read and interpreted on the host where `vmcheckxxx` and `vmupdate` are running as part of the robot inventory operation.

You choose how media IDs are created by defining rules that specify which characters of a barcode on tape will be used. You also can specify alphanumeric characters to be inserted in the ID.

Multiple media ID creation entries can be specified, allowing media ID generation to be specific for each robot; or for each barcode format having different numbers of characters in the barcode. This allows flexibility for multi-media.

If `MEDIA_ID_BARCODE_CHARS` entries are not present in `vm.conf` or you enter an invalid entry, Media Manager uses the right-most (the last) six characters of the barcode to create its media ID as the default.

robot_num is the robot number.

barcode_length is the length of the barcode.

A *media_ID_rule* consists of a maximum of six fields delimited by colons. Numbers in the fields of the rule define the positions of the characters in the barcode that are to be extracted (numbering is from the left). For example, 2 in a field extracts the second character from the barcode. The numbers can be specified in any order.

Characters prefixed by # in a field, result in that character being inserted in that position in the generated ID. Any alphanumeric characters that are specified must be valid for a media ID. You can use rules to create media IDs of many varied formats, but keep in mind that the difference in the label on the media and the generated media ID may make it difficult to manage your media. The following is an example rule and the resulting generated media ID:

```
Barcode on the tape: 032945L1
Media ID rule:      #N:2:3:4:5:6
Generated media ID: N32945
```

Also see “Media ID Generation Rules” on page 325.



Media ID Prefix

`MEDIA_ID_PREFIX = media_id_prefix`

If this entry is specified in `vm.conf`, it defines the media ID prefixes to use for media without barcodes. This entry is read and interpreted on the host where `vmcheckxxx` and `vmupdate` are running as part of the robot inventory operation.

The best way to add media to a robot is to use the Robot Inventory Update Volume Configuration operation.

See “Media Settings Tab (Advanced Options)” on page 168.

Not Allowing a Host To Manage Databases

`NOT_DATABASE_HOST`

If this entry is specified in `vm.conf`, any requests to add, change, or delete any records in the volume, volume pool, or barcode rule databases will be denied. This is useful if you wish to enforce only one volume database in an operating environment. In that case, add this entry in the `vm.conf` file of all the media servers (*except* the volume database host) to prevent other hosts from having their own volume database.

Preferred Group

`PREFERRED_GROUP = netgroup_name`

If this entry is specified in `vm.conf`, it is used by all callers in Media Manager and NetBackup (other than `bpgetmedia` and `bptm`) for authentication/authorization for `vmd`. This entry is read and interpreted by all callers that are connecting to `vmd`.

netgroup_name is case sensitive.

If this entry is specified, a check is made to determine if the user is a member of `domain\group`. This check is limited to Windows global groups. If `PREFERRED_GROUP` is set to a domain local group, a match does not occur and the user's primary `domain\group` is used.

If a `PREFERRED_GROUP` entry is not specified or the user is not a member of the `domain\group`, the user's primary `domain\group` is obtained. If the domain name is an empty string or the name of the local machine, it is considered to be local.

If a `PREFERRED_GROUP` entry is not specified, the `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config` registry key is checked for an entry.

To achieve a platform independent implementation, *netgroup_name* is case sensitive. The following is an example entry:

```
PREFERRED_GROUP = NTDOMAINNAME\Backup Operators
```

Prevent Media Removal (for TL8 Robots)

```
PREVENT_MEDIA_REMOVAL
```

This entry is read and interpreted on the host where the robot control daemon or process (tl8cd) is running.

Specifying this entry changes the default operation for TL8 robots. Without this entry present, Media Manager allows the removal of media.

If this entry is specified in `vm.conf`, TL8 robots will execute the SCSI command `PREVENT MEDIUM REMOVAL`. You then will not be able to open the robot's main door or gain access to the media access port while the robotic control daemon is running.

▼ To override this action

Do one of the following:

- ❖ Use the test utility and execute `allow media removal`.
- ❖ Use `inject/eject` for access, when adding or moving volumes.

Random Port Numbers

```
RANDOM_PORTS = YES|NO
```

If this entry is specified in `vm.conf`, it specifies whether Media Manager chooses port numbers randomly or sequentially when Media Manager requires a port number for communication with Media Manager on other hosts. This entry is read and interpreted on hosts where `vmd` is running.

If `RANDOM_PORTS = YES` is specified or a `RANDOM_PORTS` entry is not specified (the default), Media Manager chooses port numbers randomly from those that are free in the allowed range. For example, if the range is from 1024 through 5000, Media Manager chooses randomly from the numbers in this range.

If `RANDOM_PORTS = NO` is specified, Media Manager chooses numbers sequentially, starting with highest number that is available in the allowed range. For example, if the range is from 1024 through 5000, Media Manager chooses 5000 (assuming it is free). If 5000 is being used, port 4999 is chosen.



If you do not specify random ports in the NetBackup configuration, you should also specify `RANDOM_PORTS = NO` in the Media Manager configuration file (`vm.conf`).

▼ **To specify no random ports in the NetBackup configuration file**

Do one of the following:

- ❖ Specify `RANDOM_PORTS = NO` in the `bp.conf` file on UNIX.
- ❖ Use the NetBackup **Host Properties** on Windows.

Cluster Name, Media Manager Name, Required Network Interface

```
CLUSTER_NAME = cluster_alias
MM_SERVER_NAME = host_name
REQUIRED_INTERFACE = host_name
```

These three entries are used in determining the server name others should use when referring to this server. The algorithm for determining the server name is as follows:

1. Use the `CLUSTER_NAME` entry if present in `vm.conf`.
2. Use the `MM_SERVER_NAME` entry if present in `vm.conf`.
3. Use the `REQUIRED_INTERFACE` entry if present in `vm.conf`.
4. Use the same name that NetBackup is using, as set in `bp.conf`.
5. Use the `gethostname()` name.

If the `REQUIRED_INTERFACE` entry is present in `vm.conf`, it specifies the network interface that Media Manager uses when connecting to another Media Manager server. This entry is read and interpreted on the host where the required interface is needed.

A Media Manager server can have more than one network interface and by default, the operating system determines the one to use. To force Media Manager connections to be through a specific network interface, use `REQUIRED_INTERFACE` and specify the network host name of that interface.

Refer to the NetBackup system administrator's guide for more information on NetBackup network configuration.

Return Media to the Scratch Pool

```
RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL = YES|NO
```

This entry is read and interpreted on hosts where `vmc` is running.

If `RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL = YES` is specified or if no entry is specified in `vm.conf`, Media Manager returns expired and unassigned media (media that was originally from the same scratch pool) to the scratch volume pool automatically.

If `RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL = NO` is specified, the automatic behavior of returning media to the scratch pool is disabled and must be done using one of the Media Manager administration interfaces.

RSM Media Mapping

```
RSM_mediatype = Media_Manager_mediatype
```

If this entry is specified in `vm.conf`, Windows 2000 (and later supported releases) Removable Storage Manager (RSM) media types are mapped to Media Manager media types. This entry is read and interpreted on the host where `vmcheckxxx` and `vmupdate` are running.

See the appendix, “Microsoft Removable Storage Manager (RSM)” on page 391 for more information.

Scratch Pool Configuration

```
SCRATCH_POOL = pool_name
```

If this entry is specified in `vm.conf`, the specified volume pool is configured as the scratch pool. This entry is read and interpreted on hosts where `vmc` is running.

The scratch pool is a special volume pool from which media is moved as needed into volume pools that have no available media.

You can specify any scratch pool name, except the names: `NetBackup`, `DataStore`, or `None`. If the specified volume pool does not exist, Media Manager creates a pool and sets the host to `ANYHOST`, the user to `root`, the group to `NONE`, and the description for the pool to `Scratch Pool`.

If you subsequently delete this entry, the specified volume pool will no longer be the scratch pool.

See “Adding a New Volume Pool or Scratch Volume Pool” on page 109.



Server Entry

```
SERVER = host_name
```

If this entry is specified in `vm.conf` it is used for security, and specifies which hosts can monitor and control devices on this host. This entry is read and interpreted on hosts where `vmd` is running.

Without any `SERVER` entries and authentication enabled, any host can manage the devices and volumes on the local host. For security you can add entries allowing only specific hosts to remotely access the devices. If a host's `vm.conf` file contains any `SERVER` entries, there must also be a `SERVER` entry for that host or it will not be able to manage its own devices.

SSO DA Re-register Interval

```
SSO_DA_REREGISTER_INTERVAL = minutes
```

This configuration entry applies only to NetBackup Enterprise Server.

This `vm.conf` entry is used only with the shared storage option (SSO) feature and is read and interpreted on the host where `ltid` is running.

`ltid` on a scan host periodically re-registers its shared drives with `vmd/DA` to ensure that it is still providing the drive scanning function on behalf of other hosts sharing the drives. This re-registration allows conditions such as a device allocator restart to have minimal impact on use of shared drives.

The default for the re-registration interval is 5 minutes. You can use this entry to tune this interval. After adding this entry, `ltid` must be stopped and restarted for the change to take effect.

SSO DA Retry Time

```
SSO_DA_RETRY_TIMEOUT = minutes
```

This configuration entry applies only to NetBackup Enterprise Server.

This `vm.conf` entry is used only with the shared storage option (SSO) feature and is read and interpreted on the host where `ltid` is running.

If `ltid` encounters problems during communications with `vmd/DA`, or a failure while attempting to reserve a shared drive, `ltid` delays before trying again.

The default value for the delay is 3 minutes. You can use this entry to tune this delay period. After adding this entry, `ltid` must be stopped and restarted for the change to take effect.

SSO Host Name

```
SSO_HOST_NAME = host_name
```

This configuration entry applies only to NetBackup Enterprise Server.

This `vm.conf` entry is used only with the shared storage option (SSO) feature and is read and interpreted on the host where `ltid` is running.

This entry specifies the name used by the current host to register, reserve, and release shared drives with `vmid/DA`. The default is the local host name.

SSO Scan Ability Factor

```
SSO_SCAN_ABILITY = scan_factor
```

This configuration entry applies only to NetBackup Enterprise Server.

This `vm.conf` entry is used only with the shared storage option (SSO) feature and is read and interpreted on the host where `ltid` is running.

A scan ability factor can range from zero to 9, with a default value of 5. This factor allows the assignment of scan hosts to be prioritized, if a drive's scan host changes. Scan hosts that have a higher scan ability factor are chosen first.

In some SSO configurations, you may have servers that are undesirable for use as the scan host for a drive. This may be because they have limited resources, are behind firewalls, or are being administered by people other than NetBackup administrators. These servers can be configured to never become the scan host for any drive. A *scan_factor* of zero means that a server will not become the scan host.

Caution A drive is unavailable for use until a scan host can be assigned for it. If all hosts that register for a particular drive use *scan_factor* = 0, the drive will enter an unusable state until a host with a *scan_factor* of non-zero registers for the drive. If all hosts with a *scan_factor* of non-zero have the drive DOWN, then again the drive becomes unavailable due to the lack of a scan host.

The decision to use a *scan_factor* of zero for a server, reduces the level of resiliency in your SSO configuration. Careful attention to those servers that can be a scan host is required, as the loss of a scan host for a drive makes it unavailable to any server.

Release Level Considerations

Media Manager servers prior to NetBackup 4.5 FP3 cannot be configured with a *scan_factor* of zero. If zero is specified, the default value of 5 is used.



NetBackup release 4.5 (or any 4.5 MP release) device allocation (DA) hosts will accept registrations from NetBackup 4.5 FP3 media servers (or SAN media servers) with a *scan_factor* of zero. A 4.5 release device allocation host handles the zero scan factor the same as any other legal value. A value of zero is just a scan factor less than one.

Device allocation hosts running NetBackup releases 4.5 FP3 thru 5.0 will not select as a scan host servers that have a scan factor of zero. The case where all servers are registered with a value of zero, causing the drive to have no scan host, will not occur if any registered host is at the 4.5 release level (since this host will not send a zero scan factor). So, a device allocation host running NetBackup releases 4.5 FP3 thru 5.0 can have some hosts with a zero scan factor and work correctly in a mixed server environment.

TLH Media Mapping

TLH_mediatype = Media_Manager_mediatype

This configuration entry applies only to NetBackup Enterprise Server.

If this entry is specified in *vm.conf*, IBM ATL media types in Tape Library Half-inch (TLH) robots are mapped to Media Manager media types. This entry is read and interpreted on the host where *vmcheckxxx* and *vmupdate* are running as part of the robot inventory operation.

See the appendix, “IBM Automated Tape Library (ATL)” on page 399 for more information.

TLM Media Mapping

TLM_mediatype = Media_Manager_mediatype

This configuration entry applies only to NetBackup Enterprise Server.

If this entry is specified in *vm.conf*, DAS/SDLC media types in Tape Library Multimedia (TLM) robots are mapped to Media Manager media types. This entry is read and interpreted on the host where *vmcheckxxx* and *vmupdate* are running as part of the robot inventory operation.

