



# **VERITAS NetBackup™ 6.0 Media Manager**

## **System Administrator's Guide**

**for UNIX and Linux**

N15259B

September 2005

---

## 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 © 1993-2005 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo, and VERITAS NetBackup are trademarks or registered trademarks of VERITAS Software Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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 650-527-2908  
[www.veritas.com](http://www.veritas.com)

## Third-Party Copyrights

For a list of third-party copyrights, see the *NetBackup Release Notes* appendix.



# Contents

---

<b>Preface</b> .....	<b>xxvii</b>
How To Use This Guide .....	xxvii
Getting Help .....	xxviii
Finding NetBackup Documentation .....	xxviii
Accessing the VERITAS Technical Support Web Site .....	xxviii
Contacting VERITAS Licensing .....	xxx
Accessibility Features .....	xxx
Comment on the Documentation .....	xxxi
 <b>Chapter 1. Introduction to Media Manager</b> .....	<b>1</b>
Media Manager Features .....	1
Media Manager Hosts .....	3
Enterprise Media Manager (EMM) Server .....	3
Master Servers .....	4
Media Servers .....	4
SAN Media Servers .....	4
NetBackup and Media Manager Databases .....	5
Enterprise Media Manager (EMM) Database .....	5
NetBackup Catalog .....	6
Media Manager Administrator and User Interfaces .....	7
Java Administrative Interface .....	7
Starting the Java Administration Interface .....	8
Shortcut Menus .....	10
Menu-Based Administrative Interfaces .....	10



---

Command Line Administrative Interfaces (CLI) .....	11
The Device Configuration Wizard .....	11
The Volume Configuration Wizard .....	11
Device and Media Configuration Overview .....	12
Using Media Manager .....	13
Requesting Volumes .....	13
Checking Barcodes .....	14
Volume Pools .....	14
Security Issues .....	15
<b>Chapter 2. Configuring Storage Devices .....</b>	<b>17</b>
Starting Device Management .....	18
Using the Device Management Window .....	18
Menus and Commands .....	19
Toolbars .....	22
Tree Pane .....	22
Managing the Columns of the Display Pane .....	23
Managing Devices on Other Servers .....	23
Drives Pane .....	23
Physical Drives Pane .....	24
Drive Paths Pane .....	27
Robots Pane .....	29
Hosts Pane .....	30
NDMP Hosts Pane .....	31
Topology Pane .....	32
Topology Icons .....	32
Topology Connections .....	33
Selecting Topology Objects .....	33
Messages Pane .....	34
Shortcut Menus and Commands .....	34



---

Customizing the Window .....	35
Viewing and Rearranging Columns .....	35
Changing the View of the Topology Pane .....	35
Performing Initial Device Configuration .....	36
Managing the Device Manager Service (Windows) or the Device Daemon (UNIX) ..	38
The Device Mapping File .....	39
NetBackup Mixed Server Configurations .....	39
Administering Devices on Other Servers .....	41
Remote Administration of Other UNIX Servers .....	42
Administration Example .....	42
Adding SERVER Entries in the NetBackup bp.conf File .....	43
Media Manager Security .....	44
Example SERVER Entries .....	44
The Enterprise Media Manager (EMM) Server .....	45
A Single Host is Required .....	45
How This Host is Determined .....	46
Managing The EMM Server .....	46
Why You Should Use the Media Manager Wizards .....	47
The Device Configuration Wizard .....	48
Operating System Changes .....	48
Possible EMM Server Host Conflict .....	49
Managing Devices that are Partially-Configured .....	49
Learning More About the Device Configuration Wizard .....	49
Starting the Device Configuration Wizard .....	49
Activate/Deactivate Hosts .....	50
Adding NDMP Hosts .....	50
Adding Robots Manually .....	51
Dialog Entries for Adding and Changing Robots .....	52
Device Host .....	53
Robot Type .....	53



---

Robot Number .....	53
Robot Control Section of the Dialog .....	54
Robot is Controlled Locally by this Device Host .....	56
Robot Control is Handled by a Remote Host .....	58
Robot Control is Attached to an NDMP Host .....	59
Adding Shared Drives .....	60
Using the Device Configuration Wizard to Configure Shared Drives .....	60
Using Alternate Interfaces to Configure Shared Drives .....	61
tpconfig menus .....	61
tpconfig Command Line Interface .....	61
Adding Drives .....	61
Dialog Entries for Adding or Changing Drives .....	62
Drive Name Section of the Dialog .....	63
Drive Name .....	63
Drive Name Rule .....	64
Host and Path Information Section of the Dialog .....	66
Host and Path Information .....	66
No Rewind Device .....	66
Drive Information Section of the Dialog .....	67
Drive Type .....	67
Cleaning Frequency .....	67
Drive Status .....	68
Robotic Drive Information Section of the Dialog .....	68
Drive is in a Robotic Library .....	69
Robotic Library .....	69
Robot Drive Number .....	69
Adding Optical Drives .....	71
Dialog Entries for Adding or Changing Optical Drives .....	72
Drive Name Section of the Dialog .....	73
Drive name .....	73



---

Use drive name rule .....	73
Host and Path Information Section of the Dialog .....	73
Host and Path Information .....	73
Data/Device path .....	74
Volume Header Device Path .....	74
Robotic Information Section of the Dialog .....	74
Drive is in a robotic library .....	74
Robotic library .....	75
Robot drive number .....	75
Managing Your Device Configuration .....	76
When to Perform Device Configuration Changes .....	76
Using the Device Configuration Wizard for Configuration Changes .....	77
Changing a Robot Configuration .....	77
Changing the Configuration of a Drive .....	77
Changing a Non-Shared Drive to a Shared Drive .....	78
Deleting Robots .....	78
Deleting Drives .....	79
Performing Device Diagnostics .....	79
Executing Diagnostic Tests for a Drive .....	79
Executing Diagnostic Tests for a Robotic Library .....	81
Exiting a Diagnostic Test When Testing is Complete .....	83
Stopping a Diagnostic Test and Changing the Device to be Tested .....	83
Obtaining Detailed Information For a Particular Test Step .....	83
Managing a Test Step that Requires Operator Intervention .....	83
Printing Your Device Configuration .....	84
Robot and Drive Configuration Examples .....	84
Example 1: Configuring a Robot on a Server .....	85
Example 2: Configuring Standalone Drives on a Server .....	88
Example 3: Configuring a Robot Distributed Among Multiple Servers .....	91
Configuration on the Windows Server eel .....	92



---

Configuration on the Windows Server shark .....	92
Configuration on the UNIX Server whale .....	93
Example 4: Configuring an ACS Robot on a UNIX Server .....	95
Example 5: Configuring a TLH Robot on a UNIX Server .....	98
Example 6: Configuring a TLM Robot on a UNIX Server .....	100
<b>Chapter 3. Managing Media .....</b>	<b>103</b>
Starting Media Management .....	104
Using the Media Management Window .....	105
Menus and Commands .....	105
Toolbars .....	107
Tree Pane .....	108
Volumes Pane .....	109
Volume Pools List .....	109
Volume Groups List .....	111
Robots List .....	112
Volumes List .....	113
Messages Pane .....	120
Shortcut Menus and Commands .....	120
Customizing the Window .....	121
Administering Media on Other Servers .....	122
Managing Media on Other Servers .....	122
Adding New Volumes .....	123
Methods Available for Adding Volumes .....	123
Robotic Volumes (Volumes Located in a Robot) .....	123
Standalone Volumes (Volumes To Be Used in Standalone Drives) .....	124
NetBackup Catalog Backup Volumes .....	124
Notes on Labeling NetBackup Volumes .....	124
Adding Volumes Using a Robot Inventory Update .....	125
Adding Volumes Using the Actions Menu .....	126





---

Dialog Entries for New Volumes .....	128
Media Type .....	128
Volume Is In a Robotic Library .....	128
Select Robot Section of the Dialog .....	129
Device Host .....	129
Robot .....	129
Number of Volumes (or Number of platters) .....	129
Media ID Naming Style .....	130
Media ID or First Media ID .....	130
Partner ID .....	131
Media Description .....	131
First Slot Number .....	131
Maximum Mounts or Maximum Cleanings .....	132
Volume Group .....	132
Volume Pool .....	134
Label Optical Media .....	134
Using the Volume Configuration Wizard .....	134
Learning More About the Volume Configuration Wizard .....	135
Starting the Volume Configuration Wizard .....	135
Configuring Volume Pools .....	135
Adding a New Volume Pool or Scratch Volume Pool .....	136
Adding a Scratch Volume Pool .....	138
Changing the Attributes of a Volume Pool .....	139
Changing a Volume Pool To be a Scratch Volume Pool .....	140
Deleting a Volume Pool .....	141
Using WORM Media .....	141
Supported Drives .....	142
Managing Your WORM Media in Media Manager .....	143
Using WORM Volume Pools to Manage WORM Media .....	143
Using Unique Drive and Media Types to Manage WORM Media .....	145



---

Disabling WORM Tape Support .....	145
WORM Tape Limitations .....	145
Methods Available for Injecting and Ejecting Volumes .....	146
Performing a Volume Configuration Update Using Robot Inventory .....	146
Using the Eject Volumes From Robot Command .....	147
Media Ejection Timeout Periods .....	147
Ejecting Volumes From Robots (Actions Menu Command) .....	148
Rescanning and Updating Barcodes for a Robot .....	149
When to Use Rescan/Update .....	149
When Not to Use Rescan/Update .....	149
Rescanning/Updating Barcodes .....	150
Moving Volumes .....	151
Moving Volumes Using the Robot Inventory Update Option .....	151
Moving Volumes Using the Actions Menu .....	151
Dialog Entries for Move Volumes .....	153
Volumes to Move .....	153
Volume Is In a Robotic Library .....	153
Select Robot Section of the Dialog .....	153
Device Host .....	154
Robot .....	154
Volume Group .....	154
First Slot Number .....	155
When to Delete Volumes .....	155
Deleting Volumes .....	156
Deleting a Volume Group .....	156
Labeling Media .....	157
Erasing Media Functions .....	159
SCSI Quick Erase .....	159
SCSI Long Erase .....	160
Erasing Media .....	160



---

Deassigning Volumes .....	161
Determining Which Application is Using a Volume .....	161
Deassigning NetBackup Volumes .....	161
Deassigning NetBackup Regular Backup Volumes .....	162
Deassigning NetBackup Catalog Backup Volumes .....	162
Deassigning Storage Migrator Volumes .....	163
Changing the Attributes for a Volume .....	163
Dialog Entries for Change Volumes .....	164
Maximum Mounts .....	165
Expiration Date .....	165
Description .....	166
Volume Pool .....	166
Number of Cleanings Remaining .....	167
Changing the Volume Pool Assignment for a Volume .....	167
Changing the Volume Group of a Volume .....	168
Moving A Volume Group .....	169
Exchanging Volumes .....	170
Exchanging a Volume and Using a New Media ID .....	171
Exchanging a Volume and Using the Old Media ID .....	171
Recycling Volumes .....	172
Recycling Volumes Using the Existing Media ID .....	172
Recycling Volumes Using a New Media ID .....	172
<b>Chapter 4. Managing Media in Robots (Robot Inventory) .....</b>	<b>175</b>
Overview of Robot Inventory Operations .....	175
Accessing the Robot Inventory Dialog .....	177
Showing the Contents of a Robot .....	179
How Contents Reports for API Robots are Generated .....	180
ACS Robots .....	181
TLH Robots .....	181



---

TLM Robots .....	181
Comparing Robot Contents with the Volume Configuration .....	182
Compare Volume Configuration Reports .....	182
Updating the Volume Configuration for a Robot .....	184
When to Use Update Volume Configuration .....	185
When Not to Use Update Volume Configuration .....	186
Updating the Volume Configuration for Non-Barcoded Media .....	187
Procedure To Update the Volume Configuration .....	187
Example Update Volume Configuration Reports .....	189
Media Settings Tab (Advanced Options) .....	190
Setting Media Options .....	191
Properties for the Media Settings Tab .....	191
Media Which Have Been Removed From the Robot .....	192
Media Which Have Been Moved Into or Within the Robot .....	193
Use the Following Media ID Prefix .....	194
Label Optical Media (Local Host Only) .....	195
Use Barcode Rules .....	196
Media Type .....	197
Volume Pool .....	201
Barcode Rules Tab (Advanced Options) .....	202
Adding a New Barcode Rule .....	202
Changing a Barcode Rule .....	203
Deleting a Barcode Rule .....	204
Dialog Properties for Adding or Changing Barcode Rules .....	204
Media ID Generation Tab (Advanced Options) .....	207
Adding a New Media ID Generation Rule .....	208
Changing a Media ID Generation Rule .....	209
Deleting a Media ID Generation Rule .....	210
Dialog Properties for Adding or Changing Media ID Generation Rules ....	210
Media Type Mappings Tab (Advanced Options) .....	211



---

How the Mapping Defaults Shown on the Tab are Determined .....	211
Using the Tab to Change Media Type Mappings .....	212
Adding Mapping Entries to vm.conf .....	213
Default and Allowable Media Types for API Robots .....	214
Examples of Updating a Volume Configuration .....	218
Example 1: Removing a Volume from a Robot .....	218
Example 2: Adding Existing Standalone Volumes to a Robot .....	219
Example 3: Moving Existing Volumes Within a Robot .....	222
Example 4: Adding New Volumes to a Robot .....	223
Example 5: Adding Cleaning Tapes to a Robot .....	225
Example 6: Moving Existing Volumes Between Robots .....	226
Example 7: Adding Existing Volumes when Barcodes are Not Used .....	227

<b>Chapter 5. Monitoring Storage Devices .....</b>	<b>231</b>
Starting the Device Monitor .....	232
Using the Device Monitor Window .....	232
Menus and Commands .....	233
Toolbars .....	236
Drive Status Pane .....	236
Drive Paths Pane .....	240
Pending Requests Pane .....	243
Messages Pane .....	246
Shortcut Menus and Commands .....	246
Customizing the Window .....	246
Controlling the Media Manager Device Daemon .....	247
Monitoring Devices on Other Servers .....	248
Changing the Operating Mode of a Drive .....	249
Changing Mode Example .....	250
Resetting a Drive .....	250
Drive Cleaning Functions .....	251