See the appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 411 for more information.

Vault Media Description Reset

VAULT_CLEAR_MEDIA_DESC

When NetBackup media is returned from the off-site vault during a typical tape rotation, it is expired and is ready for reuse by new backups. To avoid confusion, it may be helpful to clear the old media description information when an expired tape is returned to the robot.

If this entry is specified in `vm.conf`, the media description field will be cleared when other Vault information is cleared from the Media Manager volume database.

Verbose Message Logging

VERBOSE

If this entry is specified in `vm.conf`, all Media Manager components on the host are started with verbose logging enabled.

Use this option only if problems occur or if requested by VERITAS support. After the problem is resolved, remove any debug logs that were created or add a `DAYS_TO_KEEP_LOGS` entry.

Example vm.conf File

The following is an example of a `vm.conf` file, on host yak:

```
SERVER = yak
SERVER = whale
MEDIA_ID_PREFIX = NV
MEDIA_ID_PREFIX = NETB
ACS_3490E = HCART2
SCRATCH_POOL = ScratchPool
```



STK Automated Cartridge System (ACS)

B

Note *This appendix applies only to NetBackup Enterprise Server.*

Under Media Manager, robotic support for Automated Cartridge System robots is classified as ACS and these robots are considered API robots (a Media Manager grouping of robots where the robot manages its own media).

Media Manager operates differently with a StorageTek ACS robot (STK library or STK silo) than it does with most other robots. The main difference is that Media Manager does not keep slot locations for the media, since this information is provided by the ACS library software component of an ACS robot.

The *ACS library software* component can be any of the following STK products. See “Sample ACS Configuration” on page 378.

- ◆ Automated Cartridge System Library Software (ACSL)
- ◆ STK Library Station
- ◆ Storagetek 6000 Storage Domain Manager (SN6000)

This STK hardware serves as a proxy to another ACS library software component (such as, ACSL).

The term *Automated Cartridge System (ACS)* can refer to any of the following:

- ◆ A type of Media Manager robotic control.
- ◆ The StorageTek (STK) system for robotic control.
- ◆ The highest-level component of the STK ACS library software, which refers to a specific standalone robotic library or to multiple libraries connected with a media passthru mechanism.

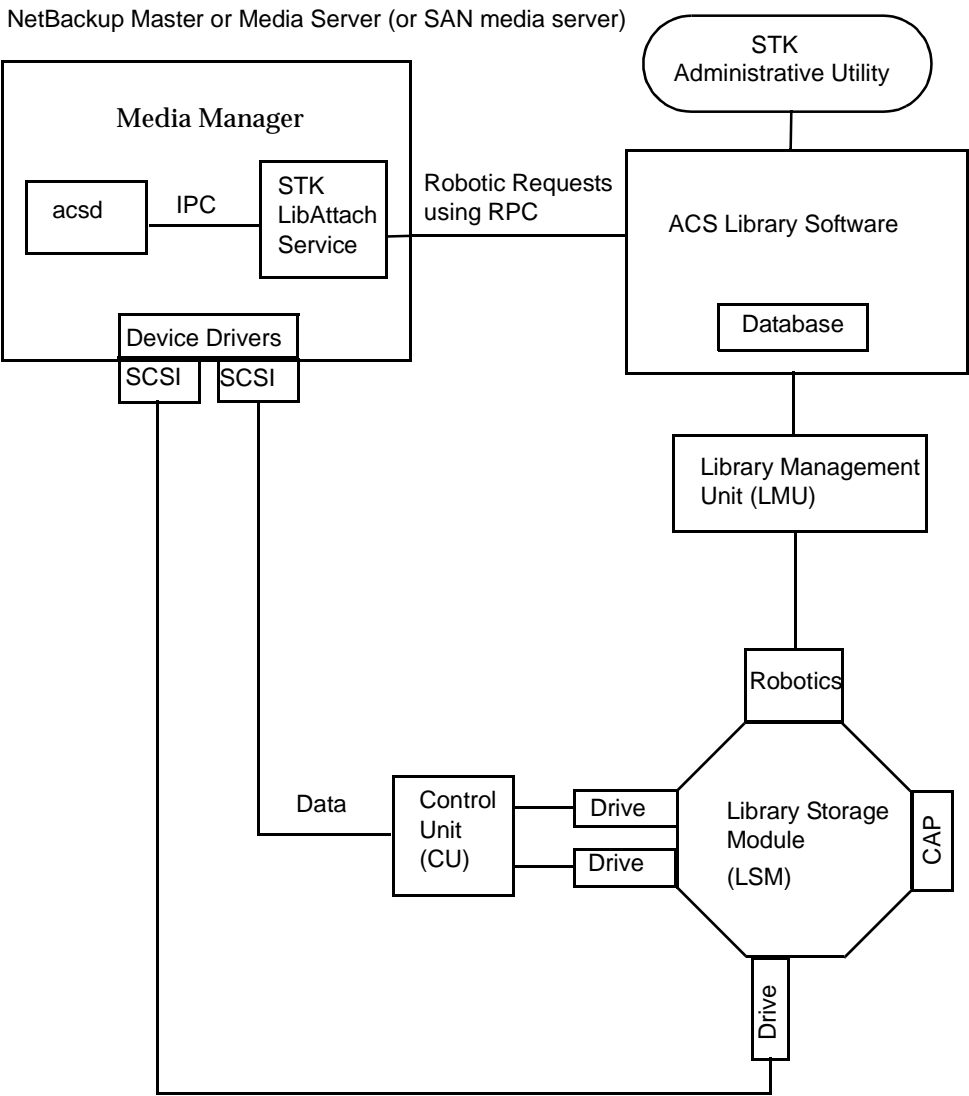
The topics in this appendix include the following:

- ◆ Typical ACS configurations.
- ◆ How Media Manager components handle media requests for an ACS robot.
- ◆ Configuration and operational differences to be aware of when using these robots.
- ◆ Advanced ACS topics.



Sample ACS Configuration

The following figure and accompanying table show a typical Automated Cartridge System configuration, and explain the major components in this configuration.



Component	Description
Media Manager server	<p>Acts as a client to the ACS library software host.</p> <p>The ACS robotic process (<code>acsrd</code>) formulates requests for mounts, unmounts, and inventories. An API then routes these requests to the STK LibAttach service using IPC communications. This service sends the requests to the ACS library software.</p>
STK LibAttach Service	<p>Library Attach for Windows is an ACS library software client application that enables Windows servers to use the StorageTek Nearline enterprise storage libraries.</p> <p>LibAttach provides the connection between Windows and ACS library software, through a TCP/IP network.</p> <p>Note LibAttach for Windows is not available for servers running Windows 2003.</p>
<p>ACS library software (any of the following)</p> <ul style="list-style-type: none"> Automated Cartridge System Library Software (ACSL) STK Library Station Storagenet 6000 Storage Domain Manager (SN6000) 	<p>Receives robotic requests from Media Manager and uses the Library Management Unit to find and mount, or unmount the correct cartridge on requests involving media management.</p> <p>On compatible host platforms, you may be able to configure ACS library software and Media Manager software on the same host.</p>
Library Management Unit (LMU)	Provides the interface between the ACS library software and the robot. A single LMU can control multiple ACS robots.
Library Storage Module (LSM)	Contains the robot, drives, and/or media.
Control Unit (CU)	<p>The Media Manager server connects to the drives through device drivers and a Control Unit (tape controller). The Control Unit may have an interface to multiple drives. Some Control Units also allow multiple hosts to share these drives.</p> <p>Most drives do not require a separate Control Unit. In these cases, the Media Manager server connects directly to the drives.</p>
CAP	Cartridge Access Port.



Media Requests

A request for media in an ACS robot begins in the same manner as other media requests. The NetBackup Device Manager service, `ltid`, receives the request for a specific tape volume and drive density, and queries the NetBackup Volume Manager service, `vmd`, for the location of the media. `vmd` returns only the robot number and media type, since Media Manager does not manage slot information for media in an ACS robot.

`ltid` verifies that the requested volume's media type and density are compatible. Next, `ltid` checks its internal tables (these tables are based on the device databases) to determine if there is an available drive and sends a mount request to the ACS process, `acsd`.

`acsd` formulates the request and uses Internal Process Communications (IPC) to send it to the STK LibAttach service. The request is then sent to the ACS library software by the LibAttach service.

ACS library software locates the media and sends the necessary information to the Library Management Unit, which directs the robotics to mount the media in the drive. When the LibAttach service (on the Media Manager server) receives a successful response from the ACS library software, it returns the status to `acsd`.

`acsd` waits for `avrd` to scan the drive. When the drive is ready, `acsd` sends a message to `ltid` that completes the mount request and enables the requesting application (for example, NetBackup) to start sending data to the drive.

Configuring ACS Robotic Control

When adding an ACS robot, specify the robot number, robot type, and the name of the host that contains the ACS library software. A device file is not used. The robotic control path is through the ACS library software host, and requests are handled by LibAttach (on Windows servers) or the `acssi` process (on UNIX servers).

Also see “Configuring Storage Devices” on page 17 for information on configuring ACS robots.

Configuring ACS Drives

An ACS robot supports DLT or 1/2-inch cartridge tape drives. If an ACS robot contains more than one type of DLT or 1/2-inch cartridge tape drive, you can configure an alternate drive type.

This means that there can be up to three different DLT and three different 1/2-inch cartridge drive types in the same robot. If you are using alternate drive types, it is important that the volumes are configured using the same alternate media type. Six drive types are possible, as follows: DLT, DLT2, DLT3, HCART, HCART2, and HCART3.

Use the same methods to create or identify device files for these drives as for other drives. If the drives are SCSI and connect to the robot through a shared control unit, you must specify the logical unit number (lun) for each drive, as they share the same SCSI ID.

Refer to the system documentation for your platform and operating system for details on configuring drives and logical unit numbers. The NetBackup Media Manager device configuration guide also has information on configuring device files.

Although device file configuration is essentially the same as for other robot-controlled drives, you must include the following additional information when defining the drives in Media Manager as robotic.

ACS Drive Coordinate	Description
ACS number	The index, in ACS library software terms, that identifies the robot that has this drive.
LSM number	The Library Storage Module that has this drive.
Panel number	The panel where the drive is located.
Drive number	The physical number of the drive in ACS library software terms.

Also see “Configuring Storage Devices” on page 17 for information on configuring ACS drives.

The following figure shows the location of this information in a typical ACS robot:



▼ To use the Device Configuration wizard

1. Run the Device Configuration wizard on one of the hosts where drives in an ACS-controlled library are attached. Allow the drives to be added as standalone drives.
2. Add the ACS robot definition and update each drive to indicate its appropriate position in the robot. Make each drive robotic and add the ACS, LSM, Panel, and Drive information.

See “Correlating Device Files to Physical Drives When Adding Drives” on page 306 for help in determining the correct addressing and verifying the drive paths.

3. After the drive paths have been verified on one host, re-run the wizard and specify that all hosts that have ACS drives in the library should be scanned.

The wizard will add the ACS robot definition and the drives to the remaining hosts with correct device paths (assuming that the devices and their serial numbers were successfully discovered and that the drive paths were correctly configured on the first host).

The use of SANs (including switches rather than direct connection) can increase the possibility of errors. If you are experiencing errors, you can manually define the tape drive configuration by using the NetBackup Administration Console or the command line.

Care must be taken to avoid any errors. With shared drives, the device paths must be correct for each server. Also ensure that the drives are defined correctly to avoid errors where drives are defined to be in ACS index number 9, instead of ACS index 0.

Using the STK SN6000

The StorageTek SN6000 provides tape drive virtualization. Logical tape drives are presented to host operating system interfaces (tape drivers), while robotic control is accomplished through the ACS API.

Some SN6000 configurations may involve a different number of *logical* drives compared to the number of *physical* drives (or equivalent resources) available for satisfying requests for drives. Also, the relationship between the number of logical drives and physical drives may change if hardware failures occur.

NetBackup scheduling, drive allocation, and drive assignment algorithms are only able to determine *logical* drive availability, and will attempt to fully utilize all configured and available logical drives. If the number of logical drives being utilized exceeds the number of physical drives available, a NetBackup job may be started when insufficient drive



resources are available to satisfy the job. The NetBackup job will encounter a resource issue when the scheduler initiates a job resulting in an ACS tape mount request. The mount request will then be re-queued within the ACS robotic process.

Should SN6000 Drives Be Configured as Shared Drives?

The answer depends on how you connect hosts to SN6000 ports. Each SN6000 port presents a distinct set of logical drives. Drives accessed from different ports have different ACS drive addresses (ACS, LSM, Panel, and Drive numbers) for each drive, as well as different serial numbers.

You must enter the Shared Drives license key on each media server where ACS drives in the SN6000 are configured.

Hosts Connected To a Single Port

If multiple hosts are connected to a single port, the logical drives accessible through that port are shared among the hosts connected to that port. The drive address and serial number is the same for each host on that port. In this type of configuration, the drives should be configured as *shared drives* in the NetBackup device configuration.