---

Adding or Changing a Drive Comment .....	253
Obtaining Information About a Drive .....	253
Managing Drive Paths .....	254
Handling Pending Requests and Pending Actions .....	254
Pending Requests .....	254
Pending Requests (Storage Unit Specific) .....	255
Pending Actions .....	255
Resolving Pending Requests .....	256
Resolving a Pending Request Example (Drive in AVR mode) .....	257
Resolving Pending Actions .....	259
Resubmitting Requests .....	259
Denying Requests .....	260
Shared Storage Option Summary Reports .....	261
<b>Chapter 6. Managing the Media Manager Daemons .....</b>	<b>263</b>
Overview of Media Manager Daemons .....	263
Robotic Daemons and Robotic Control Daemons .....	264
Library Sharing (or Robot Sharing) .....	264
Media Manager Device Daemon (ltid) .....	265
Starting the Device Daemon .....	265
Stopping the Device Daemon .....	266
Automatic Volume Recognition Daemon (avrd) .....	266
Enterprise Media Manager (nbemm) .....	267
Media Manager Volume Daemon (vmd) .....	267
Media Manager Status Collection Daemon (vmscd) .....	267
Robotic Daemons .....	268
Starting and Stopping Robotic Daemons .....	270
Displaying Process Status using the vmpps Script .....	271
Logging of Errors .....	272
<b>Chapter 7. Tape I/O Commands .....</b>	<b>273</b>



---

Requesting Tapes .....	273
drive_mount_notify Script .....	274
tpreq Example .....	274
Reading and Writing Tape Files .....	274
Positioning Tape Files .....	275
Rewinding Tape Files .....	275
Removing Tape Files .....	275
drive_unmount_notify Script .....	276
Using an Optical Disk .....	276
External Access to Media Manager Controlled Devices .....	277
User Error Messages .....	278
<b>Chapter 8. Shared Storage Option (SSO) Topics .....</b>	<b>279</b>
What is SSO? .....	279
An Extension of Media Manager .....	280
A SAN is not Required for SSO .....	280
Sample SSO Configuration with SAN Components .....	280
Configuring and Verifying Your SSO Hardware .....	281
Using the Media Manager Device Configuration Guide .....	282
Configuration Tasks .....	282
Verifying Your Hardware is Connected and Working .....	283
Installing the Shared Storage Option .....	284
System Requirements for SSO .....	284
Enterprise Media Manager (EMM) Device Allocator Requirements .....	285
Supported Robot Types for SSO .....	285
Supported Media Servers for SSO .....	285
SSO Restrictions and Limitations .....	286
SSO Installation .....	287
Configuring SSO in NetBackup .....	287
Configuring SSO Devices in Media Manager .....	287



---

Configuring NetBackup Storage Units and Backup Policies .....	288
Configuring Storage Units for Each Media Server .....	288
Configuring a Backup Policy for Each Media Server .....	288
Verifying Your SSO Configuration .....	289
Using Media Manager with SSO .....	292
Using the Device Monitor with SSO .....	293
The Drive Status Pane .....	293
Changing the Operating Mode for a Shared Drive .....	293
Adding or Changing a Comment for a Shared Drive .....	293
Performing Drive Cleaning Functions for a Shared Drive .....	293
Shared Storage Option Summary Reports .....	294
Adding SSO Configuration Options .....	294
Troubleshooting SSO Issues .....	294
Hardware Configuration Guidelines .....	294
Media Manager Configuration Guidelines .....	295
Operating System Help .....	296
Common Configuration Issues with SSO .....	296
Frequently Asked Questions About SSO .....	297
SSO Reference Topics .....	298
SSO-Related Terms and Concepts .....	298
Shared Drive .....	298
Backup Exec Shared Storage Option .....	298
Sharing Robotic Libraries Without Using SSO .....	299
Media Servers and NetBackup SAN Media Servers .....	299
SSO Components in Media Manager .....	299
nbemm/DA .....	299
Example SSO Configuration Showing Media Manager Components .....	300
Scan Host .....	301
Device Allocation Host .....	302





---

<b>Appendix A. Media Manager Reference Topics .....</b>	<b>303</b>
NetBackup Media Manager Best Practices .....	304
General Practices .....	304
Enterprise Media Manager Domain Management .....	305
Media Management .....	305
Device Management .....	306
Performance and Troubleshooting .....	307
Other Best Practices .....	307
Allowable Media Manager Characters .....	308
Robot Overview .....	308
Media Manager Robot Types .....	309
Media Manager Media Types .....	310
Alternate Media Types .....	311
Robot Attributes .....	311
ACS Robots .....	312
ODL Robots .....	313
TL4 Robots .....	314
TL8 Robots .....	315
TLD Robots .....	316
TLH Robots .....	317
TLM Robots .....	318
TSH Robots .....	319
Table-Driven Robotics .....	320
Robotic Test Utilities .....	320
Frequently Asked Questions About Device Discovery .....	321
How NetBackup Uses SCSI Reserve/Release .....	324
Background Topics .....	324
NetBackup Releases Prior to NetBackup 4.5 .....	324
NetBackup 4.5 and Later Releases .....	325
SCSI Reserve/Release Commands .....	325



---

How NetBackup Uses SCSI Reserve/Release Commands .....	326
Issuing the Reserve .....	326
Checking for Data Loss .....	326
Checking for Tape/Driver Configuration Errors .....	327
Issuing the Release .....	328
SCSI Reserve/Release Logging and Conflict Notification .....	329
Issuing Reset Commands to Break a Reservation .....	330
Controlling SCSI Reserve/Release .....	331
SCSI Reserve/Release Requirements and Limitations .....	331
Using TapeAlert .....	332
Requirements for Using TapeAlert with Media Manager .....	332
TapeAlert Log Codes .....	333
Correlating Device Files to Physical Drives When Adding Drives .....	336
On Windows Hosts .....	336
On UNIX Hosts .....	338
Drive Cleaning .....	339
Available Types of Cleaning .....	340
Reactive Cleaning (TapeAlert) .....	340
TapeAlert and Media Manager .....	341
TapeAlert and Frequency-Based Cleaning .....	341
Library-Based Cleaning .....	341
Frequency-Based Cleaning .....	341
Frequency-Based Cleaning Limitations .....	342
Managing Frequency-Based Cleaning .....	342
Operator-Initiated Cleaning .....	343
Using a Cleaning Tape .....	343
Volume Pools and Volume Groups .....	344
Volume Pools .....	344
Volume Groups .....	344
Rules for Assigning Volume Groups .....	345



---

Volume Pool and Volume Group Example .....	345
Scratch Volume Pools .....	347
Scratch Pool Example .....	347
Scratch Pool Usage .....	348
Moving Volumes .....	349
Move Operations .....	349
Physical and Logical Moves .....	349
Barcodes .....	350
Barcode Advantages .....	350
Barcode Best Practices .....	351
Barcode Rules .....	352
Media Manager Actions for Barcodes .....	352
Example Barcode Rules .....	353
Media ID Generation Rules .....	354
Using the Physical Inventory Utility for Non-Barcoded Media .....	354
Why Use vmphyinv? .....	355
Features of vmphyinv .....	355
Requirements and Restrictions for vmphyinv .....	356
When to Use vmphyinv .....	356
How vmphyinv Performs a Physical Inventory .....	357
Obtaining a List of Drives Used to Mount the Media .....	357
Obtaining a List of Media to be Mounted .....	357
Mounting Media and Reading the Tape Header .....	359
Updating the EMM Database .....	360
Making Changes to Your Hardware Configuration .....	363
Replacing Devices .....	363
Decommissioning a Media Server .....	365
Moving the EMM Server .....	367
Labeling Media .....	369
Pre-labeling of Media .....	369



---

Mounting and Unmounting of Media .....	370
Suspending Media Or Downing Devices .....	370
How Media Manager Selects a Drive for a Robotic Mount Request .....	370
How NetBackup Selects Media in Robots .....	371
Spanning Media .....	372
How NetBackup Selects Media in Standalone Drives .....	373
Media Selection Using Standalone Drive Extensions .....	373
Disabling Standalone Drive Extensions .....	374
Spanning Media .....	374
Keeping Standalone Drives in the Ready State .....	375
Media Formats .....	375
Standard Tape Format .....	376
QIC/WORM Tape Format .....	376
Optical Media Format .....	376
Fragmented Backups .....	377
Multiplexing Format .....	377
Spanning Tapes .....	377
Media Manager Security .....	378
NetBackup Authentication/Authorization .....	378
Media Manager Authentication/Authorization .....	379
No vm.conf Entry Present .....	379
vm.conf Entry is Present .....	380
Media Manager Security (Using SERVER Configuration Entries) .....	381
Possible NetBackup and Media Manager Conflicts .....	381
Media Manager Enhanced Authorization .....	381
Supported Commands and Daemons .....	382
Allowing Enhanced Authorization .....	382
Enabling Robot Authorization .....	383
Administrators Quick Reference .....	383
Media Manager Commands .....	383



---

Media Manager Log Files .....	386
The Media Manager Configuration File (vm.conf) .....	387
ACS Media Mapping .....	389
ACSSSEL Listening Socket .....	389
ACSSSI CSI Host Port .....	389
ACSSSI Host Name .....	390
ACSSSI Inet Port .....	390
ACSSSI Listening Socket .....	391
ACSSSI RPC Communication Method .....	392
Adjacent LSM Specification for ACS Robots .....	392
API Robot Barcode Rule Enable .....	393
Authorization Required .....	394
Automatically Empty Robot MAP .....	394
AVRD Pending Status Delay .....	394
AVRD Scan Delay .....	395
Cleaning Drives Timeout .....	395
Client Port Range .....	396
Connect to Firewall Options .....	396
DAS Client Name .....	397
Days To Keep Debug Logs .....	397
Automatic Path Remapping .....	398
Enable Robot Authorization .....	398
Inventory Robot Filter .....	398
Media Access Port Default for ACS Robots .....	399
Media Access Port Timeout Control .....	400
Media ID Generation .....	400
Media ID Prefix .....	401
Preferred Group .....	401
Prevent Media Removal (for TL8 Robots) .....	402
Random Port Numbers .....	402



---

Cluster Name, Media Manager Name, Required Network Interface .....	403
Server Entry .....	403
SSO DA Re-register Interval .....	404
SSO DA Retry Time .....	404
SSO Host Name .....	405
TLH Media Mapping .....	405
TLM Media Mapping .....	405
Verbose Message Logging .....	405
Example vm.conf File .....	406

## **Appendix B. Using tpconfig ..... 407**

Robot Number .....	407
Robotic Control Path .....	407
Host Name .....	408
No Rewind On Close Device Name .....	408
Character Device Name .....	408
Volume Header Device Name .....	409
Drive Status .....	409
Starting the tpconfig Utility .....	409
Adding Robots .....	410
Adding Drives .....	412
Updating Robot and Drive Configurations .....	413
Updating Robot Configurations .....	413
Updating Drive Configurations .....	414
Deleting Drives and Robots .....	414
Deleting Drives .....	414
Deleting Robots .....	415
Configuring Drive Paths .....	416
Configuring NDMP Host Credentials .....	417
Displaying and Printing Your Device Configuration .....	418



---

<b>Appendix C. Using the Media Management Utility (vmadm) .....</b>	<b>419</b>
Starting vmadm .....	419
Starting and Stopping vmd .....	419
The vmadm Main Menu .....	420
Configuring Volume Pools .....	421
Adding Volumes for Standalone Drives .....	424
Adding a Single Standalone Volume .....	424
Adding a Range of Standalone Volumes .....	428
Adding Volumes to a Robot .....	431
Auto-Populating a Robot .....	431
Using Auto-Populate .....	432
Adding a Single Volume to a Robot (Without Auto-Populate) .....	433
Adding a Range of Volumes to a Robot (Without Auto-Populate) .....	435
Displaying the Volume Configuration .....	439
Moving Volumes .....	442
Moving Volumes (With Inventory and Update) .....	442
Moving a Single Volume (Without Inventory and Update) .....	443
Moving Multiple Volumes .....	445
Moving a Volume Group .....	448
Deleting a Single Volume .....	449
Deleting Multiple Volumes .....	450
Deleting a Volume Group .....	451
Changing a Volume's Description .....	451
Changing a Volume's Volume Pool .....	452
Changing the Expiration Date for Volumes .....	453
Changing the Volume Group for Volumes .....	454
Change Vault Name for Volumes .....	455
Change Date Volumes are Sent to Vault .....	456
Change Date Volumes Return from Vault .....	456
Change Vault Slot for Volumes .....	457



---

Change Vault Session ID for Volumes .....	458
Setting the Maximum Mounts for Volumes .....	458
Changing the Cleanings Allowed for a Cleaning Tape .....	459
Updating Barcodes for Selected Volumes in a Robot .....	460
Inventory and Report Robot Volume Configuration .....	461
Inventory and Compare Robot Volume Configuration .....	463
Inventory and Update Robot Volume Configuration .....	465
To Inventory and Update Robot Volume Configuration .....	465
Changing Update Options .....	469
Configuring Barcode Rules .....	477
Barcode Rule Sorting .....	478
Barcode Rule Examples .....	478
Barcode Rule Menu .....	479
Adding a Barcode Rule .....	479
Changing a Barcode Rule .....	481
Deleting a Barcode Rule .....	481
Listing Barcode Rules .....	482
Formatting Optical Disks .....	482
<b>Appendix D. STK Automated Cartridge System (ACS) .....</b>	<b>483</b>
Sample ACS Configuration .....	484
Media Requests .....	485
Configuring ACS Drives .....	486
Configuring Shared ACS Drives .....	488
Using the STK SN6000 .....	489
Should SN6000 Drives Be Configured as Shared Drives? .....	490
Hosts Connected To a Single Port .....	490
Hosts Connected To Different Ports .....	490
Adding Volumes .....	491
Removing Volumes .....	491





---

Removing Volumes Using the STK Utility .....	492
Removing Volumes Using Media Manager .....	492
Robot Inventory Operations .....	492
Advanced ACS Robot Topics .....	494
ACS Daemon (acsd) .....	494
ACS Storage Server Interface (acsssi) .....	495
Using the ACS_SSI_SOCKET Environment Variable .....	495
Starting acsssi Manually .....	496
Optional Environment Variables .....	496
ACS SSI Event Logger (acsssel) .....	497
Using acsssel with a Different Socket Name .....	497
ACS Robotic Test Utility (acstest) .....	499
Making ACS Robotic Configuration Changes .....	499
Multiple ACS Robots with One ACS Library Software Host .....	500
Multiple ACS Robots and ACS Library Software Hosts .....	500
Robotic Inventory Filtering .....	501
Inventory Filtering Example .....	502
ASCLS Firewall Configuration .....	502
<b>Appendix E. IBM Automated Tape Library (ATL) .....</b>	<b>505</b>
Sample TLH Configurations .....	505
Media Requests for a TLH Robot .....	508
Configuring Robotic Control .....	509
Robotic Control on an AIX System .....	509
Determine the Path to the LMCP Device File .....	509
Verify Library Communications .....	510
Configure the Robotic Device File .....	510
Robotic Control on a Non-AIX System .....	511
Determine the Library Name .....	511
Verify Library Communications .....	512



---

Configure the Robotic Device File .....	513
Configuring Drives for TLH Robots .....	513
Cleaning Drives .....	515
Adding Volumes .....	515
Removing Volumes .....	515
Robot Inventory Operations .....	516
Robotic Inventory Filtering .....	518

## **Appendix F. ADIC Distributed AML Server/Scalar Distributed Library Controller 519**

Sample TLM Configuration .....	519
Media Requests Involving a TLM Robot .....	521
Configuring TLM Robotic Control .....	521
Configuring TLM Drives on a DAS/SDLC Server .....	521
Installing ADIC Software for the Client Component .....	522
Configuring the DAS/SDLC Client Name .....	522
Allocating TLM Drives on a DAS Server .....	523
Configuring TLM Drives on a SDLC Server .....	523
Configuring TLM Drives in Media Manager .....	524
To add drives manually .....	524
Configuring Shared TLM Drives .....	525
Configuring the ADIC DAS Server .....	525
Configuring the ADIC SDLC Server .....	526
Using the Device Configuration Wizard in Media Manager .....	527
Providing Common Access to Volumes .....	528
Adding Volumes .....	528
Removing Volumes .....	529
Robot Inventory Operations .....	530

## **Index ..... 533**



## Preface

---

This guide describes using the NetBackup Administration Console (Java administrative interface) to manage Media Manager software and its components on a UNIX server.