Hosts Connected To Different Ports

If each host is connected to a different port, each host will have its own set of logical drives and the drives should *not be* configured as shared drives in the NetBackup device configuration.

With this type of configuration, the SN6000 hardware is providing drive sharing and the NetBackup scheduler and robotic drive selection components are unable to avoid oversubscribing the drives. Tuning of the media mount timeout and backup policy windows may be needed to avoid backup, restore, or duplication delays, and media mount time outs.

NetBackup Tuning When Using Different Ports

Since there is a fixed limit for the number of drives that can be in use at any one time in this type of configuration, you should configure backup windows so the different NetBackup storage units tied to the same physical drives are active only at non-overlapping times. Also, raise or set the media mount timeout to infinite to prevent job failures when the job cannot get a physical drive due to all the drives being busy.

Adding Volumes

ACS robotic control software supports the following characters in a volume ID that are *not* considered valid media ID characters in NetBackup and Media Manager. (Volume ID is the ACS term for media ID).

- ◆ \$ (dollar sign)
- ◆ # (pound sign)
- ◆ The yen symbol
- ◆ Leading and trailing spaces

▼ To add ACS media

1. Add barcode labels to the media and insert the media into the robot using the media access port.
2. Do one of the following to empty the media access port and have the Library Storage Module read the barcode labels and pass the barcode information to the ACS library software, which uses the barcodes for volume IDs. The ACS library software also tracks the location of the tape within the robot.
 - ◆ Issue the ACS `enter` command from the STK Administrative interface (ACSSA).
 - ◆ Issue the ACS `enter` command from the Media Manager utility, `acctest`.
3. Define the media for Media Manager using the ACS volume IDs as media IDs. Do one of the following to define the media:
 - ◆ Update the volume configuration using the robot inventory function as explained in “Updating the Volume Configuration for a Robot” on page 162.
 - ◆ Add new volumes as explained in “Adding New Volumes” on page 119.

Since the ACS volume IDs and barcodes are the same, Media Manager also has the barcodes for the media. Note that you do not enter a slot location because that information is managed by ACS library software.
4. Use **Show Contents** and **Compare Contents with Volume Configuration** from the Media and Device Management Robot Inventory dialog to verify your configuration.

Removing Volumes

You can remove tapes using the STK utility or by using Media Manager.



Removing Volumes Using the STK Utility

If you remove media from an ACS robot, for example through the Cartridge Access Port using the STK administrative utility (see the figure in “Sample ACS Configuration” on page 378), you must logically move the media to standalone in the Media Manager volume database. To accomplish this, do one of the following:

- ❖ Update the volume configuration, as explained in “Updating the Volume Configuration for a Robot” on page 162.
- ❖ Move volumes as explained in “Moving Volumes” on page 130.

If you do not do this, Media Manager will not be aware that the media is missing and may issue mount requests for it. The result is an error, such as Misplaced Tape.

It does not matter, however, if you move media from one location to another within the robot. The ACS library software will find the requested media, if its database is current.

Removing Volumes Using Media Manager

You can remove volumes using one of the following methods. Either of these methods performs the logical move and the physical move.

- ❖ Use the NetBackup Administration Console (see “Methods for Ejecting Volumes From a Robot” on page 115).
- ❖ Use the `vmchange` command (see the NetBackup commands for Windows reference guide).

Robot Inventory Operations

Note An `INVENTORY_FILTER` entry is required in the `vm.conf` file if you are doing a robot inventory for an ACS robot and the ACS library software host is an STK Library Station.

Media Manager considers an ACS robot as one that supports barcodes. The following sequence explains what occurs when you select an operation that requires a robotic inventory of an ACS robot:

1. Media Manager requests volume information from the ACS library software.
2. The server responds by providing a listing of the volume IDs and media types from its database. The following table is an example of the ACS information that Media Manager receives:

ACS Volume ID	ACS Media Type
100011	DLTIV
200201	DD3A
412840	STK1R
412999	STK1U
521212	JLABEL
521433	STK2P
521455	STK2W
770000	LTO_100G
775500	SDLT
900100	EECART
900200	UNKNOWN

3. Media Manager translates the volume IDs into media IDs and barcodes. For example in the previous table, volume ID 100011 becomes media ID 100011 and the barcode for that media ID is also 100011.
4. If the operation does not require updating the volume configuration, Media Manager uses the media type defaults for ACS robots when it creates its report.
 “How Contents Reports for API Robots are Generated” on page 158 shows an example of this report.
5. If the operation requires updating the volume configuration, Media Manager maps the ACS media types to the Media Manager media types as explained in “Media Type Mappings Tab (Advanced Options)” on page 188.



The Update Volume Configuration report for an ACS robot is similar to the figure shown for an API robot in “Procedure To Update the Volume Configuration” on page 165.

Advanced ACS Robot Topics

The following sections cover these advanced NetBackup Enterprise Server topics:

- ◆ ACS Process (acsd)
- ◆ ACS Robotic Test Utility (acstest)
- ◆ Robotic Inventory Filtering

ACS Process (acsd)

acsd provides robotic control for mounting and dismounting volumes, and requesting inventories of volumes in a robotic library that is under the control of ACS library software. acsd interacts with and is started by the NetBackup Device Manager service (ltid).

acsd requests SCSI tape unloads through the system’s tape driver before using the ACS API to request tape dismounts. This matches other types of Media Manager robotic control, and accommodates configurations involving SCSI multiplexors. Loaded tapes are not forcibly ejected when a dismount operation occurs.

ACS Robotic Test Utility (acstest)

acstest allows you to verify ACS communications and provides a remote system administrative interface to an ACS robot. It can also be used to query, enter, eject, mount, unload, and dismount volumes. In addition, acstest allows you to define, delete, and populate ACS library software scratch pools.

acstest depends on the STK LibAttach service being started successfully. You can verify this service is started by using the **Services** tool available in **Administrative Tools** in the Windows control panel. acstest attempts to communicate with ACS library software using the LibAttach service.

acstest should not be used while acsd is servicing requests. Communication problems may occur if acsd and acstest are making ACS requests at the same time.

The usage format follows:

```
acstest -r ACS_library_software_host [-d device_name ACS, LSM, panel, drive] ... [-C sub_cmd]
```

The following example assumes that the LibAttach service has been started:

```
install_path\volmgr\bin\acstest -r einstein -d Tape0 0,0,2,1
```

Robotic Inventory Filtering

If your site has many volumes configured under ACS library software but you only want NetBackup to use a subset of them, you may be able to use inventory filtering.

Note An `INVENTORY_FILTER` entry is required if you are doing a robot inventory for an ACS robot and the ACS library software host is an STK Library Station.

Partial inventory functionality for ACS is accomplished by using the STK Administrative interface to create an ACS library software scratch pool or set of scratch pools. Then NetBackup can use these pools for backups.

The list of volumes returned in an ACS partial inventory includes the volumes that currently exist in the ACS scratch pool. ACS library software moves volumes out of the scratch pool after they have been mounted.

Therefore, a partial inventory *also* includes those volumes in the Media Manager volume database which Media Manager can validate exist in the robotic library, whether or not the volumes are in the ACS scratch pool. This complete list of volumes that exist in the robotic library is returned to prevent losing track of previously mounted volumes.

Inventory Filtering Example

1. Use the following STK Administrative interface (ACSSA) command to create a scratch pool, ID 4, with 0 to 500 as the range for the number of volumes:

```
ACSSA> define pool 0 500 4
```

2. Use the following STK Administrative interface (ACSSA) command to define the volumes in scratch pool 4:

```
ACSSA> set scratch 4 600000-999999
```

3. On the Media Manager server where the inventory request will be initiated add an `INVENTORY_FILTER` entry in the `vm.conf` file.

```
INVENTORY_FILTER = ACS robot_number BY_ACS_POOL acs_scratch_pool1
[acs_scratch_pool2 ...]
```

where

- ◆ *robot_number* is the number of the robot as configured in Media Manager.



- ◆ *acs_scratch_pool1* is the scratch pool ID as configured in ACS library software.
- ◆ *acs_scratch_pool2* is a second scratch pool ID (up to 10 scratch pools are allowed).

The following entry causes ACS robot number 0 to query scratch volumes from STK pool IDs 4, 5, and 6.

```
INVENTORY_FILTER = ACS 0 BY_ACS_POOL 4 5 6
```


Microsoft Removable Storage Manager (RSM)

C

Media Manager provides support for robotics under control of the Microsoft Windows Removable Storage Manager (RSM) interface.

In Media Manager, RSM-attached robotic devices are

- ◆ Classified as Media Manager robot type RSM
- ◆ Considered API robots (the robot manages its own media)

Support for these devices is different than for other types of Media Manager robotic control. This appendix provides an overview of those differences.

Media Manager and Microsoft RSM

Microsoft RSM presents a common interface to devices that are RSM-compatible and attached to a Microsoft Windows 2000 or later supported server. Media Manager supports the changer library devices listed on the Microsoft web site that contain drives that are shown in the supported drives list on the VERITAS support web site. Many of these devices vary in their support of features like barcodes and tape cleaning (tape cleaning is supported using the RSM application see “The Microsoft RSM Interface” on page 392).

Microsoft *RSM Libraries* represent physical layouts of the system (for example, robots and drives) and *RSM Media Pools* represent a logical layout of RSM media.

Media Manager *libraries* represent an individual changer, silo, robot, and so on. Also, Media Manager uses *Volume Pool* for a logical grouping of media (for example, all tapes currently available for backups) and *Volume Group* for a physical grouping of media (for example, all the tapes in a specific robot).

Because the devices and media are directly managed by Microsoft RSM, the Media Manager RSM process (`rsmcmd`) must always be running to configure media in Media Manager.

Considerations When Using Microsoft RSM

Before you configure a robot as an RSM robot, consider the following points:



- ◆ Your Media Manager device host must be running Windows 2000 or a later supported level.
- ◆ Microsoft Removable Storage Manager will control the robot and drives, rather than Media Manager.
- ◆ Media Manager library sharing, standalone drives, and shared drives (Shared Storage Option) are not supported.
- ◆ A robot configured as an RSM robot, cannot also be used as a Media Manager direct-controlled (SCSI) robot (for example, TLD).
- ◆ RSM robotic libraries could potentially be used by other applications.

The Microsoft RSM Interface

Use the Microsoft Removable Storage Manager to configure and manage your RSM media and devices. This interface is located in the **Computer Management** application. Documentation on how to use this interface is provided by Microsoft.

▼ To use the RSM interface

- ❖ Click **Start > Settings > Control Panel > Administrative Tools > Computer Management**.

Media Requests Involving an RSM Robot

A request for media in an RSM robot begins in the same manner as other media requests. The NetBackup Device Manager service (`ltid`) receives the request and queries the NetBackup Volume Manager service (`vmd`) for the location of the media. `vmd`, in this case, returns only the robot number and the type RSM for the robot.

Since Microsoft RSM manages the media and slots in RSM robots, the Media Manager volume database does not contain slot information for media in an RSM robot.

`ltid` then queries the volume database to retrieve the identifier (GUID or Globally Unique ID) assigned by RSM. `ltid` sends this information, along with the media name to the Media Manager RSM process (`rsmd`).

`rsmd` forwards the request to the Microsoft RSM software (the Removable Storage service). The Removable Storage service locates the media and directs the robotics to mount the media in the drive. When the host (where Media Manager is installed) receives a success response from the Removable Storage service, it allows the requesting application (for example, NetBackup) to start sending data to the drive.

Configuring RSM Robotic Control

Before adding any devices, it is important to verify that the Removable Storage service is aware of your device. Use the Removable Storage Manager application (see “The Microsoft RSM Interface” on page 392) to verify this.

Adding RSM-attached robots is similar to adding any robot on a Windows 2000 or later supported server. But instead of specifying the corresponding robot type for the device, you specify **RSM** as the Media Manager robot type. See “Adding Robots” on page 46 for information on configuring RSM robots.

As an alternative to using the **Devices** node of the NetBackup Administration Console, the following example uses the `tpconfig` command to configure an RSM robot:

```
tpconfig -add -robot 123 -roptype rsm -robpath changer0
```

The command returns the following information:

```
Added robot number 123 of type RSM to configuration
```

Configuring RSM Drives in Media Manager

Before configuring any device make sure that the Removable Storage service is aware of your device, by using the Removable Storage Manager application (see “The Microsoft RSM Interface” on page 392). Also, in order to configure an RSM drive, first configure the corresponding robot and be sure to specify this robot when configuring the drive.

Configuring a drive is similar to configuring any other drive on a Windows 2000 or later supported server. See “Adding Drives” on page 60 for information on configuring RSM drives.

As an alternative to using the **Devices** node of the NetBackup Administration Console, the following example uses the `tpconfig` command to configure an RSM drive:

```
tpconfig -add -drive -type dlt -name Tape0 -robot 123 -roptype rsm
                                             -robdrnum 1
```

The command returns the following information:

```
added drive index 0 of type dlt to configuration
```

Verifying a Configuration

You can use the `tpconfig -d` command to verify your configuration, which displays results similar to the following:

Index	DriveName	DeviceName	Type	Multihost	Status
*****	*****	*****	****	*****	*****



```
0    Drive0                \\.\\Tape0    dlt        NO        UP
      RSM(123) Definition    DRIVE=1
```

```
Currently defined robotics are:
RSM(123)    RSM Device Name = \\.\\Changer0,
            volume database host = host5
```

Activating a Configuration

If your changes are complete, stop and restart the NetBackup Device Manager service (this also stops and restarts any robotic processes).

▼ **To restart the Device Manager service**

1. Stop the NetBackup Device Manager service using **Stop/Restart Device Manager Service**, found on the **Actions** menu of the **Devices** node of the NetBackup Administration Console.
2. *This step applies only to NetBackup Enterprise Server.*
In the dialog, the arrow to the right of the **Device Host** box allows you to select a device host. The Current Status box shows the status of this host.
3. Start the NetBackup Device Manager service using **Stop/Restart Device Manager Service**.

Adding Volumes

Because the devices and media are directly managed by Microsoft RSM, RSM keeps track of volumes using its own database.

▼ **To add volumes**

1. Use the Microsoft RSM application (see “The Microsoft RSM Interface” on page 392) to move volumes from the Free Media Pool (the default media pool) to the NetBackup Media Pool. All volume activity (for example, mounts or dismounts) is through the NetBackup Media Pool.

Media names have to be unique within the Microsoft RSM library, even among different media types. For Media Manager to recognize media names they should be on both the Media Name and Side Name in the Microsoft RSM property sheet for the media.

The media ID used in the Media Manager volume database is the last six characters of the RSM media name. Therefore, two volumes with RSM media names of A000001 and B000001 are *not* considered to be unique by Media Manager.

If the last six characters of the RSM media name contain spaces, only the characters back to the first space are used. For example, for an RSM media name of AA BBB CCCC, the Media Manager media ID will be CCCC.

2. Since RSM volumes are tracked by their physical and partition GUIDs, volumes that are added must be located in the RSM database to capture their GUIDs. Therefore volumes added by Media Manager have to exist within the RSM NetBackup Media Pool for that robot.

Define the volumes for Media Manager using one of the following procedures:

- ◆ Update the volume configuration as explained in “Updating the Volume Configuration for a Robot” on page 162.
- ◆ Add new volumes as explained in “Adding New Volumes” on page 119.

Update the configuration when media has been moved or may have moved residences (see “Removing Volumes” on page 396).

3. Use **Show Contents** and **Compare Contents with Volume Configuration** from the Robot Inventory dialog of the **Media** node to verify your configuration.
4. The NetBackup **Allow media overwrite** setting must allow overwrite on MTF1 (this is necessary because Free Media Labels are in MTF format). Do the following:
 - a. From the NetBackup Administration Console, click **Host Properties**.
 - b. Select a media server.
 - c. Select **Actions > Properties**.
 - d. Select **Media**.
 - e. In the **Media** dialog, check the **MTF1** setting.
 - f. Click **OK**.



Removing Volumes

▼ To remove volumes

1. Use the Media Manager eject command, as explained in “Moving Volumes” on page 130 to remove the media from the RSM library.
2. Remove the media from the library as directed by the Removable Storage Manager interface. RSM moves volumes that have been ejected to the Off-line Media library.

Media Manager moves the volume to standalone in the Media Manager volume database. Media Manager also moves the volume to the RSM NetBackup Standalone Media media pool.

Robot Inventory Operations

Media Manager considers an RSM robot as one that supports barcodes. The following sequence explains what occurs when you select an operation that requires a robotic inventory for an RSM robot:

1. Media Manager requests volume information from the Removable Storage service.
2. The Removable Storage service responds by providing a list of media names and associated information from its database. Media Manager then displays a list of volumes obtained from the service along with their RSM and Media Manager media types. The following table indicates an example of information displayed by Media Manager:

RSM Media Name	Robot Contents RSM Media Type	Robot Contents Media Manager Media Type
MC120	AIT1_8mm	8mm
NN0402	DDS_4mm	4mm
002455	MP2_8mm	8mm

3. If the inventory operation does not require updating the volume configuration, Media Manager uses the media type defaults for RSM robots when it creates its report.

“How Contents Reports for API Robots are Generated” on page 158 shows an example of this report.



4. If the operation requires updating the volume configuration, Media Manager maps the RSM media types to the Media Manager media types, as explained in “Media Type Mappings Tab (Advanced Options)” on page 188.

The Update Volume Configuration report for an RSM robot is similar to the figure shown for an API robot in “Procedure To Update the Volume Configuration” on page 165.



Note *This appendix applies only to NetBackup Enterprise Server.*

Media Manager provides support for robotics under control of the IBM Automated Tape Library (ATL), including the IBM Magstar 3494 Tape Library.

Under Media Manager, robotic support for ATL robots is classified as Tape Library Half-inch (TLH) and these robots are also API robots (the robot manages its own media). Support for these devices is different than for other types of Media Manager robotic control. This appendix provides an overview of those differences.

Sample TLH Configurations

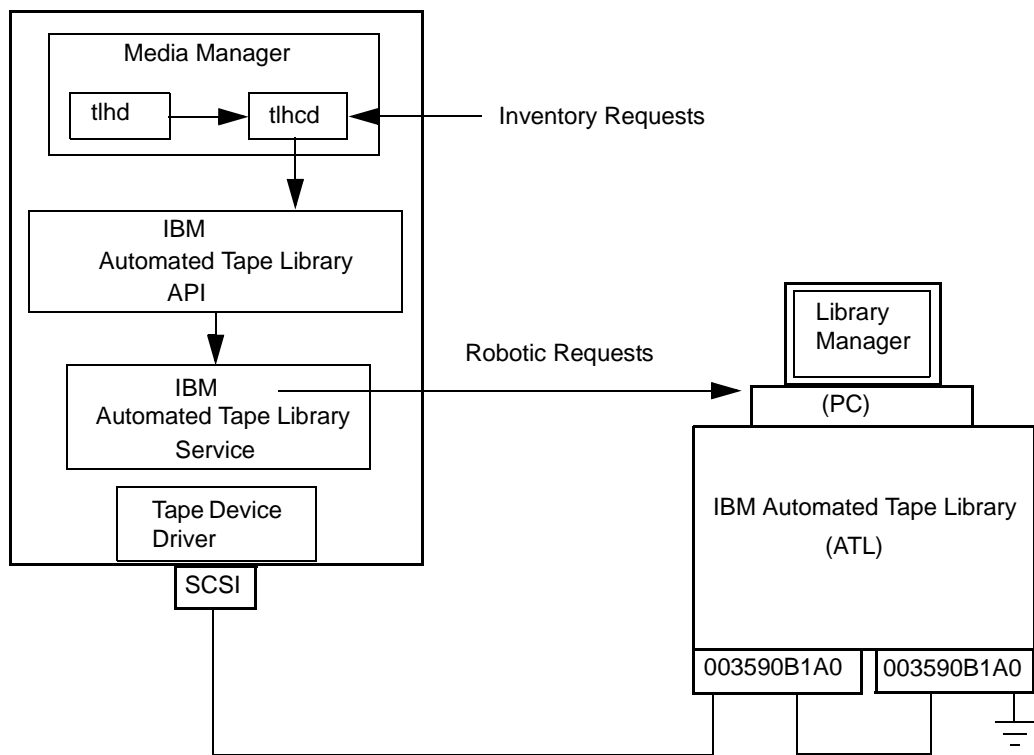
The following figures and accompanying table show two possible ATL configurations, and explain the major components in these sample configurations.



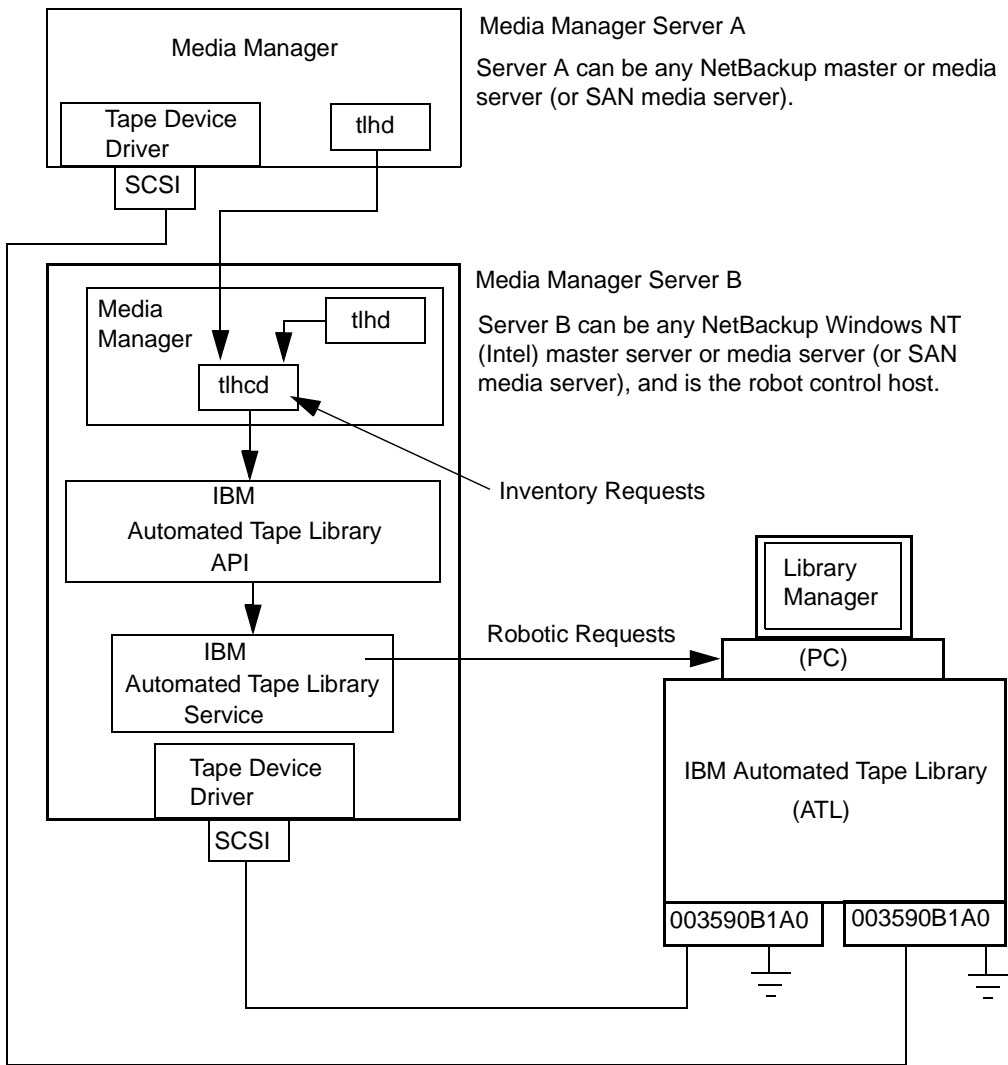
Robotic Control on Host with ATL Drives

Media Manager Server

This server can be a NetBackup master or media server (or SAN media server).



Robotic Control and Robot Connection on Separate Hosts



Component	Description
Media Manager Server	This host has Media Manager software installed and acts as a client to the Automated Tape Library through the IBM ATL service. The Netbackup Device Manager service forwards mount and dismount requests to the Tape Library Half-inch service (<code>tlhd</code>).
Tape Library Half-inch process (<code>tlhd</code>)	This process resides on a Media Manager server and passes mount and dismount requests to the Tape Library Half-inch control process (<code>tlhcd</code>) on the robotic control host.
Tape Library Half-inch control process (<code>tlhcd</code>)	This process receives mount or dismount requests from <code>tlhd</code> , or robot inventory requests through an external socket interface. <code>tlhcd</code> must reside on the same system that communicates with the IBM ATL service.
IBM Automated Tape Library service	A component of IBM ATL support. This software handles all communications with the Library Manager and must be running on any system from which the Automatic Tape Library is directly controlled.
Library Manager	A component of IBM ATL support that provides control of the robotics and robotic library. This is a PC that is usually located within the robot cabinet.
IBM Automated Tape Library (ATL)	An IBM physical library under automated robotic control.

Media Requests for a TLH Robot

A request for media in a TLH robot in an IBM Automated Tape Library begins in the same manner as other media requests. The Media Manager device service (`ltid`) receives the request and queries the Media Manager volume service (`vmd`) for the location of the media. The volume service, in this case, returns only the robot number and type for the TLH robot, since Media Manager does not manage slot information for media in a TLH robot.

`ltid` verifies that the type and density of the requested volume are compatible. Next, `ltid` checks its internal tables (these tables are based on the device databases) to determine if there is an available drive and sends a mount request to the TLH process (`tlhd`). This process passes the request to the TLH control process (`tlhcd`).