See “Introduction to Media Manager” on page 1 for a description of the other Media Manager administrative interfaces that are available. See the NetBackup release notes for information about the supported UNIX server platforms for NetBackup.

Media Manager is the component of VERITAS NetBackup™ and VERITAS Storage Migrator™ 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 UNIX systems in general.

## 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.
- ◆ The term Storage Migrator refers to VERITAS Storage Migrator.
- ◆ Portions of this guide apply only to specific robot types (for example, API, 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 probably will want to read every chapter.

An operator should read the chapter “Monitoring Storage Devices” on page 231. A tape user, who has no responsibility for administration, may have an interest in reading the chapter “Tape I/O Commands” on page 273, which describes the user command interface.



## Getting Help

You can find answers to questions and get help from the NetBackup documentation and from the VERITAS technical support web site.

### Finding NetBackup Documentation

A list of the entire NetBackup documentation set appears as an appendix in the *NetBackup Release Notes*. All NetBackup documents are included in PDF format on the NetBackup Documentation CD.

For definitions of NetBackup terms, consult the online glossary.

#### ▼ 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.

### Accessing the VERITAS Technical Support Web Site

The address for the VERITAS Technical Support Web site is <http://support.veritas.com>.

The VERITAS Support Web site lets you do any of the following:

- ◆ 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



From <http://support.veritas.com>, you can complete various tasks to obtain specific types of support for NetBackup:

1. Subscribe to the VERITAS Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.
  - a. From the main <http://support.veritas.com> page, select a product family and a product.
  - b. Under Support Resources, click **Email Notifications**.

Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.
2. Locate the telephone support directory at <http://support.veritas.com> by clicking the **Phone Support** icon. A page appears that contains VERITAS support numbers from around the world.

---

**Note** 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.

---

3. Contact technical support using e-mail.
  - a. From the main <http://support.veritas.com> page, click the **E-mail Support** icon.

A wizard guides you to do the following:

    - ◆ Select a language of your preference
    - ◆ Select a product and a platform
    - ◆ Provide additional contact and product information, and your message
    - ◆ Associate your message with an existing technical support case
  - b. After providing the required information, click **Send Message**.



## Contacting VERITAS Licensing

For license information, you can contact us as follows:

- ◆ Call 1-800-634-4747 and select option 3
- ◆ Fax questions to 1-650-527-0952
- ◆ In the Americas, send e-mail to [amercustomercore@veritas.com](mailto:amercustomercore@veritas.com).  
In the Asia and Pacific areas, send email to [apaccustomercore@veritas.com](mailto:apaccustomercore@veritas.com).  
In all other areas, send email to [internationallicense@veritas.com](mailto:internationallicense@veritas.com).

## 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 Installation Guide*.



## Comment on the Documentation

Let us know what you like and dislike about the documentation. Were you able to find the information you needed quickly? Was the information clearly presented? You can report errors and omissions or tell us what you would find useful in future versions of our manuals and online help.

Please include the following information with your comment:

- ◆ The title and product version of the manual on which you are commenting
- ◆ The topic (if relevant) on which you are commenting
- ◆ Your comment
- ◆ Your name

Email your comment to [NBDocs@veritas.com](mailto:NBDocs@veritas.com).

Please only use this address to comment on product documentation. See “Getting Help” in this preface for information on how to contact Technical Support about our software.

We appreciate your feedback.







# Introduction to Media Manager

---

1

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

- ◆ Media Manager Features
- ◆ Media Manager Hosts
- ◆ NetBackup and Media Manager Databases
- ◆ Media Manager Administrator and User Interfaces
- ◆ Device and Media Configuration Overview
- ◆ Using Media Manager
- ◆ 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 304.

## Media Manager Features

Media Manager is used by NetBackup and Storage Migrator to provide media and device management capabilities for tape and optical disk drives. These capabilities include the following:

- ◆ Media and device management interfaces that allow configuration of storage devices.
- ◆ Device monitor interfaces that display the current status of all defined tape devices and pending requests for volumes, allowing the operator to assign tapes or optical disks to the appropriate drives and respond to problems.
- ◆ Automatic scanning of devices for loaded media with automatic volume recognition of recorded volume labels.



**Note** Automatic volume recognition is the only aspect of ANSI labeled tapes that Media Manager supports. Once a tape is assigned to a request, all volumes are treated as unlabeled, and the user or application is responsible for reading or writing labels if applicable.

---

- ◆ Support of numerous robotic tape library and optical disk library devices that can automatically retrieve, mount, assign, unmount, and store removable volumes.
- ◆ An Enterprise Media Manager (EMM) database containing location and other information about volumes that can be used to identify and retrieve volumes in the robotic devices.
- ◆ Allow any user to request and unmount a specific volume.
- ◆ Ability to inventory a robot, provide reports, and update the EMM database to match the results of the inventory. This simplifies administration, by permitting you to quickly determine the contents of a robot and provides efficient media tracking.

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 can use the physical inventory utility (`vmphysinv`).

- ◆ The capacity to record media statistics. For example, the first and last time the volume was mounted, the date it was created, an expiration date, and the number of times the volume was mounted.
- ◆ Grouping volumes into volume pools for convenience and protection.
- ◆ Capability to perform automated drive cleaning, based on the TapeAlert feature or a frequency-based cleaning schedule. Cleaning tapes that are not configured correctly are also recognized.
- ◆ *The following capability applies only to NetBackup Enterprise Server.*

Capability to automatically share tape drives across multiple hosts that have physical access to shared drives through appropriate hardware. This capability requires the installation of the Shared Storage Option (SSO). See “Shared Storage Option (SSO) Topics” on page 279 for more information.

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



## 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 server software.

Key Media Manager hosts are described in the following topics.

### Enterprise Media Manager (EMM) Server

The host where the Enterprise Media Manager (EMM) database is located is called the EMM Server. The EMM Server provides a centralized repository for managing a subset of NetBackup catalog data. Potentially shared by multiple master/media server environments, EMM catalog data includes:

- ◆ device attributes
- ◆ robotic library/standalone drive residence attributes
- ◆ NDMP attributes
- ◆ barcode rule attributes
- ◆ volume pool attributes
- ◆ tape and optical disk volume attributes
- ◆ media attributes
- ◆ storage unit attributes
- ◆ storage unit group attributes
- ◆ hosts, including Shared Storage Option (SSO) hosts, having assigned tape drives
- ◆ media and device errors



## Master Servers

NetBackup and Media Manager support both master server and media servers. A master server manages the NetBackup backups, archives, and restores. The Enterprise Media Manager (EMM) database is typically located on this host. The Master server, and the EMM Server specifically, is responsible for media and device selection for NetBackup. Media servers 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.

*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 the next section “SAN Media Servers” on page 4.

*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. SAN media servers cannot back up data residing on other clients.

## NetBackup and Media Manager Databases

NetBackup and Media Manager use internal databases to keep information about the media and device configuration. Database names and locations have changed in NetBackup Release 6.0. The restructuring allows for improved performance, scalability and manageability of NetBackup media and devices.

---

**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.

---

### Enterprise Media Manager (EMM) Database

The EMM database contains a subset of NetBackup catalog data, including information about volumes that have been configured for use by Media Manager. In addition to media data, the EMM database also stores information about the robots and drives that are in NetBackup storage units. When you configure devices, Media Manager stores this information in the EMM database. The NetBackup Resource Broker can then query the EMM database in order to allocate storage units, drives (including drive paths), and media.

Data that has been consolidated in the EMM database includes the following:

- ◆ `volmgr/database/globDB`
- ◆ `volmgr/database/ltidevs`
- ◆ `volmgr/database/robotic_def`
- ◆ `volmgr/database/.namespace.chksum` (NDMP)
- ◆ `volmgr/database/ruleDB`
- ◆ `volmgr/database/poolDB`
- ◆ `volmgr/database/volDB`
- ◆ `netbackup/db/media/mediaDB`
- ◆ `netbackup/db/config/storage_units`
- ◆ `netbackup/db/config/stunit_groups`
- ◆ `volmgr/vm.conf` (Some entries)
- ◆ `netbackup/bp.conf` or the Windows registry (Some entries)
- ◆ Some touch files



## NetBackup Catalog

NetBackup keeps a catalog with information that correlates backups to the volume where they are stored. NetBackup refers to the catalog when it needs a volume for a backup or restore. If the catalog does not contain suitable volume for a backup job, NetBackup has Media Manager assign one. In this manner, the catalog is populated as NetBackup uses new media for backups.

When the retention period has ended for all backups on a volume, NetBackup deletes the volume from the catalog. NetBackup then sends a request to Media Manager to unassign the volume so it is available for later reassignment.

Volumes for online, hot backups use media from the CatalogBackup volume pool only, so you can find them in case the NetBackup catalog is damaged (they are unassigned only if you delete them from your catalog backup settings).

Volumes for offline, cold backups use media from the NetBackup volume pool only. Volumes for offline, cold backups of the NetBackup catalogs are a special case and do not appear in the NetBackup catalog. For more information about catalogs and catalog backups, see the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I*.

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 354.

## Media Manager Administrator and User Interfaces

The following table shows the Media Manager administrative interface choices that are available. The terminology, general Media Manager concepts, and results are the same, regardless of which interface you use.

Media Manager Administrative Interfaces

	Java Interface	Menus		CLI	Wizards
Task	jnbSA	tpconfig	vmadm		
Configure Devices	X	X		X	X
Configure Media	X		X	X	X
Manage Devices	X			X	
Manage Hosts				X	
Manage NDMP Credentials	X	X		X	X

See the following sections for more information:

- ◆ “Java Administrative Interface” on page 7.
- ◆ “Menu-Based Administrative Interfaces” on page 10.
- ◆ “Command Line Administrative Interfaces (CLI)” on page 11.
- ◆ “The Device Configuration Wizard” on page 11.
- ◆ “The Volume Configuration Wizard” on page 11.

**Note** For ease of use, the wizards are recommended for device and media configuration.

### Java Administrative Interface

The NetBackup Administration Console allows you to configure and manage media and devices from one main interface. This interface is supported only on certain UNIX platforms.

See the NetBackup release notes for information on platform support and on configuring and using the NetBackup Administration Console on UNIX.



## Starting the Java Administration Interface

1. To start the NetBackup Administration Console (the Java administrative interface) enter the following command:

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

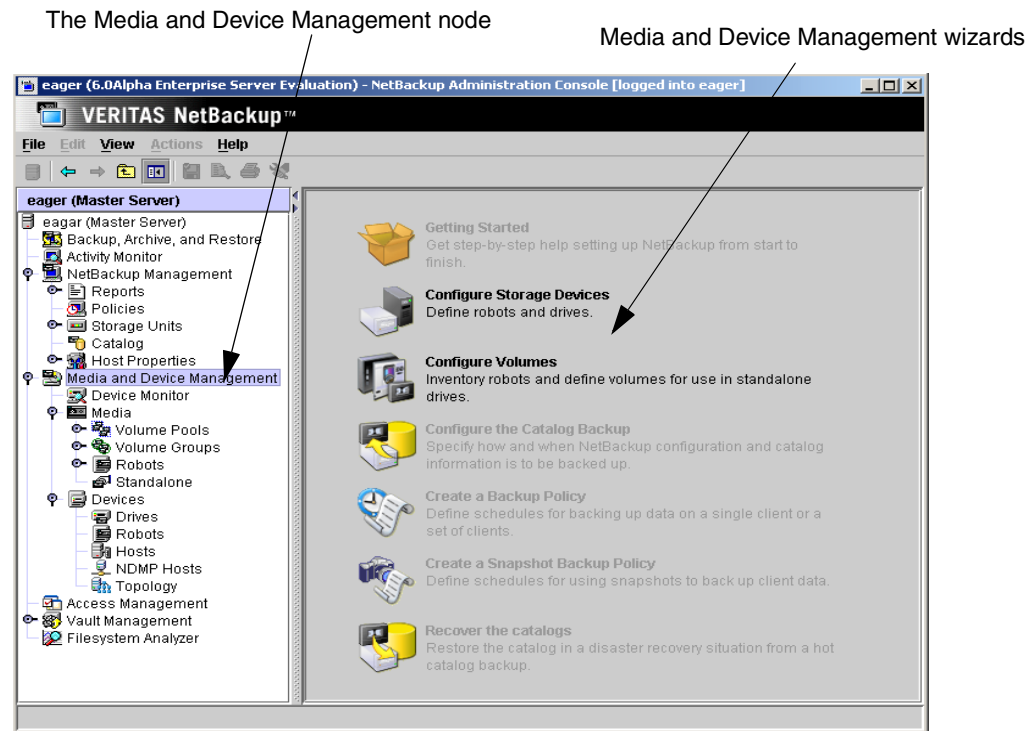
The NetBackup Administration Console is the starting point for administering NetBackup. The left pane of the console window has a node for each major area of NetBackup administration (including nodes for optional VERITAS software products).

2. Select **Media and Device Management**. **Media and Device Management** contains the Media Manager utilities.

The right pane initially contains the key NetBackup wizards that apply to **Media and Device Management**. The following figure shows these Media Manager wizards. These wizards have the following links:

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





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

**Note** See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I*, for details on the other portions of NetBackup Administration Console, other NetBackup administration utilities, and menu commands available.

- ◆ Select **Device Monitor**. The device monitor has commands for monitoring the operation of storage devices.  
"Monitoring Storage Devices" on page 231 explains how to use the Device Monitor.
- ◆ Select **Media**. **Media** has commands for managing media.  
"Managing Media" on page 103 and "Managing Media in Robots (Robot Inventory)" on page 175 explain how to manage your media.



- ◆ Select **Devices**. **Devices** 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

Right-clicking while the mouse pointer is over areas of the NetBackup Administration Console will display a shortcut menu. Different menus appear depending on where your pointer is positioned.

## Menu-Based Administrative Interfaces

The following Media Manager utilities are available from a menu-based interface and can be used by terminals that do not support Java capabilities:

Utility	Description
tpconfig	Used for device configuration. See “Using tpconfig” on page 407 for more information.
vmadm	Used for media configuration. See “Using the Media Management Utility (vmadm)” on page 419 for more information.



## Command Line Administrative Interfaces (CLI)

Many Media Manager administrative commands are available from the command line and can be used by terminals that do not support Java capabilities. For information about other available Media Manager commands (for example, `tpclean`, `vmadd`, and `vmupdate`), see the *VERITAS NetBackup Commands for UNIX and Linux*.

The commands shown in the following table are for users and administrators that are not using NetBackup or Storage Migrator. For more information about these commands see “Tape I/O Commands” on page 273 and *VERITAS NetBackup Commands for UNIX and Linux*.

Command	Description
<code>tpreq</code>	Used to request and mount volumes.
<code>tpunmount</code>	Used to unmount volumes.

## The Device Configuration Wizard

You can use the Device Configuration wizard to configure robots, non-shared drives, and shared drives.

This wizard is available from the right pane of the NetBackup Administration Console (select **Configure Storage Devices**).

## The Volume Configuration Wizard

You can use the Volume Configuration wizard to configure media (volumes). This wizard configures volumes for all supported standalone drives and robotic libraries.

This wizard is available from the right pane of the NetBackup Administration Console (select **Configure Volumes**).



## Device and Media Configuration Overview

The following items summarize the steps for configuring storage devices and media. After configuring your devices, complete your NetBackup policy and storage unit configuration as explained in the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I*.

### ▼ To configure devices and media

1. Physically attach the storage devices to the Media Manager server and perform any configuration steps specified by the device or operating system vendor. Also, see the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

2. Create the system device files for the drives and robotic control.

This is usually done during installation. Device files are created automatically on some UNIX servers. Explicit configuration of device files is required on some UNIX servers to make full use of NetBackup features. See the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for more information.

3. Use the Device Configuration wizard to configure robots, drives, and shared drives. For more information, see “The Device Configuration Wizard” on page 48.

For more information on configuring shared drives, see “Adding Shared Drives” on page 60 and “Shared Storage Option (SSO) Topics” on page 279.

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

4. Use the Volume Configuration wizard to define the media that you will be using in your 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 of the robot occurs and the EMM database is updated to reflect the contents of the robotic library.

To manually configure volumes for devices, use the menus available in **Media**. See “Managing Media” on page 103 and “Managing Media in Robots (Robot Inventory)” on page 175 for advanced robot inventory options.

## Using Media Manager

When configuration is complete, you enable device management by starting the Media Manager device daemon (`ltd`). This starts the following daemons:

- ◆ Media Manager device daemon (`ltd`). This daemon allows Media Manager to mount volumes on the tape or optical storage devices in response to user requests.
- ◆ Media Manager volume daemon (`vmd`). This daemon is a point of contact on each media server that allows Media Manager to start local device management daemons.
- ◆ Automatic volume recognition daemon (`avrd`). If a tape or optical volume is labeled and mounted in a drive, `avrd` automatically reads the label. If the label matches information contained in a pending request, Media Manager assigns the drive to that request.
- ◆ Robotic daemons. If you defined any robots in your configuration, `ltd` starts the corresponding robotic daemons.

Once these daemons are started, applications and users can request back ups and restores.

## Requesting Volumes

NetBackup and Storage Migrator requests for volumes include the volume's media ID and device density. A request for a volume has a file name used to link to the device that is assigned. The external media ID should correspond to the Media Manager media ID. When Media Manager receives a request for a volume, it searches its EMM database for the media ID.

If the volume is in a robot, the EMM database information includes the specific robot that has the volume and the location of the volume within the robot (if applicable). Media Manager then issues a mount command to the robotic daemon controlling the robot and the volume is mounted. Control is returned to NetBackup or Storage Migrator and the media read or write operation proceeds.

---

**Note** For standalone drives, NetBackup attempts to use the media in the drive, if the media meets the selection criteria in the request. For more information, see the topic on standalone drive extensions in the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I*.

---



## Checking Barcodes

Media Manager checks barcodes to ensure that the robot loads the correct tape, in the event that the EMM database is incorrect. If the barcode on the tape does not match the barcode in the mount request, Media Manager logs an error and stops the operation. In the case of a backup or restore, NetBackup also logs an error.

If a requested volume is not in a robot, a pending request message appears 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.

If the volume is labeled (tape or optical platter), the automatic volume recognition daemon reads the label and the drive is assigned to the request. If the volume is unlabeled and not associated with a robot, the operator manually assigns the drive to the request.

## Volume Pools

Media Manager also uses a concept called volume pools. A volume pool is a set of media that can be used only by the users that you designate when you configure the pool. You specify volume pools and assign media to them when you configure Media Manager. The Media Manager device daemon validates access to volume pools.

Whenever a new volume is required for a robotic or standalone drive, Media Manager allocates it from the volume pool requested by the application. If there are no volumes available in the requested volume pool and a scratch pool has been configured, Media Manager allocates a volume from the scratch pool.

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

See “Volume Pools and Volume Groups” on page 344 for more information.

## Security Issues

See the topic, “Media Manager Security” on page 378 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 Media Manager volume daemon).
- ◆ Controlling user access to Media Manager robotic daemons and services.







## Configuring Storage Devices

---

## 2

The device management window is used to add, configure, and manage the devices (drives and robotic libraries) that Media Manager uses.

The following topics provide an overview of the NetBackup Devices window. If this is the first time you have configured devices, read the topics in the order they are presented.

- ◆ “Starting Device Management” on page 18
- ◆ “Using the Device Management Window” on page 18
- ◆ “Performing Initial Device Configuration” on page 36
- ◆ “Managing the Device Manager Service (Windows) or the Device Daemon (UNIX)” on page 38
- ◆ “The Device Mapping File” on page 39
- ◆ “NetBackup Mixed Server Configurations” on page 39
- ◆ “Administering Devices on Other Servers” on page 41
- ◆ “The Enterprise Media Manager (EMM) Server” on page 45
- ◆ “The Device Configuration Wizard” on page 48
- ◆ “Activate/Deactivate Hosts” on page 50
- ◆ “Adding NDMP Hosts” on page 50
- ◆ “Adding Robots Manually” on page 51
- ◆ “Adding Shared Drives” on page 60
- ◆ “Adding Drives” on page 61
- ◆ “Adding Optical Drives” on page 71
- ◆ “Managing Your Device Configuration” on page 76
- ◆ “Printing Your Device Configuration” on page 84
- ◆ “Robot and Drive Configuration Examples” on page 84

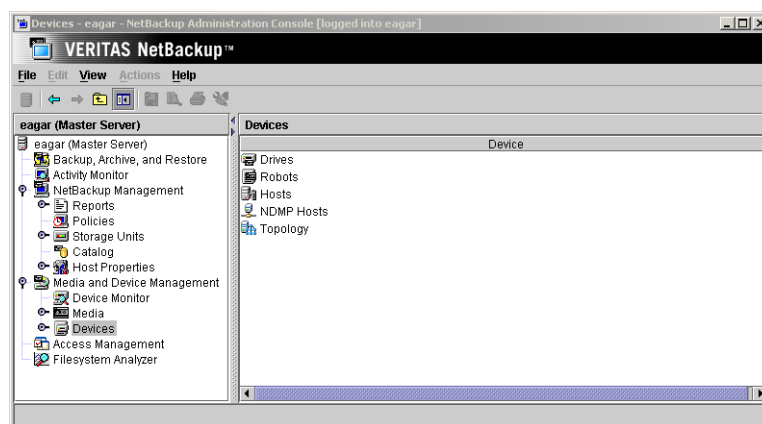


*The following topic applies only to NetBackup Enterprise Server.*

- ◆ “Administering Devices on Other Servers” on page 41

## Starting Device Management

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



## Using the Device Management Window

The following topics provide an overview of the contents of the device management window:

- ◆ “Menus and Commands” on page 19
- ◆ “Toolbars” on page 22
- ◆ “Tree Pane” on page 22
- ◆ “Messages Pane” on page 34
- ◆ “Shortcut Menus and Commands” on page 34
- ◆ “Customizing the Window” on page 35

## Menus and Commands

The items on the menus are enabled based on what you have currently selected in the NetBackup Administration Console. For example if a robot is selected in the **Robots** pane, **Inventory Robot** is enabled on the **Actions** menu.

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

Device Management Menus and Commands

Menu	Commands	Note
<b>File</b>	<p><b>Change Server</b> - Displays a dialog that allows you to change to a different server that is running NetBackup. See "Administering Devices on Other Servers" on page 41 for details.</p> <p><b>New Console</b> - Starts another instance of NetBackup Administration Console.</p> <p><b>New Window from Here</b> - Starts another instance of the NetBackup Administration Console node that was active.</p> <p><b>Adjust Application Time Zone</b> - Displays a dialog that allows you to manage the timezone. NetBackup Console can execute in a different timezone than the timezone of the server on which it was initiated. See the <i>VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I</i> for more information.</p> <p><b>Export</b> - Saves configuration information or data about the selected device monitor to a file.</p> <p><b>Page Setup</b> - Displays a setup dialog for printing.</p> <p><b>Print Preview</b> - Previews the print image.</p> <p><b>Print</b> - Prints the pane that is active in the right window.</p> <p><b>Close Window</b> - Closes the current window.</p> <p><b>Exit</b> - Closes all open windows.</p>	
<b>Edit</b>	<p><b>Change</b> - Displays a dialog for changing the configuration of the selected items.</p> <p><b>Delete</b> - Deletes selected items from the configuration.</p> <p><b>Find</b> - Command for finding items in the display lists.</p>	
<b>View</b>	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 35.	



## Device Management Menus and Commands (continued)

Menu	Commands	Note
<b>Actions</b>	<b>New</b> - Displays choices for adding robots or tape drives, or optical drives to a configuration.	
	You can also add shared drives to a configuration.	Requires Shared Storage Option license.
	Also displays a dialog for adding an NDMP host to your configuration.	Requires NDMP license.
	<b>Enterprise Media Manager Database</b> - Displays a sub-menu that allows you to synchronize the device databases of NetBackup 5.x Media Servers with the Enterprise Media Manager (EMM) 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 a menu item for removing NetBackup device hosts from the EMM database. See “The Enterprise Media Manager (EMM) Server” on page 45.	Applies only to NetBackup Enterprise Server.
	<b>Inventory Robot</b> - 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.	
	<b>Drive Diagnose</b> - Displays a dialog with choices for running diagnostic tests on a drive.	
	<b>Drive Qualify</b> - Displays a dialog with choices for running device qualification tests on a drive.	Requires Device Qualification Tools license.
	<b>Robot Diagnose</b> - Displays a dialog with choices for running diagnostic tests on a robotic library.	
	<b>Robot Qualify</b> - Displays a dialog with choices for running qualification tests on a robotic library	Requires Device Qualification Tools license.



## Device Management Menus and Commands (continued)

Menu	Commands	Note
	<p><b>Stop/Restart Media Manager Device Daemon</b> - Controls the Media Manager device daemon.</p> <p><b>Activate</b> - Activates selected hosts. Once activated, NetBackup will schedule jobs on the host as needed.</p> <p><b>Deactivate</b> - Deactivates selected hosts. When a host is deactivated:</p> <ul style="list-style-type: none"> <li>◆ Current jobs on the host are allowed to complete</li> <li>◆ No new jobs are scheduled for the host</li> <li>◆ If the host is part of a shared drive configuration, it will not scan drives while deactivated</li> </ul>	
Help	<p><b>Help Topics</b> - Provides online help information for the NetBackup Console.</p> <p><b>Troubleshooter</b> - Helps you to debug errors.</p> <p><b>License Keys</b> - Provides information about your active and registered license keys.</p> <p><b>Current NBAC User</b> - Provides NetBackup Access Control information for the current user. Gives the permissions for the user that you are currently logged in as.</p> <p><b>About NetBackup Administration Console</b> - Displays program information, version number, and copyright information.</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 35.

### ▼ To show or hide the toolbar buttons

1. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
2. Select **View > Show Toolbar**.

## Tree Pane

The tree pane for **Devices** contains entries for the following device areas. Each of these device entries in the tree can be expanded. Relevant device information for each is displayed in the window panes on the right.

### ◆ Drives

See “Drives Pane” on page 23 and “Drive Paths Pane” on page 27.

### ◆ Robots

See “Robots Pane” on page 29.

### ◆ Hosts

See “Hosts Pane” on page 30.

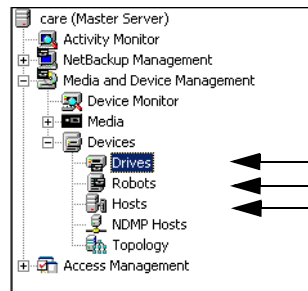
- ◆ **NDMP Hosts** (NDMP requires an NDMP license. However, this entry is visible without an NDMP license to allow you to add NearStore credentials).

See “NDMP Hosts Pane” on page 31.

### ◆ Topology

See “Topology Pane” on page 32.

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



Select a device host, robot, or drive, and the Display Pane shows information filtered for that specific selection. Select Topology and the Display Pane shows a visual representation of devices configured in your environment.

## Managing the Columns of the Display Pane

The **Edit** and **View** menus have commands for finding or showing device-related 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

- ❖ Select **View > Column Layout**

## Managing Devices on Other Servers

*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 41 for more information.

## Drives Pane

A pane showing information about all physical drives in the configuration is displayed on the right when you select **Drives**. See “Physical Drives Pane” on page 24.

The following panes are also displayed if needed:

- ◆ A pane showing path information for drives. This pane appears only if a drive is configured as a shared drive or if there are multiple paths to a drive. See “Drive Paths Pane” on page 27.
- ◆ A pane for task progress messages.



## Physical Drives Pane

This pane allows you to view detailed information about drives configured with Media Manager. The following table describes the columns in the drives list. Check the Note column for any restrictions.