`tlhcd` resides on the host that has the Automatic Tape Library. This can be the same host where `tlhd` is running or another host. The control process communicates with the IBM ATL service through Tape Library system calls from an application library interface.

The IBM service passes the information to the Library Manager, which then locates the media and directs the TLH robotics to mount the media in the drive. When the host (where Media Manager is installed) receives a success response from the Library Manager, it allows NetBackup to start sending data to the drive.

Configuring Robotic Control

When adding TLH robotic control to Media Manager ensure that the following are true:

- ◆ The IBM Automated Tape Library is physically connected and configured correctly.

For information on configuring the IBM components of the Automated Tape Library, see the IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide (or any related publications).

For information on platform support for TLH robotic control, see the NetBackup release notes and the VERITAS support web site (<http://www.support.veritas.com>).

- ◆ You are using a recommended firmware version for the Automated Tape Library. Visit the VERITAS support web site to locate the recommended levels.

Robotic Control on a Windows System

The following topics explain the steps needed to configure robotic control when the Media Manager server is on a Windows system.

Determine the Library Name

Use the library name when configuring the robot in NetBackup. This name is set up when the Automated Tape Library is first configured (see the IBM system documentation). The library name is configured in the `C:\winnt\ibmatl.conf` file. Determine the library name by viewing the file.

The following is an example entry in that file:

```
3494AH          176.123.154.141          ibmpc1
```

Where:

- ◆ 3494AH is the library name.



- ◆ 176.123.154.141 is the IP address of the PC workstation that is running the Library Manager software.
- ◆ ibmpc1 is the host name of the PC workstation that is running the Library Manager software.

Verify Library Communications

After you determine the library name, verify library communications through the IBM-provided `mtlib` interface. Resolve all errors before attempting to configure IBM 3494 (TLH) support in Media Manager.

To verify communications with a specific library, specify the library name with the `mtlib` command. For example, if the library name is 3494AH, the following command verifies communications with the library:

```
mtlib -l 3494AH -qL
```

The following is the output from this command:

```
Library Data:
operational state.....Automated Operational State
                        Dual Write Disabled
functional state.....000
input stations.....1
output stations.....1
input/output status.....ALL input stations empty
                        ALL output stations empty
machine type.....3494
sequence number.....11398
number of cells.....141
available cells.....129
subsystems.....2
convenience capacity.....30
accessor config.....01
accessor status.....Accessor available
                        Gripper 1 available
                        Gripper 2 available
                        Vision system operational
comp avail status.....Primary library manager installed.
                        Primary library manager available.
                        Primary hard drive installed.
                        Primary hard drive available.
                        Convenience input station installed.
                        Convenience input station available.
                        Convenience output station installed.
                        Convenience output station available.
library facilities.....00
```

```

bulk input capacity.....0
bulk input empty cells.....0
bulk output capacity.....0
bulk output empty cells....0
avail 3490 cleaner.....0
avail 3590 cleaner.....92

```

Configure the Robotic Library Name

Configure the robotic path as explained in “Configuring Storage Devices” on page 17. When the configuration is complete you can view the robotic device information.

The following example uses `tpconfig -d` to view the robotic device information. This example has one TLH drive and one TLD drive.

```
tpconfig -d
```

```

Index  DriveName          Device Name      Type   Shared  Status
****  *
0      DRIVE2            \\.\\tape0      hcart   No      UP
      TLH(0) IBM Device Number = 156700
1      DRIVE1            \\.\\tape1      dlt     No      UP
      TLD(5) Definition  DRIVE=1
Currently defined robotics are:
      TLH(0)    library name = 3494AH, volume database host = grozer
      TLD(5)    SCSI port=3, bus=1, target=6, lun=0    volume database
                                                    host = grozer
Standalone drive volume database host = grozer

```

In this example, note the following line:

```
      TLH(0)    library name = 3494AH, volume database host = grozer
```

Where 3494AH is the library name and grozer is the volume database host for this robot.

Configuring Drives for TLH Robots

The TLH robot has half-inch cartridge tape drives, usually with a SCSI interface. You must install a system tape driver according to the appropriate system and vendor documentation.

See “Configuring Storage Devices” on page 17 for instructions on adding drives to your Media Manager configuration.



Caution When adding drives to Media Manager, it is important to assign the correct IBM device number to each drive. If the IBM device number is incorrect, tape mounts or backups may fail.

Use the Media Manager TLH test utility to determine the TLH drive designations. The following example uses `tlhtest` and shows which drives in the robot are under Media Manager control:

```
tlhtest -r 3494AH
```

The following is the output from `tlhtest` (the user entered the `drstat` command on the third line). You would use 003590B1A00 and 003590B1A01 when adding these drives in Media Manager.

```
Opening 3494AH
Enter tlh commands (? returns help information)
drstat
Drive information:
  device name:          003590B1A00
  device number:        0x156700
  device class:         0x10 - 3590
  device category:      0x0000
  mounted volser:       <none>
  mounted category:     0x0000
  device states:        Device installed in ATL.
                        Dev is available to ATL.
                        ACL is installed.

Drive information:
  device name:          003590B1A01
  device number:        0x156600
  device class:         0x10 - 3590
  device category:      0x0000
  mounted volser:       <none>
  mounted category:     0x0000
  device states:        Device installed in ATL.
                        Dev is available to ATL.
                        ACL is installed.

QUERY DEVICE DATA complete
```

Cleaning Drives

The IBM ATL interface does not allow applications to request or configure drive cleaning. For this reason, you cannot assign cleaning tapes to a TLH robot in the Media Manager volume configuration. You must configure drive cleaning by using an IBM administrative interface.



Adding Volumes

▼ To add volumes

1. Add barcode labels to the media and insert the media into the robot using the media access port.

The Library Manager reads the barcodes and classifies the media by media type. A category is assigned to each volume. Some volume categories will restrict application access to certain volumes. Volume locations are tracked by the Library Manager.

2. Define the media to Media Manager by using the ATL volume IDs as media IDs. To accomplish this, do one of the following:
 - ◆ Update the volume configuration using the robot inventory function, as explained under “Updating the Volume Configuration for a Robot” on page 162.
 - ◆ Add new volumes as explained under “Adding New Volumes” on page 119.

Since the ATL volume IDs and barcodes are the same, Media Manager has the barcodes for the media. Notice that you do not enter slot location because that information is kept by the ATL software.

3. Use **Show Contents** and **Compare Contents with Volume Configuration** from the Robot Inventory dialog of the **Media** node to verify your configuration.

Removing Volumes

▼ To remove volumes

1. Physically remove the media from the library using one of the following:
 - ◆ An IBM Library Manager interface.
 - ◆ The `eject` command in the Media Manager `tlhtest` utility.
 - ◆ The NetBackup Administration Console (see “Methods for Ejecting Volumes From a Robot” on page 115).
 - ◆ The `vmchange` command (see the NetBackup commands for Windows reference).
2. If you are using the `vmchange` command or the NetBackup Administration Console (see step 1), you can skip this step.

Update the Media Manager volume database to indicate the new location of the media as being standalone. To accomplish this, do one of the following:



- ◆ Update the volume configuration, as explained in “Updating the Volume Configuration for a Robot” on page 162.
- ◆ Move volumes as explained in “Moving Volumes” on page 130.

Otherwise, Media Manager is not aware that the media is missing and may issue mount requests for it. The result is an error such as Misplaced Tape.

It does not matter if you physically move media from one location to another within the robot. The Automated Tape Library will find the media when Media Manager requests it.

Robot Inventory Operations

Media Manager considers a TLH robot as one that supports barcodes. The following sequence explains what occurs when you select an operation that requires a robotic inventory for a TLH robot:

1. Media Manager requests volume information from the Library Manager through the Library Manager Control Point IBM service.
2. The Library Manager responds by providing a list of volume IDs and volume attributes from its database. Media Manager then filters out volume categories that cannot be used and displays a list of volumes obtained along with a translated version of the volume's media type. The media type is based upon the attributes that were returned.

The following table shows an example of the types of information that Media Manager receives:

TLH Volume ID	TLH Media Type
PFE011	3480
303123	3490E
CB5062	3590J
DP2000	3590K

3. Media Manager translates the volume IDs into media IDs and barcodes. In the previous table, volume ID PFE011 becomes media ID PFE011 and the barcode for that media ID is also PFE011.

4. If the operation does not require updating the volume configuration, Media Manager uses the media type defaults for TLH robots when it creates its report.

“How Contents Reports for API Robots are Generated” on page 158 shows an example of this report.

5. If the operation requires updating of the volume configuration, Media Manager maps the TLH media types to the Media Manager media types as explained in “Media Type Mappings Tab (Advanced Options)” on page 188.

The Update Volume Configuration report for an ACS robot is similar to the figure shown for an TLH robot in “Procedure To Update the Volume Configuration” on page 165.

Robotic Inventory Filtering

If your site has many volumes configured, but you only want NetBackup to use a subset of them, you may be able to use inventory filtering.

The IBM Library Manager maintains the concept of a volume category, which can be used to classify volumes into pools, including pools by application.

On the Media Manager server where the inventory request will be initiated, you can add an `INVENTORY_FILTER` entry in the `vm.conf` file. The format for this entry follows:

```
INVENTORY_FILTER = TLH robot_number BY_CATEGORY value1 [value2 . . .]
```

where

- ◆ *robot_number* is the robot number.
- ◆ *value1* is a filter value of type IBM category (if *filter_type* = `BY_CATEGORY`).
- ◆ *value2* is a second filter value (up to 10 filter values are allowed).

For example:

```
INVENTORY_FILTER = TLH 0 BY_CATEGORY 0xcdb0
```





ADIC Distributed AML Server/Scalar Distributed Library Controller

E

Note *This appendix applies only to NetBackup Enterprise Server.*

Media Manager provides support for robotics under control of either an ADIC Distributed AML Server (DAS) or a Scalar Distributed Library Controller (SDLC), including those in the ADIC Automated Media Library (AML) family. See “Sample TLM Configuration” on page 411.

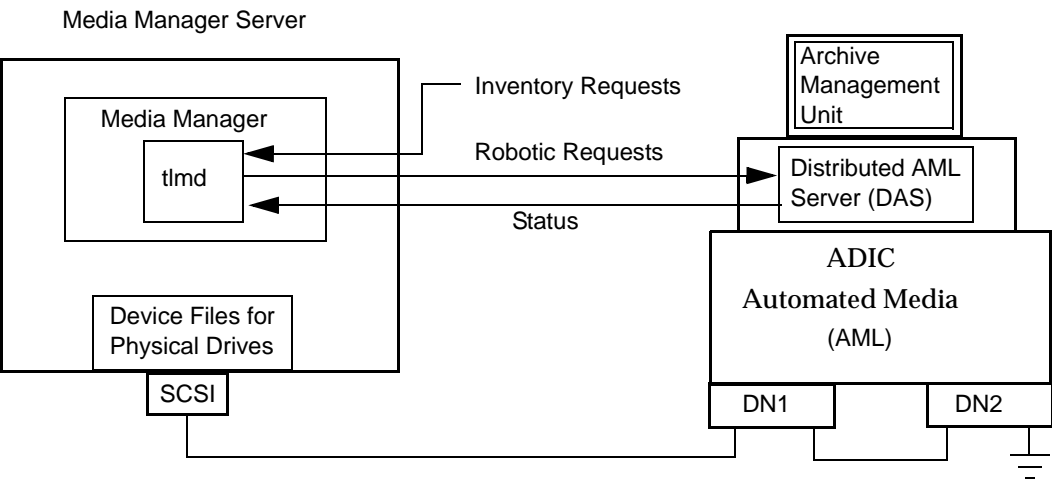
Portions of this appendix use the term *DAS/SDLC* to refer to either of these ADIC software products. Other portions use the terms *DAS* or *SDLC* when referring to a particular ADIC software product.

Under Media Manager, robotic support for these robots is classified as Tape Library Multimedia (TLM) and these robots are also API robots (the robot manages its own media). Support for these devices is different than for other types of Media Manager robotic control and this appendix provides an overview of those differences.

Sample TLM Configuration

The following figure and accompanying table show a possible configuration using Distributed AML Server software, and explain the major components in this sample configuration.





Component	Description
Media Manager Server	A host that has Media Manager software and acts as a client to the DAS/SDLC server. Netbackup Device Manager service forwards mount and dismount requests to the TLM service (t1md).
TLM process (t1md)	This process passes mount and dismount requests to the DAS/SDLC server and handles return status. t1md also receives and handles robot inventory requests.
Archive Management Unit (AMU)	A PC running an IBM OS/2, Windows NT, or Windows 2000 operating system, usually located in or near the AML cabinet. The ADIC software runs on the AMU.
Distributed AML Server (DAS) Scalar Distributed Library Controller (SDLC)	These are two ADIC client/server software products that reside in the Archive Management Unit and provide shared access to the family of Automated Media Libraries (AML). The Media Manager robotic process (or TLM process) acts as a client to the DAS/SDLC server.
Automated Media Library (AML)	An ADIC multimedia robotic library.