Physical 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. See “Topology Icons” on page 32.	
Device Host	Contains the name of the device host (media server) where this drive is attached. If the drive has multiple paths configured, this column contains Multiple. If the drive is configured as a shared drive (SSO), this column contains Multiple.	
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 49 for details.	
Robot Type	Specifies the type of robot that contains this drive. For example, TL4. If this column is blank (UNIX) or displays <b>None</b> (Windows), 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 49 for details.	
Robot Number	Contains the number of the robot. If the drive is a standalone drive, 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.





## Physical 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	Windows - Empty. The SCSI coordinates are displayed in the appropriate columns. UNIX - Contains the path for the drive. For example, /dev/rmt/2cbn. If the drive has multiple paths configured, this column contains Multiple.  If the drive is configured as a shared drive (SSO), this column contains Multiple.	
Enabled	Contains Yes if the path is enabled. Contains No if the path is not enabled. If the drive has multiple paths configured, this column contains Multiple.  If the drive is configured as a shared drive (SSO), this column contains Multiple.	
Serial Number	Contains the drive serial number, if the drive reports a serial number.	



## Physical Drives List (continued)

Column	Description	Note
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).
Port	This column contains the SCSI port number of the drive. This column is empty for UNIX. Contains Multiple if there are multiple paths to the drive.	Applies only to NetBackup Windows servers.
Bus	This column contains the SCSI bus number of the drive. This column is empty for UNIX. Contains Multiple if there are multiple paths to the drive.	Applies only to NetBackup Windows servers.
Target	This column contains the SCSI target number (or SCSI ID) of the drive. This column is empty for UNIX. Contains Multiple if there are multiple paths to the drive.	Applies only to NetBackup Windows servers.
LUN	This column contains the SCSI logical unit number of the drive. This column is empty for UNIX. Contains Multiple if there are multiple paths to the drive.	Applies only to NetBackup Windows servers.
Cleaning Frequency	Contains the cleaning frequency for the drive (in hours). For drives in robots that do not support frequency-based cleaning, this column is blank.	
TapeAlert Enabled	Contains Yes, if TapeAlert is enabled.	
Volume Header Path	This column specifies the volume header device path for the drive.	Applies only to optical disk drives on some NetBackup UNIX servers.
Drive Comments	Contains any user comments added for the drive.	

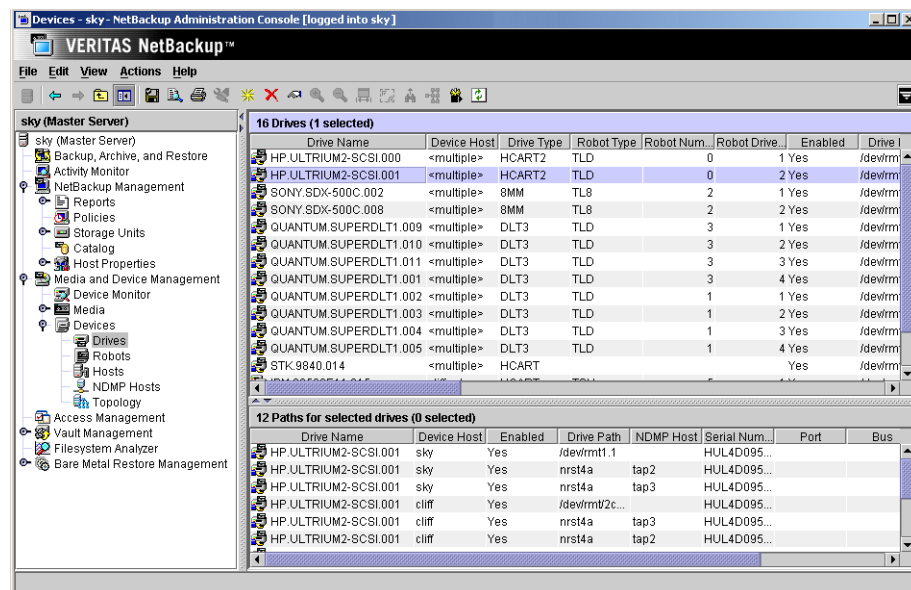


## Physical Drives List (continued)

Column	Description	Note
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. If the drive has multiple paths configured, this column contains Multiple.  If the drive is configured as a shared drive (SSO), this column contains Multiple.	Requires NDMP license.  Applies only to NetBackup Enterprise Server.
Drive Index	Drive index assigned to the drive during configuration.	

## Drive Paths Pane

This pane shows path information for drives. This pane is displayed only if a drive is configured as a shared drive (SSO option), or if there are multiple paths to a drive configured.



The following table describes the columns displayed in this pane. Review the Note column for any restrictions. All columns in this table also appear in the Drives list.

**Drive Paths List**

<b>Column</b>	<b>Description</b>	<b>Note</b>
Drive Name	Contains the configured name of the drive.	
Enabled	Contains Yes if the path is enabled. Contains No if the path is not enabled.	
Host	Contains the name of the device host (media server) where this drive is attached.	
Path	Contains the path for the drive. For example, /dev/rmt/2cbn.	
NDMP Host	Contains the name of the NDMP control host.	Requires NDMP license.
Serial Number	Contains the drive serial number, if the drive reports a serial number.	
Port	On Windows, this column contains the SCSI port number of the drive. This column is empty on UNIX hosts.	Applies only to NetBackup Windows servers.
Bus	On Windows, this column contains the SCSI bus number of the drive. This column is empty on UNIX hosts.	Applies only to NetBackup Windows servers.
Target	On Windows, this column contains the SCSI target number (or SCSI ID) of the drive. This column is empty on UNIX hosts.	Applies only to NetBackup Windows servers.
LUN	On Windows, this column contains the SCSI logical unit number of the drive. This column is empty on UNIX hosts.	Applies only to NetBackup Windows servers.



## Robots Pane

A pane showing information about all robots in your configuration is displayed on the right when you select **Robots**. The robots list displayed in this pane presents detailed information about robots configured with Media Manager.

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 49 for details.	
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 309 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.	
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, /dev/sg/c2t5l0.	
NDMP Host	Contains the name of the NDMP control host.	Requires NDMP license.
Enabled	Contains Yes if the path to the robot is enabled. Contains No if the path is not enabled.	
Robot Control Host	If the robot is not controlled by the local host, this column contains the name of the host that is providing the robotic control.	Applies only to NetBackup Enterprise Server.



## Robots List (continued)

Column	Description	Note
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.	

## Hosts Pane

A pane showing information about all hosts in your configuration is displayed on the right when you select **Hosts**.

This pane allows you to view detailed information about the servers that are referenced in your NetBackup configuration. The following table describes the columns in the hosts list:

## Hosts List

Column	Description
Host Name	Contains the name of the device host or Virtual Cluster.



## Hosts List (continued)

Column	Description
Status	<p>Contains the current host status for this server. Possible values are:</p> <p><b>Active for Tape</b> - the media server can be used for backups to tape</p> <p><b>Active for Disk</b> - the media server can be used for backups to disk</p> <p><b>Active for Tape and Disk</b> - the media server can be used for backups to both disk and tape</p> <p><b>Offline</b> - the media server is not available to be used for disk or tape backups, it will be Active again when it becomes available for disk and/or tape backups</p> <p><b>Deactivated</b> - the media server has been deactivated by the user and will only be used if the user activates it</p> <p><b>Virtual Cluster</b> - indicates that the host is a Virtual Cluster host. The active node and the cluster name are then displayed in the appropriate column. See the <i>NetBackup High Availability System Administrator's Guide for Windows, UNIX, and Linux</i> for more information.</p>
NetBackup Version	Contains the NetBackup software version.
NDMP Hosts	Contains the name of NDMP control hosts in your environment.
Active Node	For a Virtual Cluster, displays the active node. See the <i>NetBackup High Availability System Administrator's Guide for Windows, UNIX, and Linux</i> for more information.
Cluster Name	For a Virtual Cluster, displays the cluster name. See the <i>NetBackup High Availability System Administrator's Guide for Windows, UNIX, and Linux</i> for more information.

## NDMP Hosts Pane

A pane showing information about all NDMP hosts in the configuration is displayed on the right when you select **NDMP Hosts** (NDMP requires an NDMP license). A NetBackup NDMP license is *not* required to create a NearStore storage unit. See “Adding NDMP Hosts” on page 50 for more information.

This pane allows you to view detailed information about the NDMP servers that are referenced in your Media Manager configuration.



The following table describes the columns in the NDMP hosts list:

NDMP Hosts List

Column	Description
Host Name	Contains the name of the NDMP host.
Media Servers	Contains the name of a device host, if any.

## Topology Pane

A description bar is displayed at the top of the topology pane.

Your view and use of the topology pane can be customized. See “Changing the View of the Topology Pane” on page 35. 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 EMM database and is displayed in this pane.

See the following related topics:

- ◆ “Topology Icons” on page 32
- ◆ “Topology Connections” on page 33
- ◆ “Selecting Topology Objects” on page 33

## 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



Robot media



Drive



Drive that is partially configured



Drive that is shared



## 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 EMM database connections are always shown.
- ◆ Media is represented as in a robotic library. A line attaches the media to the EMM server doing media management.

## Selecting Topology Objects

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:



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

## Messages Pane

The **Messages** pane appears on the right and is used to display messages about a task that is running as a background process. This pane is displayed only if there is an informative message or error message for the task. If the task completes normally, the pane is not displayed.

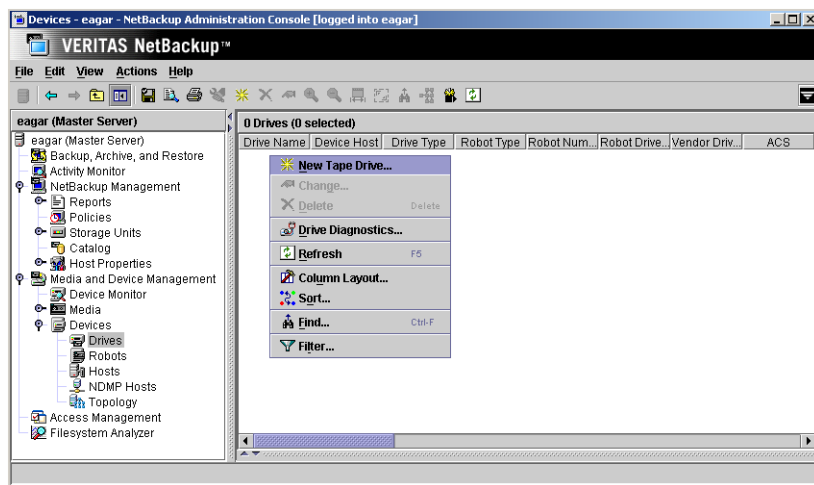
## Shortcut Menus and Commands

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

### ▼ To display a shortcut menu

- ❖ Right click on any object or section in the pane

Shortcut 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 35
- ◆ “Changing the View of the Topology Pane” on page 35

See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* for more details.

### Viewing and Rearranging Columns

This is useful if you are managing many devices. Some of the columns are initially hidden by default.

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

- ❖ Select **View > Column 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. Select **View > Options > Devices**.
2. Select **Fit topology to window on startup**.

#### ▼ To enlarge the topology diagrams

This command can be done multiple times.

- ❖ Select **View > Zoom > Zoom In**.

#### ▼ To decrease the size of the topology diagrams

This command can be done multiple times.

- ❖ Select **View > Zoom > Zoom Out**.



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

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

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

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

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

2. Use the mouse to move the selection tool (a rectangle) to select desired objects in the configuration. The selected objects will be the focus of the main topology pane.

▼ **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.

- ❖ Select **View > HighLighted Connections Only**.

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

- ❖ Select **View > HighLighted Connections Only** again.

## Performing Initial Device Configuration

For NetBackup to recognize and communicate with the connected devices, and for device discovery to discover devices, NetBackup issues SCSI passthru 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 for your UNIX server platform in the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

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 38 for information on manually controlling `ltid`.

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

The following steps describe a general method for attaching devices to a UNIX media server.



1. Physically attach the storage devices to the server and perform any required configuration steps specified by the device or operating system vendor.
2. Create any required system device files for the drives and robotic control. This is usually done during installation of the operating system.

Device files are created automatically on some UNIX platforms. Explicit configuration of device files is required on some UNIX servers to make full use of NetBackup features.

3. If the host on which you are configuring devices is not the EMM server, add the host to the `bp.conf` file on the EMM server. In order to configure devices, the device host must also be added to the list of hosts known to the EMM server. The device host is automatically added to the list of hosts known by the EMM server if the EMM server is running when the device host is installed. This is the recommended installation order. If the EMM server is not running, use the `nbemmcmd -addhost` command to add the device host.

For information about adding a host to the `bp.conf` file, see the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume II* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume II*.

See the *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for Windows* for information about using the `nbemmcmd` command.

4. 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 48.
  - ◆ “Adding Robots Manually” on page 51.
  - ◆ “Adding Drives” on page 61.
  - ◆ “Adding Shared Drives” on page 60.

*The following point applies only to NetBackup Enterprise Server.*

- ◆ If you are adding the device to a remote host, see “Administering Devices on Other Servers” on page 41.



## 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. Stopping and restarting `ltid` does not stop and start the EMM Server. The EMM Server is `nbeemm`, which runs as a daemon on UNIX and as the NetBackup Enterprise Media Manager service on Windows. Typically, it is not necessary to restart the EMM Server.

---

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

---

### ▼ To manage this daemon

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.

2. Select **Actions > Stop/Restart Media Manager Device Daemon**.

3. *The following step applies only to NetBackup Enterprise Server.*

Select a device host. The dialog also shows the current status of this daemon.

If the device host is known to NetBackup to be a Backup Exec server, the server does not appear in the list.

4. The **Action** section allows you to start, stop, or stop/restart the service. Select the action you want to perform.
5. The **Options** section allows you to eject media from a standalone drive and control the level of debug logging. Select the option you want to perform.
6. Click **OK** or **Apply**.

You may find it useful to select **Stop** and click **Apply**, and then select **Start** and click **Apply**.

*The following point applies only to NetBackup Enterprise Server.*

By using **Apply**, you can select device hosts and actions for more than one device host before clicking **OK** to close the dialog.

## The Device Mapping File

The device 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 determine which protocols and settings to use when communicating 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 requires that you download a file from the VERITAS support web site to the EMM server, run a VERITAS-supplied utility on the EMM server, and configure the devices.

---

**Note** The contents of this file do 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://support.veritas.com>) to download the latest External Types file for your devices. The files that you download are named similar to the following files: `Mappings_6_#####.TAR` and `Mappings_6_#####.ZIP`. Download the file to `/usr/opensv/var/global` on the EMM server.
2. Run `tpext` from `/usr/opensv/volmgr/bin` on the EMM server. There are no parameters for this utility. `tpext` updates the EMM database with new versions of the device mapping file and external attributes file.
3. In order for each media server in your configuration to be updated with the new device information, you must stop and restart `ltid`. This is typically done automatically as part of the device configuration process but can also be done manually.
4. Refer to the README file that is supplied with the device mappings file for additional instructions.

## 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.



**Note** Because NetBackup 6.0 allocates drives prior to starting a job, it is possible for a NetBackup 6.0 media server to override a drive selection for a job originating on a NetBackup 5.x media server. Drive selection will be optimized when all servers in your environment are at NetBackup 6.0.

---

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

- ◆ The EMM 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 6.0 can inter-operate with media servers running NetBackup 5.0, 5.1, and either of these versions with maintenance patches installed.

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

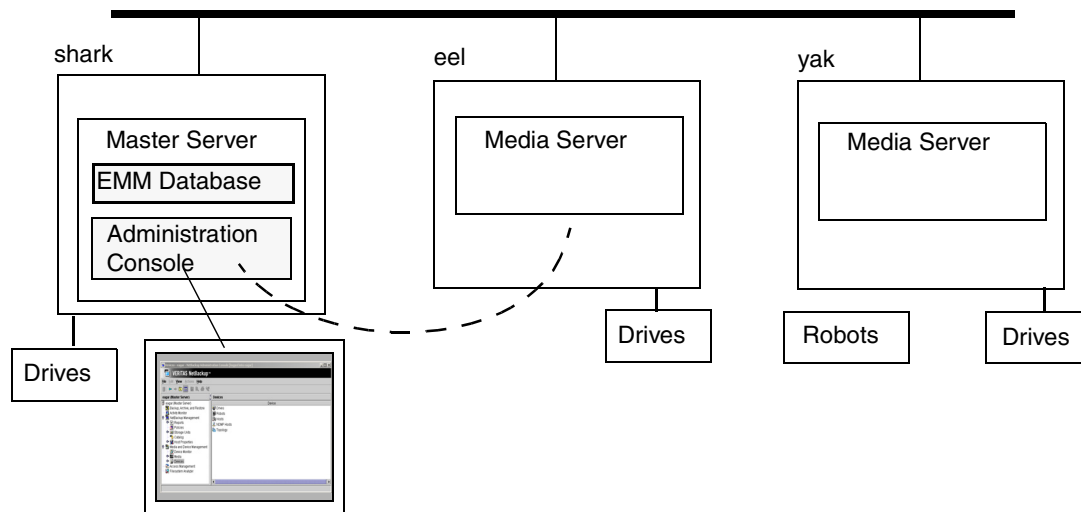
If you are using SSO, be sure to review the “Enterprise Media Manager (EMM) Device Allocator Requirements” on page 285.



## 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 EMM server.

Note that the media server must be included in the list of known device hosts with the EMM server before devices can be configured. The media server is automatically registered with the EMM server if the EMM server is running when the media server is installed. This is the recommended installation order. If the EMM server is not running, when the media server is installed, use the `nbemmcmd -addhosts` command to add the device host once the EMM Server is up. See the *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for Windows* for information about using the `nbemmcmd` command.

Once configured, these devices will be displayed 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.



You cannot change from a NetBackup Server to a NetBackup Enterprise Server. You also cannot change to a back-level server.

Also see “Remote Administration of Other UNIX Servers” on page 42.

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

1. In the NetBackup Administration Console, select the server name shown at the top of the tree.
2. Select **File > Change Server**.
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.You can also click **Remove** to delete a server from the list.
4. Click **OK**.

The name of the new server appears, and the right pane shows device information for the new server.

## Remote Administration of Other UNIX Servers

In addition to using **File > Change Server** to administer devices on other servers, you can specify a different server when logging into NetBackup.

The name of the UNIX server that you specify in the Login box, when starting the NetBackup Administration Console, must be in the NetBackup `bp.conf` file on the remote UNIX server where you want to manage devices.

### Administration Example

Refer to the previous figure. You could start the administration interface from the NetBackup UNIX server (named shark) and specify the UNIX server (named eel) in the Login box.

In this example, you

- ◆ Started the interface from the host named shark. Note that the host where the interface is running must be added to the server list of the host that you are logging into.

- ◆ Are managing NetBackup, through Java application server software running on the host named eel.
- ◆ Want to manage devices on a third host, named yak.

The `bp.conf` file on host yak must include the name of the server that you logged into (eel), *and* the host where you first started the administration interface (shark).

If you cannot connect to host yak, add hosts eel and shark to the NetBackup `bp.conf` file on host yak.

### **Adding SERVER Entries in the NetBackup `bp.conf` File**

Refer to the previous figure. Also see the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume II* for more information.

#### **▼ To add SERVER entries**

1. Add a `SERVER = host` entry below any existing server entries in the `/usr/openv/netbackup/bp.conf` file.
2. Stop and restart the NetBackup database manager (`bpdbm`) and NetBackup request daemon (`bprd`).

If you are unable to manage the devices, you may need to add a `SERVER` entry to the `vm.conf` file on host yak. See “Media Manager Security” on page 44.



## 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 as shown in the following table. 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	<i>Any</i> host can perform media and device management on this host as long as the host name where the interface is running is added to the <code>bp.conf</code> file of the server you logged into. It is not necessary to make any additions to <code>vm.conf</code> .
Any <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.

---

Media Manager authentication/authorization may affect systems where NetBackup authentication/authorization has been enabled. Connections to remote hosts will fail if authentication/authorization is enabled, an `AUTHORIZATION_REQUIRED` entry is present in `vm.conf`, and the caller does not have the required permission.

### ▼ 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 378 for more information.

### 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 Enterprise Media Manager (EMM) Server

The EMM Server is the repository for all Media Manager device configuration information. See the following topics for more information about this server:

- ◆ “A Single Host is Required” on page 45
- ◆ “How This Host is Determined” on page 46
- ◆ “Managing The EMM Server” on page 46

### 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 device configuration information.

See “Enterprise Media Manager Domain Management” on page 305 and “Frequently Asked Questions About Device Discovery” on page 321.

---

**Note** When using the Device Configuration wizard in an environment that includes NetBackup 5.x servers, 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 device information.

---



Also, the **Devices** portion of the NetBackup Administration Console requires that all hosts that are referenced need to be using the same EMM Server. **Devices** verifies database consistency between any hosts that are included for device management.

## 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 EMM server. Multiple master servers can share one EMM database located on a single host. The host containing the EMM database can be either a master server or a media server.

The **Servers** host properties must be set up to allow multiple master servers to access the EMM Server. See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* for more information about configuring host properties.

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

## Managing The EMM Server

The following topics explain the commands that are used to manage the EMM server.

### ▼ To remove a device host from the database

*This is a NetBackup Enterprise Server topic.*

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

### ▼ To synchronize the database

This procedure updates the device database on NetBackup 5.x servers to be consistent with the device configurations in the EMM server.

Synchronizing the EMM database with device databases on a back-level media server 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, select **Media and Device Management > Devices**.
2. Select **Actions > Enterprise Media Manager Database > Synchronize Enterprise Media Manager Database**.

## Why You Should Use the Media Manager Wizards

NetBackup provides a wizard for configuring devices and a wizard for configuring volumes.

Using these 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 Console or from the NetBackup Getting Started wizard. 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 the device configuration wizard to configure robots and drives.  
See “The Device Configuration Wizard” on page 48.  
*The following point applies only to NetBackup Enterprise Server.*  
If you are using the Shared Storage Option (SSO), see “Adding Shared Drives” on page 60.
2. Use the Volume Configuration wizard to configure media for robots and standalone drives.  
See “Using the Volume Configuration Wizard” on page 134.



## 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 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 39.

In some cases, the wizard may leave some devices partially configured. See “Managing Devices that are Partially-Configured” on page 49 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 321.

See the following related topics:

- ◆ “Operating System Changes” on page 48
- ◆ “Possible EMM Server Host Conflict” on page 49
- ◆ “Managing Devices that are Partially-Configured” on page 49
- ◆ “Learning More About the Device Configuration Wizard” on page 49
- ◆ “Starting the Device Configuration Wizard” on page 49

## Operating System Changes

For device discovery to discover devices, NetBackup issues SCSI passthru 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for your particular server platform.



## Possible EMM Server Host Conflict

*The following topic applies only to NetBackup Enterprise Server in environments that include 5.x Media Servers.*

When using this wizard, an EMM server conflict may be detected during device scanning. This conflict occurs when the NetBackup hosts you selected to scan in the wizard do not agree on which host stores device information. See “Managing The EMM Server” on page 46 for more information.

## 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. If you deselect a discovered device from the tree view in the wizard, the device path will be disabled.

For NetBackup 5.x device hosts, partially-configured drives are shown as **PCD** and partially-configured robots as **PCR** in the Drives list.

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 39).

## 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 49).
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. It is also available from the NetBackup 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, select **Media and Device Management > Configure Storage Devices**.

## Activate/Deactivate Hosts

Activating a host makes it available for NetBackup jobs. Deactivating a host takes it offline from your NetBackup configuration. For example, you may deactivate a host to perform maintenance. When a host is deactivated,

- ◆ Current jobs on the host are allowed to complete
- ◆ No new jobs are scheduled for the host
- ◆ If the host is part of a shared drive configuration, it will not scan drives while deactivated

▼ **To Activate or Deactivate a host**

1. In the NetBackup Administration Console, select **Media and Device Management > Hosts**.
2. From the **Hosts** pane, select the host to activate or deactivate.
3. Select **Actions > Activate or Deactivate**.

## Adding NDMP Hosts

*NDMP requires an NDMP license*

---

**Note** The credentials for a NearStore can be created using the `tpconfig` command. A NetBackup NDMP license is *not* required to create a NearStore storage unit. However, NDMP should be enabled on the NearStore since this enables the NearStore credentials to be entered using the NetBackup Administration Console.

See the *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for Windows* for details.

---

▼ **To add an NDMP host**

1. In the NetBackup Administration Console, select **Media and Device Management > NDMP Hosts**.
2. Select **Actions > New > New NDMP Host**.
3. Specify the NDMP host name.

For information about specifying NDMP hosts and NDMP host credentials, see the *NetBackup for NDMP Systems Administrator's Guide for UNIX, Windows , and Linux*.

## Adding Robots Manually

---

**Note** Using the Device Configuration wizard is the recommended method of configuring robots. See “The Device Configuration Wizard” on page 48 for more information and wizard restrictions.

---

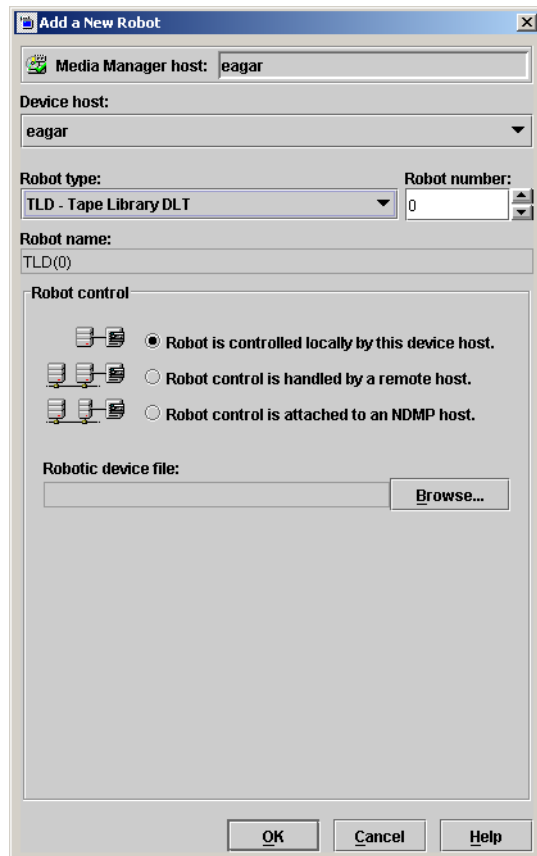
When adding a robotic library and drives, the best method is to add the robot first, as explained in the following procedure and then add the drives (see “Adding Drives” on page 61).

▼ **To add a robot**

1. Perform the steps explained in “Performing Initial Device Configuration” on page 36.
2. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
3. Select **Actions > 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.



4. Specify the properties for the robotic library as explained in “Dialog Entries for Adding and Changing Robots” on page 52.
5. Click **OK**.

## 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 53

- ◆ “Robot Type” on page 53
- ◆ “Robot Number” on page 53
- ◆ “Robot Control Section of the Dialog” on page 54

## 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.

## Robot Type

Specifies the type of robot that you are adding.

### ▼ To specify a robot type

1. Visit the VERITAS support web site (<http://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.

## 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 EMM database.

### ▼ To specify a robot number

- ❖ Enter a number or click an arrow to 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 91.

## 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 56.
- ◆ “Robot Control is Handled by a Remote Host” on page 58.
- ◆ “Robot Control is Attached to an NDMP Host” on page 59.

Also see “Robot Attributes” on page 311 for more information.

## Robot Control Configuration Overview

The following table provides an overview of robot control configuration. The first column indicates the robot control button that is valid for a particular robot type and server platform. The last column shows the configuration information that is required.

Type of Robot Control	Media Manager Robot Type	Supported Media Server Platform	Information Required for Configuration
Local	ODL	AIX, Solaris, and HP-UX (except HPIA64)	Robotic device file
Local	TL4	UNIX	Robotic device file

Type of Robot Control	Media Manager Robot Type	Supported Media Server Platform	Information Required for Configuration
Local	TL4, TL8, and TLD	Windows	Robot device or Port, Bus, Target and LUN
Local	TL8	UNIX	Robotic device file
Local	TLD	UNIX	Robotic device file
Local	TLH	UNIX (except HPIA64, AIX, Linux and Linux64) and Windows	Library name
Local	TLH	AIX	LMCP device file
Local	TSH	AIX, Solaris, Linux, and Linux64	Robotic device file
Remote	ACS	All except HPIA64 and Linux64	ACSL host
Remote	TL8	All	Robot control host
Remote	TLD	All	Robot control host
Remote	TLH	All (except Linux64)	Robot control host
Remote	TLM	All (except Linux64)	DAS/SDLC server
NDMP	ACS, TL8, TLD, and TLH	Windows, AIX, Solaris, HP-UX, and Linux (except Linux64)	NDMP host name and Robot device

### Library Sharing Example

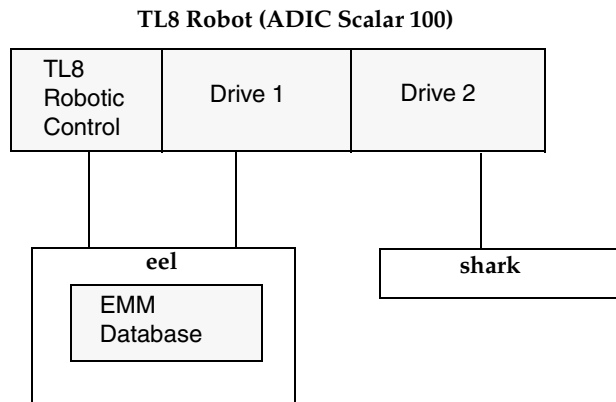
*The following example applies only to NetBackup Enterprise Server.*

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, select **Robot is controlled locally by this device host**. When you add the robot to the device configuration on shark, 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 56
- ◆ “Robot Device” on page 57
- ◆ “LMCP Device File” on page 57
- ◆ “Library Name” on page 57

#### 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**.

If the browse operation fails to find and display all of the attached robots, click **More >>** to enter the path of the device file. Your entry will be placed in **Robotic device file**.