Media Requests Involving a TLM Robot

A request for media in a TLM robot begins in the same manner as other media requests. The Media Manager device service, `ltid`, receives the request and queries the Media Manager volume service, `vmd`, for the location of the media. The volume service, in this case, returns only the robot number and type TLM robot. The Media Manager volume database does not manage slot information for media in a TLM robot.

`ltid` verifies that the type and density of the requested volume are compatible. Next, `ltid` checks its internal tables (these tables are based on the device databases) to determine if there is an available drive and sends a mount request to the TLM process, `tlmd`. This process passes the request to the DAS or SDLC server software (which resides in the Archive Management Unit).

The DAS/SDLC server locates the media and directs the robotics to mount the media in the drive. When the host (where Media Manager is installed) receives a success response from the server, it allows the requesting application (for example, NetBackup) to start sending data to the drive.

Note With TLM robotic control, the Media Manager server is considered to be a DAS/SDLC client and sends robotic control requests to the DAS/SDLC server. This relationship pertains only to the DAS/SDLC client/server model and is not related in any way to the concept of NetBackup servers or clients.

Configuring TLM Robotic Control

When configuring TLM robotic control for Media Manager, first ensure that the ADIC Automated Media Library has been physically connected and configured.

For information on initially configuring the ADIC components of the Automated Media Library, see the ADIC documentation. Pay close attention to the DAS or SDLC component, which is described in the ADIC installation and administration guides.

For information on platform support for TLM robotic control, see the NetBackup release notes.

Configuring TLM Drives on a DAS/SDLC Server

Before configuring drives for Media Manager, you must configure the DAS or SDLC server to allocate the desired drives to a specific DAS/SDLC client (the Media Manager server). The following topics pertain to this configuration.



Note See the ADIC documentation for detailed instructions on configuring the DAS/SDLC server.

Installing ADIC Software for the Client Component

Use the following procedure to install ADIC software on Windows servers. Also refer to the ADIC users guide for Windows DAS clients.

▼ To install and configure ADIC software

1. Set the following system environment variables and values on the Windows host (right-click on **My Computer** > **Properties** > **Environment**).

- ◆ Variable Name: DAS_CLIENT
- ◆ Variable Value: *name_of_NetBackup_media_server*
- ◆ Variable Name: DAS_SERVER
- ◆ Variable Value: *name_of_DAS_server*

2. Copy the following DLLs to windows\system32 (or *install_path*\Volmgr\bin).

```
aci.dll  
ezrpcw32.dll  
winpc32.dll
```

3. Run `portinst.exe`

This installs the NobleNet Portmapper for TCP service. Set this service to start automatically when the server is started. NobleNet Portmapper is provided with the Windows DAS client.

Configuring the DAS/SDLC Client Name

The DAS/SDLC client name required for the Media Manager server is entered in the configuration file on the DAS/SDLC server. It is important that this name is the same name being used by Media Manager, and that it is a valid client name.

By default the Media Manager server uses as its DAS/SDLC client name, the host name that it obtains from the `gethostname()` system call. This name is usually the one that you use for the client name in the configuration file on the DAS/SDLC server.

However, if this name is invalid for DAS/SDLC clients you will have to use another name. For example, DAS 1.30C1 does not allow hyphens in client names. If the host name (where Media Manager is installed) has a name such as dolphin-2, the DAS/SDLC server will not recognize it.

A similar problem exists if a Media Manager server's short host name is being used as the client name, but `gethostname()` returns the long host name.

▼ To resolve client name problems

1. Substitute a valid client name on the DAS/SDLC server. For example, use dolphin2.
2. Set the `DAS_CLIENT` Windows operating system environment variable to this name, for example dolphin2.
3. Stop and start the `ltid` service to enable the TLM process to use the new client name.
4. When the client names are correct, restart the DAS/SDLC server with the latest configuration file and then reallocate the drives to Media Manager.

Allocating TLM Drives on a DAS Server

When the client names are correct (see “Configuring the DAS/SDLC Client Name” on page 414), allocate the drives to the Media Manager server by using the `DASADMIN` administrative command.

The DAS administrative drive allocation commands are not available from the Media Manager TLM test utility interface. You must use an administrative interface on the DAS server or the DAS client administrative interface.

▼ To allocate TLM drives

The following example uses `DASADMIN` to allocate drives:

```
LD_LIBRARY_PATH=/usr/local/aci/lib
export LD_LIBRARY_PATH
DAS_SERVER=dasos2box
export DAS_SERVER
DAS_CLIENT=grouse
export DAS_CLIENT
cd /usr/local/aci/admin
./dasadmin listd
```

The following is sample output from this command:

```
==>listd for client: successful
    drive: DN1  amu drive: 01  st: UP  type: N  sysid:
```



```
client: grouse volser:   cleaning 0  clean_count: 17
drive: DN2  amu drive: 02  st: UP  type: N  sysid:
client: mouse volser:   cleaning 0  clean_count: 4
./dasadmin allocd
```

The following is sample output from this command:

```
==> usage: dasadmin allocd drive-name UP|DOWN clientname
```

(First allocate it DOWN on one client, then UP on another as in the following:)

```
./dasadmin allocd DN2 DOWN mouse
./dasadmin allocd DN2 UP grouse
```

Configuring TLM Drives on a SDLC Server

When the client names are correct (see “Configuring the DAS/SDLC Client Name” on page 414), configure the drives for the Media Manager server.

▼ To configure TLM drives

1. Start the SDLC console and choose **Configuration > Clients**.
Enter the client name for the value of **Name**.
Enter the network host name for the value of **Client Host Name**.
2. Select the **Drive Reservation** tab on the client and choose **UP** for the drives that you want to allocate to this client.

Configuring TLM Drives in Media Manager

A TLM robot has half-inch cartridge tape drives, usually with a SCSI interface. You must install a system tape driver according to the appropriate system and vendor documentation.

See “Configuring Storage Devices” on page 17 for instructions on how to add the drives to a Media Manager configuration.

Caution When adding drives to Media Manager, it is especially important to assign the correct DAS/SDLC drive name to each drive. If the drive name is incorrect, tape mounts or backups may fail.

Use the Media Manager TLM test utility to determine the DAS/SDLC drive designations. The following example uses `tlmtest`:

```
tlmtest -r dasos2box
```

The following is the output from this utility (the user entered the `drstat` command on the third line).

```
Current client name is 'grouse'.
Enter tlm commands (? returns help information)
drstat
Drive 1: name = DN1, amu_name = 01, state = UP, type = N,
        client = grouse, volser = , cleaning = NO, clean_count = 17
Drive 2: name = DE3, amu_name = 03, state = UP, type = E,
        client = grouse, volser = , cleaning = NO, clean_count = 480
Drive 3: name = DE4, amu_name = 04, state = UP, type = E,
        client = grouse, volser = , cleaning = NO, clean_count = 378
DRIVE STATUS complete
```

This output indicates that DAS/SDLC drive names DN1, DE3, and DE4 should be used. It also shows that grouse is the client name that is being used for the Media Manager server.

Configuring Shared TLM Drives

Use one of the following procedures depending on which ADIC client/server software you are using.

Configuring the ADIC DAS Server

Using TLM robots with SSO requires that the ADIC DAS server be configured to allow drives to be allocated simultaneously to all NetBackup media servers that are sharing the drives (for ADIC software, these servers are considered to be clients). DAS server software version 3.01.4 or higher is needed.

▼ To configure the DAS server

This example has two UNIX media servers (server_1 has IP address xxx.xxx.xxx.xxx and server_2 has IP address yyy.yyy.yyy.yyy).

In this example, the client name is set to NetBackupShared, but can be any name without special characters.

1. Modify the DAS server's `\ETC\CONFIG` file to create a shared client entry.

```
client client_name = NetBackupShared
# ip address = 000.000.000.000
hostname = any
```

2. Place the IP addresses of all media servers that will use the shared client entry in the `\MPTN\ETC\HOSTS` file on the DAS server.



```
xxx.xxx.xxx.xxx server_1
yyy.yyy.yyy.yyy server_2
```

3. Using the DASADMIN interface, choose **UP** for the drives that you want to allocate to the shared client (NetBackupShared).
4. On each of the media servers that are sharing the drives, create an entry in the `vm.conf` file with the shared DAS client name, such as the following:

```
DAS_CLIENT = NetBackupShared
```

5. Test the DAS configuration using `robtest` and `tlmtest`. Set the client name (use `client NetBackupshared` in `tlmtest`) and run the drive status command (`drstat`).

On Windows clients (media servers), the client name is obtained from the `DAS_CLIENT` environment variable so the `client` command is not needed in `tlmtest`.

Configuring the ADIC SDLC Server

Using TLM robots with SSO requires that the ADIC SDLC server be configured to allow drives to be allocated simultaneously to all NetBackup media servers that are sharing the drives (to ADIC software, these servers are considered to be clients). SDLC software version 2.3 or higher is needed.

▼ To configure the SDLC server

In this example, the client name for the shared client is set to NetBackupShared, but can be any name without special characters.

1. Start the SDLC console and choose **Configuration > Clients**.
Enter NetBackupShared for the value of **Name**.
Enter any for the value of **Client Host Name**.
2. Select the **Drive Reservation** tab on the shared client (NetBackupShared) and choose **UP** for the drives that you want to allocate to the shared client.

3. On UNIX clients (media servers) that are sharing the drives, create an entry in the `vm.conf` file with the shared client name, such as the following:

```
DAS_CLIENT = NetBackupShared
```

On Windows clients (media servers) that are sharing the drives, set the `DAS_CLIENT` Windows operating system environment variable to NetBackupShared.

4. Test the SDLC configuration using `robtest` and `tlmtest`. Set the client name (use `client NetBackupshared` in `tlmtest`) and run the drive status command (`drstat`).

On Windows clients (media servers), the client name is obtained from the `DAS_CLIENT` environment variable so the `client` command is not needed in `tlmtest`.

Using the Device Configuration Wizard in Media Manager

The following procedure uses the Device Configuration wizard to configure drives in a SSO configuration. Using this procedure can significantly reduce the amount of manual configuration required in an SSO environment. For example, if you have 20 drives shared on 30 hosts, these configuration steps require just 20 device paths to be manually configured, instead of 600 device paths.

During the setup phase, the wizard will attempt to discover the tape drives available; and for the robot types where serialization is available, the positions of the drives within the library. This wizard does not obtain drive serial numbers from the TLM robotic library control interface, so some manual configuration is required.

▼ To use the Device Configuration wizard

1. Run the Device Configuration wizard on one of the hosts where drives in an TLM-controlled library are attached. Allow the drives to be added as standalone drives.
2. Add the TLM robot definition and update each drive to indicate its appropriate position in the robot. Make each drive robotic.

See “Correlating Device Files to Physical Drives When Adding Drives” on page 306 for help in determining the correct addressing and verifying the drive paths.

3. After the drive paths have been verified on one host, re-run the wizard and specify that all hosts that have TLM drives in the library should be scanned.

The wizard will add the TLM robot definition and the drives to the remaining hosts with correct device paths (assuming that the devices and their serial numbers were successfully discovered and that the drive paths were correctly configured on the first host).

The use of SANs (including switches rather than direct connection) can increase the possibility of errors. If you are experiencing errors, you can manually define the tape drive configuration by using the NetBackup Administration Console or the command line.



Care must be taken to avoid any errors. With shared drives, the device paths must be correct for each server. Also ensure that the drives are defined correctly to avoid errors.

Providing Common Access to Volumes

If you use the same volume database for all Media Manager servers (recommended by VERITAS), each server must have access to the same sets of volumes (volsers) in the DAS/SDLC configuration. Otherwise, when you perform an update volume configuration from one of the servers, the volumes that are not configured for that server will be logically moved to a standalone residence.

As a test, you can inventory a TLM robot from each Media Manager server and compare the results. If all the inventory reports are not the same, correct the DAS/SDLC configuration. Then, perform a shutdown on the DAS/SDLC server and restart.

Adding Volumes

▼ To add media

1. Add barcode labels to the media and insert the media into the library using the media access port (insert area).
2. Do one of the following to empty the media access port and have the AMU Archive Management Software read the barcodes, classify the media by media type, and track storage cell locations for the media:
 - ◆ Select the robot inventory update inventory function and select **Empty media access port prior to update**. In step 3 continue using the robot inventory function to update the volume configuration.
 - ◆ Issue the DAS insert directive from a DAS administrative interface. You can obtain the insert area name from the DAS configuration file.
 - ◆ Issue the DAS insert directive from the Media Manager utility, `tlmtest`. You can obtain the insert area name from the DAS configuration file.
3. Define the media to Media Manager by using the DAS/SDLC volsers as media IDs. To accomplish this, do one of the following:
 - ◆ Update the volume configuration using the robot inventory function, as explained under “Updating the Volume Configuration for a Robot” on page 162.
 - ◆ Add new volumes as explained under “Adding New Volumes” on page 119.

Since the DAS/SDLC volumes and barcodes are the same, Media Manager now also has the barcodes for the media. Notice that you do not enter slot location because that information is kept by the ADIC software.

4. Use **Show Contents** and **Compare Contents with Volume Configuration** from the Media and Device Management Robot Inventory dialog to verify your configuration and maintain consistency between the DAS/SDLC database and the Media Manager volume configuration. That is, update the Media Manager configuration when media has moved or may have moved.

Removing Volumes

▼ To remove media

1. Physically remove the media from the library using one of the following:
 - ◆ A DAS/SDLC administrative interface.
 - ◆ The `eject` command in the Media Manager `tlmtest` utility.
 - ◆ The NetBackup Administration Console (see “Methods for Ejecting Volumes From a Robot” on page 115).
 - ◆ The `vmchange` command (see the NetBackup commands for Windows reference).
2. If you are using the `vmchange` command or the NetBackup Administration Console (see step 1), you can skip this step.

Update the Media Manager volume database to indicate the new location of the media as being standalone. To accomplish this, do one of the following:

- ◆ Update the volume configuration, as explained in “Updating the Volume Configuration for a Robot” on page 162.
- ◆ Move volumes as explained in “Moving Volumes” on page 130.

Otherwise, Media Manager is not aware that the media is missing and may issue mount requests for it. The result is an error such as “Misplaced Tape”.

It does not matter if you physically move media from one location to another within the robot. The DAS/SDLC AMU will find the media when Media Manager requests it.



Robot Inventory Operations

Media Manager considers a TLM robot as one that supports barcodes. The following sequence explains what occurs when you select an operation that requires a robotic inventory for a TLM robot:

1. Media Manager requests volume information from the DAS or SDLC server through a DAS/SDLC application library call.
2. The server responds by providing a list of volume IDs and associated information from its database. Media Manager filters out volumes that are not occupied in their home cell locations or in drives, then displays a list of volumes obtained along with their media types according to the DAS/SDLC server.

The following table indicates an example of information displayed by Media Manager:

TLM Volser	TLM Media Type
A00250	3480
J03123	3590
DLT001	DECDLT
MM1200	8MM
NN0402	4MM
002455	UNKNOWN

3. Media Manager translates the volsers directly into media IDs and barcodes. In the previous table, volser A00250 becomes media ID A00250 and the barcode for that media ID is also A00250.
4. If the operation does not require updating the volume configuration, Media Manager uses the media type defaults for TLM robots when it creates its report.
“How Contents Reports for API Robots are Generated” on page 158 shows an example of this report.
5. If the operation requires updating the volume configuration, Media Manager maps the TLM media types to the Media Manager media types as explained in “Media Type Mappings Tab (Advanced Options)” on page 188.



The Update Volume Configuration report for an TLM robot is similar to the figure shown for an API robot in “Procedure To Update the Volume Configuration” on page 165.





Index

Symbols

(RSM) see Removable Storage Manager

A

Access Management 19, 93, 213
accessibility features xxxi
ACS (see Automated Cartridge System)
ACS or TLM robot types 254, 267
ACS, TL8, TLD, TLH, or TLM robot
types 251
ACS, TLH, or TLM robot types 251
ACS_ vm.conf entry 357
acsd process 388
acstest 385, 388
adding
cleaning tapes 73
drives 60
robot 46
shared drives 57
volume pool 109
volumes
actions menu 122
update volume configuration 122
ADIC Automated Media Library (AML) 411
ADIC software, installing 413
ADJ_LSM, vm.conf entry 357
administrator quick reference 352
advanced configuration topics 335
advanced options, robot inventory 154, 166
Allow Backups to Span Media 341
Allow Media Overwrite 338
allowable Media Manager characters 34,
105, 229
alternate media types
ACS robots 380
defined 279
example 279
AML (see Distributed AML Server)
AMU (see Archive Management Unit)

API robots 2, 135, 166, 188, 322, 377, 391, 399,
411
API_BARCODE_RULES, vm.conf entry 358
Arbitrated Loop Physical Address
(ALPA) 260
Archive Management Unit (AMU) 412
assigned
host, drive status 223
volumes 142
assigning tape requests 239
ATL (see Automated Tape Library)
authentication/authorization 40, 347
AUTHORIZATION_REQUIRED, vm.conf
entry 359
auto cleaning 264, 310
AUTO_UPDATE_ROBOT, vm.conf
entry 359
Automated Cartridge System
adding volumes 385
barcode operations 386
configuration example 87
drive information 67
Library Server (ACSLs) 377, 379
media requests 380
removing tapes 385
special characters 385
STK Library Station 377, 379
Storagenet 6000 (SN6000) 377, 379, 383
Automated Tape Library (ATL) 402
Automatic Volume Recognition (AVR)
setting 214
AVRD_PEND_DELAY, vm.conf entry 304,
360
AVRD_SCAN_DELAY, vm.conf entry 359

B

Backup Exec, managing volumes 91, 153,
237
barcode rules



- add 179
- change 180
- overview 323
- tag 181
- barcodes
 - overview 321
 - update in robot 153, 207
- bp.conf file 305, 337
- bpclntcmd utility 250
- bpexpdate command 143

C

- changing
 - cleaning frequency 65, 74, 236
 - cleanings allowed 148, 314
 - drive configuration 70
 - host
 - for Device Monitor 231
 - for standalone drives 71
 - media description 147
 - robot configuration 69
 - shared drive configuration 70, 71
 - volume attributes 144
 - volume expiration date 146
 - volume group name 148
 - volume maximum mounts 146
 - volume pool attributes 111
 - volume pool for a volume 112, 147
- character device 64
- CLEAN_REQUEST_TIMEOUT, vm.conf entry 361
- cleaning
 - count 103
 - drives 73, 234, 406
 - frequency-based 73, 234, 310, 312
 - library-based 310
 - operator-initiated 74, 235, 310
 - reactive 310
- cleaning tape
 - change cleanings allowed 148, 314
 - number of cleanings left 103
 - set count 127
- CLIENT_PORT_WINDOW, vm.conf entry 362
- cluster environments 306, 370
- CLUSTER_NAME, vm.conf entry 370
- comment
 - drive, adding 236
 - in drive status list 224

- configuring
 - devices 247
 - drives and robots 17
 - examples, drives and robots 80
 - media 44, 119
 - STK SN6000 drives 384
 - TLM drives 413
- CONNECT_OPTIONS, vm.conf entry 362
- control mode, drive 220
- control path, robotic 53
- control unit, ACS 379
- crawlreleasebyname, vmopr cmd option 303
- create media ID generation rules 166
- customize
 - Device Monitor window 228
 - Devices window 32
 - Media window 105

D

- DAS (see Distributed AML Server)
- DAS drive name 27
- DAS_CLIENT, environment variable 415
- DAS_CLIENT, vm.conf entry 363
- DASADMIN command 415, 418
- data loss 299
- DataStore volume pool 315
- DAYS_TO_KEEP_LOGS, vm.conf entry 363
- deassign volumes 142
- decommission a media server 336
- deleting
 - drive 72
 - volume group 137
 - volume pool 113
 - volumes 136
- density for media types 226
- denying requests 243
- description, for new volume 126
- device
 - character 64
 - configuration wizard 14, 44, 58, 60, 69, 254, 261, 382, 419
 - discovery 34, 45, 295
 - drivers 247, 248
 - files 248
 - no rewind 64
 - volume header 64
- device allocation host 251, 267, 268
- Device Configuration wizard 306, 382, 419
- device databases 276



-
- device file, robotic 53
 - device host, viewing remotely 38
 - device mapping file 36
 - Device Monitor
 - add drive comment 236
 - assigning requests 239
 - changing host 231
 - display pending requests 237
 - display the window 212
 - overview 211
 - resubmit request 242
 - DEVICE_HOST, vm.conf entry 364
 - Devices management window
 - displaying 18
 - menus 19
 - status bar 31
 - toolbar 21
 - DISABLE_AUTO_PATH_CORRECTION, vm.conf entry 364
 - DISABLE_SCSI_RESERVE bp.conf entry 305
 - DISABLE_STANDALONE_DRIVE_EXTENSIONS 120
 - DISALLOW_NONNDMP_ON_NDMP_DRIVE, vm.conf entry 364
 - Distributed AML Server
 - \ETC\CONFIG file 417
 - \MPTN\ETC\HOSTS file 417
 - overview 411
 - Distributed AML Server (also see Tape Library Multimedia)
 - DO_NOT_EJECT_STANDALONE, vm.conf entry 365
 - down a device 339
 - down drive, setting 214
 - drive
 - add comment 236
 - changing operating mode 232
 - character device 64
 - cleaning 21, 215, 252, 264
 - cleaning frequency 65, 236
 - control mode 220
 - diagnose tests 21
 - dip switches 250
 - initial state 61
 - initial status 61
 - monitoring use 211
 - no rewind device 64
 - performing diagnostics 74
 - reset 233
 - robot drive number 66
 - robot library, controlling drive 66
 - servicing requests 237
 - Sony dip switches 253
 - standalone 65
 - standalone volume database host 71
 - TLH information 67
 - TLM information 68
 - type 63
 - types and densities 222
 - virtualization 383
 - volume header device 64
 - drive cleaning
 - for TLH robots 406
 - managing 313
 - manual 313
 - Media and Device Management menu 73, 234
 - operator-initiated 313
 - Drives List, Devices window 26
 - Drives status list
 - Assigned Host field 223
 - Comment field 224
 - Control field 220
 - Device Monitor window 220
 - Drive Index field 222, 224
 - Drive Name field 220
 - External Media ID field 223
 - Media Label field 223
 - Ready field 223
 - Recorded Media ID field 223
 - Request ID field 224
 - Shared field 223
 - Type field 222
 - User field 223
 - Writable field 223
 - drstat command 292
- E**
- eject volume from robot
 - for move volume 135
 - menu command 94
 - methods available 115
 - multiple volumes 94
 - empty media access port prior to update 166
 - ENABLE_ROBOT_AUTH, vm.conf entry 365
 - enhanced authorization



- allowable Media Manager commands 351
- allowing 352
- erasing media 140
- examples
 - SAN components 246
 - SSO components configuration 266
- expired media 110, 112
- External Media ID
 - drive status 223
 - pending requests 225

F

- fibre channel
 - arbitrated loop 246
 - hub 246
 - switch 246
 - switched fabric 246
- find command 20, 93, 214
- firmware levels 248, 260
- first media ID, add volume range 126
- First Mount field 102
- first slot number
 - add volumes 126
 - for move volumes 135
- format description for optical 345
- fragmented backups 345
- frequency-based drive cleaning 73, 234, 252, 264, 312

G

- get_license_key command 253
- global device database host
 - choosing 42
 - conflict 41, 45
 - default 42
- glossary of terms 2
- Glossary. *See* NetBackup Help.

H

- hardware compression 340
- help for the topology pane 32, 227
- host
 - device 8
 - for Device Monitor 231
 - for robotic control 56
 - for standalone drives 71
 - for volume pool 109, 111
 - volume database 9, 50
- Hosts List, Devices window 31

- HyperTerminal 249

I

- IBM Automated Tape Library 399
 - (also see Tape Library Half-inch)
- IBM Automated Tape Library service 402
- IBM device number 27, 67, 292, 406
- images, expiring with bpexpdate 143
- inject volume into robot
 - add volume 129
 - for move volume 135
 - methods available 114
 - multiple volumes 166
 - robot inventory 115
- install and configure ADIC software 413
- inventory and compare robot contents 160
- INVENTORY_FILTER, vm.conf entry 365

K

- key Media Manager terms 1

L

- label
 - media tapes 120
 - new media 139
- launch SANPoint Control 21, 77, 215
- Library Management Unit 379
- library sharing 52, 265, 392
- Library Storage Module 379
- library-based cleaning 264, 312
- license keys 245, 253, 384
- LMU (see Library Management Unit)
- long erase 94, 141
- LSM (see Library Storage Module)

M

- making advanced configuration
 - changes 335
- MAP_ID, vm.conf entry 366
- mapping Backup Exec
 - media types, vm.conf entry 360
 - robots, vm.conf entry 361
- master server 8
- maximum barcode lengths 322
- maximum concurrent drives for backup 255
- maximum mounts
 - add volume 127
 - change volumes 146
- media
 - catalog 275
 - density 226