See the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for details on manually adding device file entries.



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

### Robot Device

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

#### ▼ To specify the robot device

1. Click **Browse**.

If the discovery operation fails to find and display a robot, click **More >>** to display a dialog that allows you to specify the Port, Bus, Target, and LUN numbers, or the device name. If the browse operation fails for any other reason, a dialog appears allowing you to enter the information.

You can find Port, Bus, Target, and LUN numbers in the appropriate Windows application.

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

### LMCP Device File

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

#### ▼ To specify the LMCP file for TLH robot types

- ❖ 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 TLH robot on NetBackup Enterprise Server.*

For more information on TLH robots, see the appendix “IBM Automated Tape Library (ATL)” on page 505.

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

- ❖ 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 58
- ◆ “DAS Server” on page 58
- ◆ “ACSL Host” on page 59

### **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 505.

▼ **To specify the robot control host for 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 56, 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 519.

▼ **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)
- ◆ 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. Obtain the appropriate LibAttach software from STK and see the VERITAS support web site for the latest compatibility information.

---

For an overview of ACS robots, see the appendix, “STK Automated Cartridge System (ACS)” on page 483.

#### ▼ 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 Server or EMM server.

### 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 items.

- ◆ “Robot Device Path” on page 59
- ◆ “NDMP Host Name” on page 60
- ◆ “SCSI Coordinates (Windows host)” on page 60

#### Robot Device Path

#### ▼ To specify the robot device path

- ❖ Enter the name of the robotic device that is attached to the NDMP host.



### NDMP Host Name

#### ▼ To specify the host

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

### SCSI Coordinates (Windows host)

#### ▼ To specify the SCSI Coordinates

- ❖ Enter the Port, Bus, Target, and LUN for the robotic device.

## Adding Shared Drives

Using the Device Configuration wizard is recommended and is the easiest method for configuring drives in an SSO configuration. This wizard guides you through the steps involved in configuring drives that will be shared among device hosts.

There are also alternate ways that are available. In addition to configuring SSO faster, using the Device Configuration wizard 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 60
- ◆ “Using Alternate Interfaces to Configure Shared Drives” on page 61
- ◆ “Shared Storage Option (SSO) Topics” on page 279

## Using the Device Configuration Wizard to Configure Shared Drives

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 robot types that are supported with SSO (ACS, TL8, TLD, TLH, and TLM), VERITAS recommends using the Device Configuration wizard to add shared drives.

See “The Device Configuration Wizard” on page 48 for more information and instructions on starting the wizard.



## 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 the Media Manager device configuration wizard is recommended.

These alternatives also do not include important diagnostic tools available on UNIX servers, such as:

- ◆ Device management reports (see “Shared Storage Option Summary Reports” on page 261).

### tpconfig menus

*This topic applies only to NetBackup UNIX servers.*

If you use `tpconfig`, ensure all hosts that are sharing the drive use the same case-sensitive name for the drive (descriptive names are recommended)

For more information about using this utility, see the `tpconfig` appendix of the *VERITAS NetBackup Media Manager System Administrator's Guide for UNIX and Linux*.

### tpconfig Command Line Interface

If you use the `tpconfig` command interface, use the `-path <drivepath>` option with the `-add -drpath` command when you are defining multi-path drives. Use the `-add -drive` command when you are defining shared drives. Adding a drive on multiple hosts automatically makes it a shared drive. See the *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for Windows* for details.

## Adding Drives

---

**Note** Using the Device Configuration wizard is the recommended method of configuring drives. See “The Device Configuration Wizard” on page 48 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 36).
2. In the NetBackup Administration Console, select **Media and Device Management > Devices**.



**3. Select Actions > New > Tape Drive.**

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

The screenshot shows the 'Add a New Drive' dialog box. It has a title bar with the text 'Add a New Drive' and a close button. The dialog is divided into three main sections. The first section, 'Drive name', contains a text input field and a checkbox labeled 'Use drive name seed'. The second section, 'Host and path information', features a table with columns: 'Enabled', 'Host', 'NDMP...', 'Path', 'Serial N...', 'Port', 'Bus', 'Target', and 'LUN'. Below the table are 'Add...' and 'Remove' buttons. The third section, 'Drive information', includes a 'Drive type' dropdown menu, a 'Cleaning frequency (in hours)' spinner set to 0, a checkbox for 'Drive is in a robotic library.', a 'Robotic library' dropdown, and a 'Robot drive number' spinner set to 1. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

**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.

## 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.

The following topics explain the properties of the dialog:

- ◆ “Drive Name Section of the Dialog” on page 63

- “Drive Name” on page 63
- “Drive Name Rule” on page 64
- ◆ “Host and Path Information Section of the Dialog” on page 66
  - “Host and Path Information” on page 66
  - “No Rewind Device” on page 66
- ◆ “Drive Information Section of the Dialog” on page 67
  - “Drive Type” on page 67
  - “Cleaning Frequency” on page 67
  - “Drive Status” on page 68
- ◆ “Robotic Drive Information Section of the Dialog” on page 68
  - “Drive is in a Robotic Library” on page 69
  - “Robotic Library” on page 69
  - “Robot Drive Number” on page 69

## Drive Name Section of the Dialog

Specifies specific information about the drive.

- ◆ “Drive Name” on page 63
- ◆ “Drive Name Rule” on page 64

## 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. Drive names are limited to 48 characters.

### ▼ To specify the drive name

See “Allowable Media Manager Characters” on page 308 for a list of allowable characters.

- ❖ Enter a name for the drive. Alternatively, use a drive name rule to create a unique drive name. For more information on using rules for naming drives, see “Drive Name Rule” on page 64.



## Drive Name Rule

Select the **Use Drive Name Rules** checkbox to automatically create drive names based on rules you specify. You can use drive name rules when a drive is first added to your configuration. The default drive name rule creates names in the format VendorID.ProductID.INDEX. For example, the default name for a Quantum DLT8000 drive is QUANTUM.DLT8000.000. You can update the global drive name rule or create a local drive name rule.

A global rule is stored in the EMM database and used on all connected device hosts. The global rule is used for the drive name unless a host-specific rule, or local rule, is specified. Use any of the following drive attributes as part of a drive name rule.

---

**Note** The maximum length of a drive name is 48 characters.

---

- ◆ Host name
- ◆ Robot number
- ◆ Robot type
- ◆ Drive position

Drive position information varies depending on the robot type. Drive position information can be ACS coordinates, TLM/TLH vendor drive name, or simply the robot drive number.

- ◆ Drive type
- ◆ Serial number
- ◆ Vendor ID
- ◆ Product ID
- ◆ Index

A **Custom Text** field is also available which accepts any of the allowable Media Manager characters.

See “Allowable Media Manager Characters” on page 308 for a list of allowable characters.





### ▼ To configure drive name rules

1. Select **Configure** in the Add a New Drive dialog. The Configure Drive Name Rules dialog is displayed.

**Configure Drive Name Rules**

Use this dialog to automatically create drive names based on rules you specify. The default drive name rule creates names in the format VendorID.ProductID.INDEX.

**Host selection**  
Select the hosts for which to configure the rule.

☐ Global Rule

☐ hagar

**Fields and order**  
Select the fields that will be part of the drive name.

vendor ID  
serial number  
robot type  
host name  
product ID  
drive type  
robot number  
drive position  
index

Add >>

**Choose the order in which the fields appear.**

Move Up  
Move Down  
Remove

Custom text:  
Add >>

Create Rule

**Configured drive name rules**

Host Name	Rule
GLOBAL	<vendor ID>.<product ID>.<index>

Delete Rule

2. Select the **Global Rule** checkbox to update a rule for all Media Servers in your environment.

Select the check box for the device host to create a rule that will be used locally on the device host only. A local rule overrides the global rule for devices attached to the specified host.

3. Select the desired fields from which to create the drive name from the list of available fields. Click **Add>>** to make a field part of your rule.

To add your own text to the drive name rule, enter the desired text in the **Custom Text** field and click the **Add>>** button to the right of the field.

**Note** If <host name> is used in the rule construction and the drive to add is a shared drive, the host name of the first host which discovers the drive is used as the host name component in the drive name. The name for a shared drive must be identical on all servers sharing the drive.



4. Use the **Move Up**, **Move Down**, and **Remove** buttons to change the order in which to use the fields defined for the rule.
5. Click **Create Rule** to finalize the rule. Click **OK** to return to the New Drive dialog.

## Host and Path Information Section of the Dialog

Specify the properties of the media server to which you are adding the drive.

- ◆ “Host and Path Information” on page 66
- ◆ “No Rewind Device” on page 66

## Host and Path Information

Specifies the device host and path for the drive. You can specify multiple paths to the same physical device. Adding multiple paths may cause the drive to become shared.

### ▼ To specify a device host

1. Click **Add**.
2. In the **Add Path** dialog, click the arrow and select a host from the list.

### ▼ To add a path

- ❖ In the **Add Path** dialog, click **Browse** to add a path to an existing device.  
For information on specifying the device path, see “No Rewind Device” on page 66.

## 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

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`.

▼ **To specify the no rewind device file**

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

If you are using NDMP drives, see the *VERITAS NetBackup for NDMP System Administrator's Guide* for configuration information.

## **Drive Information Section of the Dialog**

Specifies information about the drive properties.

- ◆ “Drive Type” on page 67
- ◆ “Cleaning Frequency” on page 67
- ◆ “Drive Status” on page 68

## **Drive Type**

Specifies the type of drive that you are adding.

If the drive will be used to write WORM media, see “Using WORM Media” on page 141 for more information.

See “Media Manager Media Types” on page 310 for more information.

▼ **To specify the drive type**

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

## **Cleaning Frequency**

*NetBackup does not support cleaning drives in some robot types. See “Robot Attributes” on page 311 for more information.*

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 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.



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

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

You can perform drive cleaning functions from the Device Monitor. See “Drive Cleaning Functions” on page 251 for more information.

### ▼ To specify a cleaning frequency

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

## Drive Status

When a drive is added, the default drive status is UP, meaning the drive is available. When the status is up, the default mode is AVR (Automatic Volume Recognition) for all drives except optical drives on an HP9000-800, which are normally in OPR (operator control) mode.

### ▼ To change the drive status

- ❖ Click **UP** or **DOWN**.

You can also change the drive status using commands found on the **Actions** menu in **Device Monitor**.

## Robotic Drive Information Section of the Dialog

Specifies information about a drive in a robotic library.

- ◆ “Drive is in a Robotic Library” on page 69
- ◆ “Robotic Library” on page 69
- ◆ “Robot Drive Number” on page 69

## 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 68).

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

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

## 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 TL8 robot you can add drive 2 before drive 1.

If you assign the wrong number Media Manager does not detect it initially, but an error will occur when the robotic control attempts to mount media on the wrong drive. Configuration of drives using the correct Robot Drive Number is important to the proper mounting and utilization of media. The Robot Drive Number, commonly set based on correlation of the drive serial number with drive serial number information from the robotic library, should be determined and validated before the device configuration is considered complete.

---

**Note** **Robot drive number** does not apply when adding drives to API robots. See “Robot drive number for API Robots” on page 70.

---



▼ **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 336 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 70 for more information.
- ◆ TLH robots (Tape Library Half-inch). See “TLH” on page 71 for more information.
- ◆ TLM robots (Tape Library Multimedia). See “TLM” on page 71 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 483, has further information.

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

For	Enter
<b>ACS Number</b>	The index (in ACS library software terms) that identifies the robot that has this drive.
<b>LSM Number</b>	The Library Storage Module that has this drive.



For	Enter
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 initially, 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.

Media Manager does not initially detect if you have assigned the wrong device number. An error will occur when the robot mounts media on the wrong drive.

The appendix, “IBM Automated Tape Library (ATL)” on page 505, has further information about TLH robots.

## 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.

Media Manager does not initially detect if you have assigned the wrong device number. 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 519, has further information about TLM robots.

# Adding Optical Drives

**Note** Using the Device Configuration wizard is the recommended method of configuring drives. See “The Device Configuration Wizard” on page 48 for wizard restrictions and more information.



▼ **To add optical drives**

1. Complete the steps necessary for the server to recognize the attached drives (see “Performing Initial Device Configuration” on page 36).
2. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
3. Select **Actions > New > Optical 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 Optical Drives” on page 72.
5. Click **OK**.

The display now shows the new drive information.

## **Dialog Entries for Adding or Changing Optical 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.

The following topics explain the properties of the dialog:

- ◆ “Drive Name Section of the Dialog” on page 73
  - “Drive name” on page 73
  - “Use drive name rule” on page 73
- ◆ “Host and Path Information Section of the Dialog” on page 73
  - “Host and Path Information” on page 73
  - “Data/Device path” on page 74
  - “Volume Header Device Path” on page 74
- ◆ “Robotic Information Section of the Dialog” on page 74
  - “Drive is in a robotic library” on page 74
  - “Robotic library” on page 75
  - “Robot drive number” on page 75



## Drive Name Section of the Dialog

Specifies specific information about the optical drive.

### 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

See “Allowable Media Manager Characters” on page 308 for a list of allowable characters.

- ❖ Enter a name for the drive. Alternatively, use a drive name rule to create a unique drive name. For more information on using rules for naming drives, see “Drive Name Rule” on page 64.

### Use drive name rule

See “Drive Name Rule” on page 64.

## Host and Path Information Section of the Dialog

Specifies the media server to which you are adding the drive.

Specify the properties of the media server to which you are adding the drive.

- ◆ “Host and Path Information” on page 73
- ◆ “Data/Device path” on page 74
- ◆ “Volume Header Device Path” on page 74

### Host and Path Information

*Host and Path Information applies only to NetBackup Enterprise Server.*

Specifies the device host and path for the drive.

#### ▼ To specify a device host

- ❖ In the **Host and Path Information** section of the dialog, click the arrow and select a host from the list.



## Data/Device path

*Data/Device path applies only to optical disk drives on NetBackup UNIX servers.*

Data/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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*. Media Manager uses character mode device files.

### ▼ To specify the data/device path

- ❖ Enter the data/device file path for the drive or click **Browse** to locate the device.

## Volume Header Device Path

*Volume Header Device Path 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

### ▼ To specify the volume header device path

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

## Robotic Information Section of the Dialog

Specifies information about a drive in a robotic library.

- ◆ “Drive is in a robotic library” on page 74
- ◆ “Robotic library” on page 75
- ◆ “Robot drive number” on page 75

## Drive is in a robotic library

### ▼ To specify that a drive is under robotic control

1. Select **Drive is in a robotic library**.

Enter additional information about the drive in the **Robotic information** section.

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

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

## 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 an ODL robot you can add drive 2 before drive 1.

If you assign the wrong number Media Manager does not detect it initially, 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 70.

---

### ▼ 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 336 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 70 for more information.
- ◆ TLH robots (Tape Library Half-inch). See “TLH” on page 71 for more information.
- ◆ TLM robots (Tape Library Multimedia). See “TLM” on page 71 for more 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 76
- ◆ “Using the Device Configuration Wizard for Configuration Changes” on page 77
- ◆ “Changing a Robot Configuration” on page 77
- ◆ “Changing the Configuration of a Drive” on page 77
- ◆ “Changing a Non-Shared Drive to a Shared Drive” on page 78
- ◆ “Deleting Robots” on page 78
- ◆ “Deleting Drives” on page 79
- ◆ “Performing Device Diagnostics” on page 79
- ◆ “Printing Your Device Configuration” on page 84

Also see “Making Changes to Your Hardware Configuration” on page 363 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 48. 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, select **Media and Device Management > Devices**.
2. Select **Robots** in the tree pane.
3. Select the robotic library you want to change from the Robots pane on the right.
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 52).
6. Click **OK**.

## Changing the Configuration of a Drive

### ▼ To change configuration information for a drive

1. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
2. Select **Drives** in the tree pane.
3. Select the drive you want to change from the Drives pane on the right.
4. Select **Edit > Change**.



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).

5. Click **OK**.

## Changing a Non-Shared Drive to a Shared Drive

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, select **Media and Device Management > Devices**.
2. Select **Drives** in the tree pane.
3. Select the non-shared drive you want to change from the Drives pane on the right.
4. Right-click and select **Change** on the shortcut menu.

In the **Change Tape Drive** dialog, select **Add** and add a new path to the drive. Adding paths automatically shares a drive.

## Deleting Robots

---

**Note** Any drives that are configured as residing in a robot that you delete will be changed to standalone drives. Any media in the deleted robot is also moved to standalone.

---

### ▼ To delete a robot

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

## Deleting Drives

### ▼ To delete a drive

1. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
2. Select **Drives** in the tree pane.
3. Select the drive or drives that you want to delete from the pane on the right.
4. Select **Edit > Delete**.
5. Answer the delete confirmation dialog.

## Performing Device Diagnostics

Media Manager drive and robot diagnostic functions allow you to execute and manage device 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 robotic library or tape drive problems.

Device diagnostic test functions include the following tasks:

- ◆ “Executing Diagnostic Tests for a Drive” on page 79
- ◆ “Executing Diagnostic Tests for a Robotic Library” on page 81
- ◆ “Exiting a Diagnostic Test When Testing is Complete” on page 83
- ◆ “Stopping a Diagnostic Test and Changing the Device to be Tested” on page 83
- ◆ “Obtaining Detailed Information For a Particular Test Step” on page 83
- ◆ “Managing a Test Step that Requires Operator Intervention” on page 83

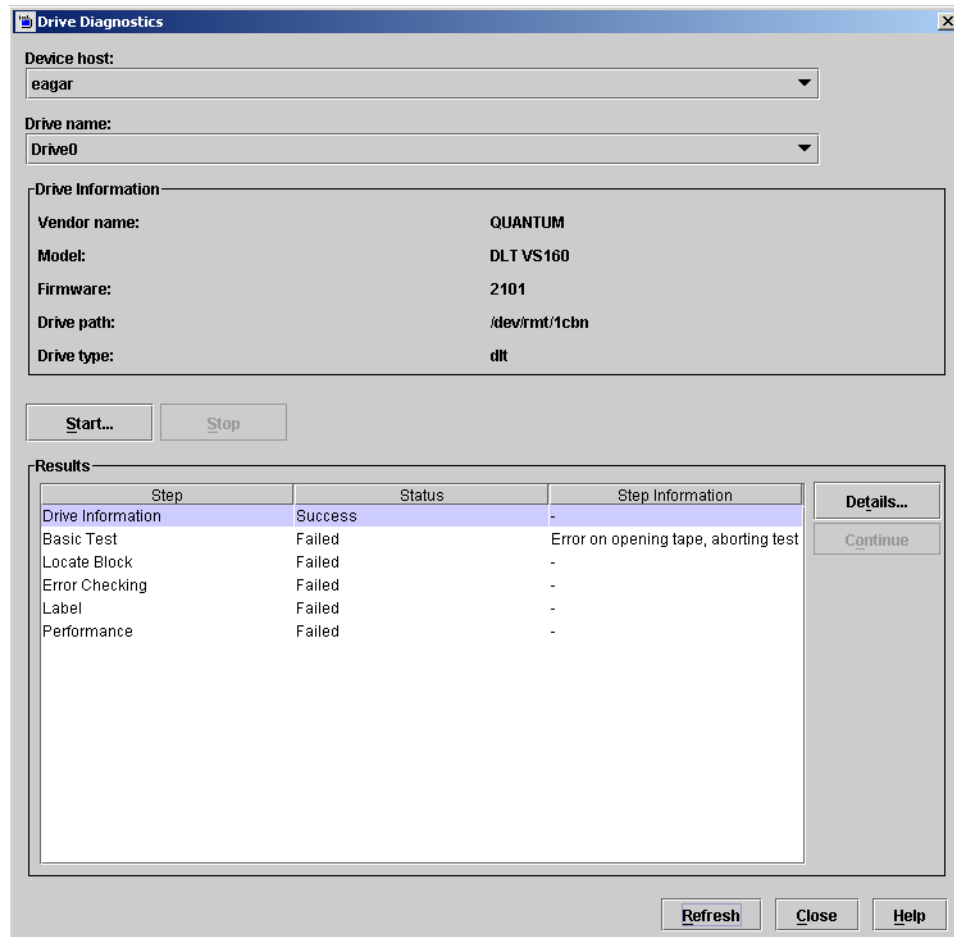
## Executing Diagnostic Tests for a Drive

### ▼ To execute tests

1. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
2. Select **Actions > Drive Diagnostics**.



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. 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.



6. For a standalone drive that you want to test, manually insert the requested pre-labelled test tape displayed in **Step Information**. For robotic drives, the media is loaded automatically.
7. The results of each step in the test are shown in the **Results** display. Click **Refresh** to update the Results display.

### Executing Diagnostic Tests for a Robotic Library

Use this procedure to diagnose TLD or TL8 robotic libraries. Diagnostic testing of API-attached robotic tape libraries and other types of SCSI-attached libraries is not supported.

Ensure that the library to be tested is properly configured for use with NetBackup. Testing is conducted using the existing NetBackup robotic control daemons or processes.

#### ▼ To execute tests

1. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
2. Select **Actions > Robot Diagnostics**.



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

The **Robot Diagnostics** dialog box contains the following sections:

- Device host:** A dropdown menu with the value "eagar".
- Robot name:** A dropdown menu with the value "TLD(0)".
- Drive Information:** A section displaying the following details:
  - Vendor name: QUANTUM
  - Model: ValueLoader
  - Firmware: 2101
  - Robot path: /dev/sg/c0t0l1
  - Robot type: tld
- Buttons:** "Start..." and "Stop" buttons are located below the Drive Information section.
- Results:** A table showing the progress of diagnostic tests.
 

Step	Status	Step Information
Device Mappings Test	Success	-
Robot Initialize	Success	-
Move Test	Success	-
Scsi Command Test	In Progress	-
Robot Error Checking	Pending	-
- Buttons:** "Details..." and "Continue" buttons are located to the right of the Results table.
- Footer:** "Refresh", "Close", and "Help" buttons are located at the bottom right of the dialog.

3. Select the media server that is the device host for the robot that you want to test in the **Device Host** box.
4. Select the robot that you want to diagnose in the **Robot Name** box.  
Information for the robot you selected is displayed in the Robot 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 Device to be Tested

### ▼ To stop a test and change the device

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 or Robot Name boxes, select the host and the device 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 display.
2. Click **Details**. A dialog appears that displays 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 tests.

3. Click **Close** to return to the Device 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.

## Printing Your Device Configuration

▼ **To print your current device configuration**

1. In the NetBackup Administration Console, select **Media and Device Management > Devices**.
2. In the tree pane select **Drives, Robots, Hosts, NDMP Hosts, or Topology**.
3. Click in the pane on the right.
4. Select **File > Print**.

▼ **To print your current device configuration using tpconfig**

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
```

---

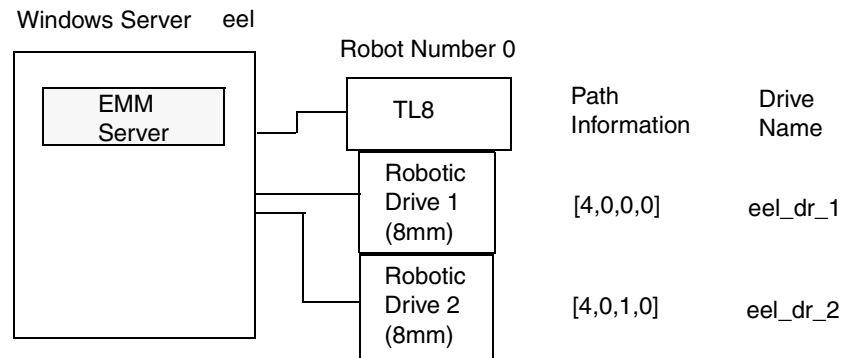
**Note** `tpconfig -d` and `tpconfig -l` may truncate drive names. Use `tpconfig -dl` to obtain the full drive name.

---

## Robot and Drive Configuration Examples

After installing Media Manager software and attaching the devices, run the Device Configuration wizard or complete the Add Robot and Add Drive dialog entries. Refer to the values shown in the tables in the examples when adding similar devices. Your entries may vary from those shown in these tables.

## Example 1: Configuring a Robot on a Server



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

### Add Robot Dialog Entries (local host)

Device Host	eel
Robot Type	TL8 (Tape Library 8MM)
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 servers.

### Add Drive Dialog Entries (Drive1)

Device Host	eel
Drive Name	eel_dr_1
Drive Type	8mm Cartridge (8mm)
Path Information	[4,0,0,0]



### Add Drive Dialog Entries (Drive1) (continued)

---

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

---

### Add Drive Dialog Entries (Drive2)

---

Device Host	eel
Drive Name	eel_dr_2
Drive Type	8mm Cartridge (8mm)
Path Information	[4,0,1,0]
Cleaning Frequency	0 (hours)
Drive is in a Robotic Library	Yes
Robotic Library	TL8(0) - eel
Robot Drive Number	2

---

If eel was a UNIX server you would complete the following dialog entries.

### Add Robot Dialog Entries (local host)

---

Device Host	eel
Robot Type	TL8 (Tape Library 8MM)
Robot Number	0
Robot is controlled locally by this device host	Set (cannot be changed for this robot type)
Robotic Device File	/dev/sg/c0t4l0

---



**Add Drive Dialog Entries (Drive1)**

---

Device Host	eel
Drive Name	eel_dr_1
Drive Type	8mm Cartridge (8mm)
No Rewind Device	/dev/rmt/5cbn
Cleaning Frequency	25 (hours)
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TL8(0) - eel
Robot Drive Number	1

---

**Add Drive Dialog Entries (Drive2)**

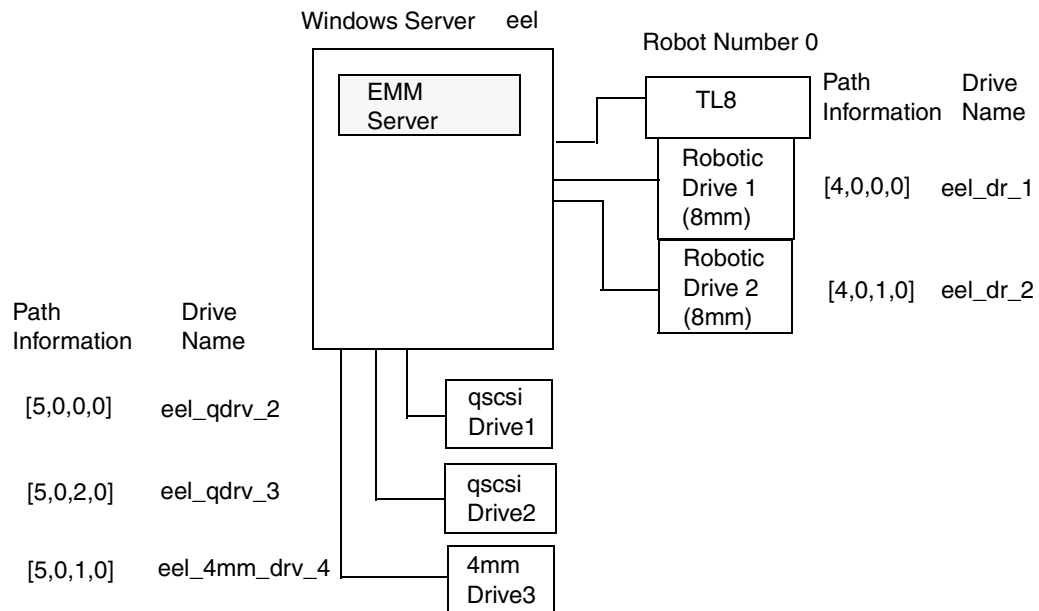
---

Device Host	eel
Drive Name	eel_dr_2
Drive Type	8mm Cartridge (8mm)
No Rewind Device	/dev/rmt/6cbn
Cleaning Frequency	25 (hours)
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TL8(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. Configuration information for the robot and its two drives is the same as in “Example 1: Configuring a Robot on a Server” on page 85 and is not repeated here.

### Add Drive Dialog Entries (Drive1)

Device Host	eel
Drive Name	eel_qdrv_2
Drive Type	1/4" Cartridge (qscsi)
Path Information	[5,0,0,0]
Drive is in a Robotic Library	No

### Add Drive Dialog Entries (Drive2)

Device Host	eel
-------------	-----



## Add Drive Dialog Entries (Drive2) (continued)

---

Drive