- formats 344
 - mount and unmount 338
 - recycling 150
 - replacing 149
 - selection algorithm 340, 342
 - servers 8
 - spanning 341, 343
 - media ID
 - generation rules 187, 325
 - prefix for update robot 172
 - style for new volumes 126
 - media ID, add volume 126
 - Media management window
 - displaying 92
 - menus 19, 93
 - status bar 31, 104
 - toolbar 22, 94
 - Media Manager
 - allowable characters 34, 105, 229
 - authentication/authorization
 - security 348
 - best practices 270
 - configuration file 356
 - hosts, overview 7
 - overview 1
 - security 39, 40, 347, 349
 - terminology 1
 - media pool (see volume pool)
 - media server 265
 - media settings tab 154
 - media type
 - 4MM 278
 - 4MM_CLN 278
 - 8MM 278
 - 8MM_CLN 278
 - 8MM2 278
 - 8MM2_CLN 278
 - 8MM3 278
 - 8MM3_CLN 278
 - DLT 278
 - DLT_CLN 279
 - DLT2 278
 - DLT2_CLN 279
 - DLT3 278
 - DLT3_CLN 279
 - DTF 278
 - DTF_CLN 279
 - for new volume 124
 - HC_CLN 278
 - HC2_CLN 278
 - HC3_CLN 278
 - HCART 278
 - HCART2 278
 - HCART3 278
 - QCART 278
 - REWR_OPT 278
 - when not an API robot 173
 - WORM_OPT 278
 - media type mappings (API robots) 189
 - MEDIA_ID_BARCODE_CHARS, vm.conf entry 367
 - MEDIA_ID_PREFIX, vm.conf entry 368
 - Microsoft RSM libraries 391
 - MM_SERVER_NAME, vm.conf entry 370
 - Mode field 226
 - mount media 338
 - mount requests, pending 237
 - move volumes
 - logical move 321
 - methods available 130
 - overview 130, 320
 - physical move 321
 - update volume configuration 131
 - multiplexed backups 346
 - multiplexing (MPX) tape format 346
- N**
- naming conventions 34, 105, 229
 - NDMP configurations 252, 254, 306
 - NDMP hosts 44
 - NetBackup
 - authentication 347
 - authorization 347
 - patches 37
 - pool 97, 101
 - volume pool 113
 - wizards 12
 - NetBackup Access Management 19, 93, 213
 - NetBackup Administration Console 12
 - NetBackup and Media Manager
 - databases 274
 - NetBackup catalogs 275
 - NetBackup Enterprise Server 107, 231, 245
 - NetBackup Server 107, 231
 - no rewind device 64
 - NOT_DATABASE_HOST, vm.conf entry 106, 271, 368
 - number of volumes 125



O

- operating mode of drive, changing 232
- operating system changes 249
- optical disk
 - format 345
 - partner ID 102
 - platter side 102
- optical volumes 133
- overview of
 - barcodes 321
 - drive cleaning 310
 - robots 276
 - shared drives 245
 - volume groups 315
 - volume pools 315

P

- partially-configured devices 45
- pending actions
 - notation 238
 - overview 238
 - resolving 241
- pending requests
 - Barcode field 226
 - Density field 226
 - External Media ID field 225
 - Host Name field 225
 - Mode field 226
 - Recorded Media ID field 225
 - Request ID field 225
 - Time field 226
 - User field 225
 - Volume Group field 226
- physical inventory utility 325
- PREFERRED_GROUP, vm.conf entry 368
- pre-labeling media 338
- PREVENT_MEDIA_REMOVAL, vm.conf entry 369
- preview volume configuration update 166
- print device configuration 78
- processes
 - robotic 292
 - robotic control 292

Q

- quick erase 94, 141

R

- RANDOM_PORTS, vm.conf entry 369
- rdevmi 267

- reactive cleaning 310
- ready status 223
- recommended method of configuring devices 44
- reconfiguring devices in a SSO
 - configuration 335
- Recorded Media ID
 - drive status 223
 - pending requests 225
- recycle media 150
- refresh rate, changing 229
- relabeling media 139
- remote device management 38
- Removable Storage Manager (RSM)
 - adding volumes 394
 - barcode operations 396
 - configuring drives 393
 - media pools 391
 - media requests 392
 - overview 392
 - removing tapes 396
 - robot types 49
- remove a server from a configuration 336
- replace media 149
- replacing a device in a SSO
 - configuration 335
- requests
 - assigning 239
 - denying 243
 - display pending 237
 - example assignment 240
 - identification number
 - drive status 224
 - pending requests 225
 - overview 237
 - resubmitting 242
- REQUIRED_INTERFACE, vm.conf entry 370
- RESERVATION CONFLICT status 303
- reset
 - drive 233
 - mount time 74, 235
- residence, update volume configuration 164
- retention period, expiring backups with
 - bpexdate 143
- RETURN_UNASSIGNED_MEDIA_TO_SCATCH_POOL, vm.conf entry 371
- right-click shortcut menus 14, 32, 104, 227
- robot



- attributes 279
- barcode rules 179
- barcode update 207
- cleaning 264
- control host 56
- destination for move volume 133
- device file 53
- device host 48
- drive number 66
- for new volume 124, 133
- inventory 129, 153
- inventory and compare contents 160
- number 49
- process 292
- sharing 265
- type 48
- update volume configuration 162
- volume database host 50
- robot type
 - ACS 277
 - LMF 277
 - ODL 277
 - RSM 277
 - TL4 277
 - TL8 277
 - TLD 277
 - TLH 277
 - TLM 277
 - TS8 277
 - TS8 277
 - TSD 277
 - TSH 277
- robotic
 - cleaning 310
 - control host 56
 - control process 292
 - device file 53
 - library 66
 - test utilities 292, 388
- robotic inventory
 - advanced options 154
 - filtering 389, 409
- Robots List
 - Devices window 29
 - Media window 99
- robtest 292, 353, 418, 419
- RSM_vm.conf entry 371

S

- SAN media server 8, 265

- SAN Shared Storage Option (see SSO)
- SANPoint Control 21, 77, 215
- scan host 266, 267
- scratch pool
 - adding 110
 - changing to 112
 - overview 318
- SCRATCH_POOL, vm.conf entry 371
- SCSI Long Erase 141
- SCSI Quick Erase 140
- SCSI reserve/release
 - break a reservation 300
 - controlling use of 305
 - crawlreleasebyname option 303
 - error recovery 303
 - in NetBackup 299, 300
 - limitations 304, 306
 - overview 298
 - PEND status 303, 304
 - requirements 306
 - RESERVATION CONFLICT 299, 303
- SCSI-to-fibre
 - bridges 249
 - mapping 248
- SERVER, vm.conf entry 39, 372
- Shared Drive wizard 14
- shared drives (see SSO)
- shared drives, definition 264
- shared media 252
- shared storage option, key 245, 253
- shared_drive_notify script 246
- shortcut menus 14, 32, 104, 227
- show robot contents 157
- slot number
 - add volume 126
 - for move volumes 135
- Sony AIT tape drives 253
- spanning media 341
 - enabling 341, 343
 - tape format 346
- SSO
 - configuration wizards 21, 44, 58, 59, 70, 71, 254
 - configuring shared ACS drives 382
 - configuring shared TLM drives 419
 - configuring TLM robot types 417, 418
 - definition 245
 - device allocation host 251, 265, 268
 - drive cleaning 313



- drive comment 236
- drive operating mode 232, 235, 236
- hardware requirements 245
- license key 384
- RSM robot types 392
- scan host 266, 267
- supported robot types 251
- supported SAN hardware 263
- supported server platforms 251
- terminology 264
- unsupported robot types 251
- vm.conf entries 372, 373
- SSO_DA_REREGISTER_INTERVAL, vm.conf entry 372
- SSO_DA_RETRY_TIMEOUT, vm.conf entry 372
- SSO_HOST_NAME, vm.conf entry 373
- SSO_SCAN_ABILITY, vm.conf entry 221, 373
- standalone drive
 - add drive 65
 - standalone extensions, disabling 343
 - volume database host 71
- status, drive initial configuration 61
- Storage Area Network (SAN) 8, 246, 247, 252, 260, 265
- storage devices, steps for attaching 35
- supported
 - robot types 251
 - SAN hardware 263
 - server platforms 251
- suspend media 339

T

- table-driven robotics 291
- tape
 - 32 bit drivers 35
 - device installer 35
 - installer 35
- tape format
 - fragmented 345
 - multiplexed 346
 - non-QIC 345
 - QIC 345
 - spanned tapes 346
- Tape Library Half-inch (TLH)
 - adding volumes 407
 - cleaning drives 406
 - configuring robotic control 403

- control daemon 402
- drive information 67
- drive mapping 406
- media requests 402
- removing tapes 407
- robot inventory 408
- service 402

Tape Library Multimedia (TLM)

- adding volumes 420
- allocating drives 413
- configuring drives 416
- configuring robotic control 413
- drive information 68
- drive mapping 416
- inventory operations 422
- media requests 413
- overview 411
- removing tapes 421
- service 412
- tape spanning 341, 343
- TapeAlert 5, 65, 252, 264, 310
- tapes and tape files
 - assigning requests 239
 - example of handling a request 240
 - labels 223
 - mode 226
 - time requested 226
- terminating drive assignment 233
- tested SAN components 263
- TLH_ vm.conf entry 374
- TLM_ vm.conf entry 374
- tlmtest 416, 418, 419, 420, 421
- toolbars, viewing and customizing 22, 94
- topology pane help 32, 227
- tpautoconf 335
- tpautoconf command 41, 271
- tpconfig menus 60

U

- unmount media 338
- unsupported
 - characters 167
 - robot types 251, 252
- up drive, standard mode (AVR) 214
- update and rescan barcodes 207
- update barcodes 207
- update robot
 - procedure 165
- update volume configuration



- when not to use 164
- when to use 163
- User field
 - drive status 223
 - pending requests 225
- using Media Manager devices with other applications 270

V

- VAULT_CLEAR_MEDIA_DESC, vm.conf entry 374
- VERBOSE, vm.conf entry 375
- VERITAS Backup Exec 252, 264
- VERITAS Storage Migrator 250, 252, 265
- VERITAS support web site 35, 37
- vm.conf file
 - ACS_ entries 357
 - adding SERVER entries 39
 - ADJ_LSM entries 357
 - API_BARCODE_RULES entries 358
 - AUTHORIZATION_REQUIRED entries 359
 - AUTO_UPDATE_ROBOT entries 359
 - AVRD_PEND_DELAY entries 360
 - AVRD_SCAN_DELAY entries 359
 - CLEAN_REQUEST_TIMEOUT entries 361
 - CLIENT_PORT_WINDOW entries 362
 - CLUSTER_NAME entries 370
 - CONNECT_OPTIONS entries 362
 - DAS_CLIENT entries 363
 - DAYS_TO_KEEP_LOGS entries 363
 - DEVICE_HOST entries 364
 - DISABLE_AUTO_PATH_CORRECTION entries 364
 - DISALLOW_NONNDMP_ON_NDMP_DRIVE entries 364
 - DO_NOT_EJECT_STANDALONE entries 365
 - ENABLE_ROBOT_AUTH entries 365
 - INVENTORY_FILTER entries 365
 - MAP_ID entries 366
 - mapping Backup Exec media type entries 360
 - mapping Backup Exec robot entries 361
 - MEDIA_ID_BARCODE_CHARS entries 367
 - MEDIA_ID_PREFIX entries 368
 - MM_SERVER_NAME entries 370
 - NOT_DATABASE_HOST entries 368
 - overview 356
 - PREFERRED_GROUP entries 368
 - PREVENT_MEDIA_REMOVAL entries 369
 - RANDOM_PORTS entries 369
 - REQUIRED_INTERFACE entries 370
 - RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL entry 371
 - RSM_ entries 371
 - SCRATCH_POOL entries 371
 - SERVER entries 372
 - SSO_DA_REREGISTER_INTERVAL entries 372
 - SSO_DA_RETRY_TIMEOUT entries 372
 - SSO_HOST_NAME entries 373
 - SSO_SCAN_ABILITY entries 373
 - TLH_ entries 374
 - TLM_ entries 374
 - VAULT_CLEAR_MEDIA_DESC entries 374
 - VERBOSE entries 375
- vmd 265
- vmd/DA, definition 265
- vmdb_merge command 9, 106, 271
- Volume Configuration wizard 14, 44, 129
- volume database host
 - for robot 50
 - recommendations 251, 261
 - requirements 251
 - selecting 106
 - with tpconfig 60
- volume group
 - add volume 128
 - changing name 148
 - deleting 137
 - field 226
 - for move volume 134
 - rules for assigning 316
- Volume Groups list, Media window 98
- volume pool
 - add volume 128
 - adding 109
 - changing attributes 111
 - changing for a volume 112
 - configuring a scratch pool 112, 318
 - DataStore pool 97
 - deleting 113
 - for update robot 178



- host name 109, 111
- HSM pool 97
- NetBackup pool 97, 101
- overview 108, 314
- Volume Pools list, Media window 97
- volumes
 - adding (see adding)
 - assigned 142
 - changing (see changing)
 - cleaning count 148
 - deleting (see deleting)
 - description for new volume 126
 - first time mounted 102
 - for move volume 133
 - header device 64
 - maximum mounts allowed 127
 - media ID style 126

- moving 130, 320
- moving, actions menu 131
- platter side 102
- recycling 150
- replacing 149
- without barcodes 6, 91
- Volumes list, Media window 100

W

- wizard
 - device configuration 14, 44, 58, 69, 248, 261, 306
 - shared drive configuration 14, 21, 58, 70, 71, 254
 - volume configuration 14
- Writable field 223

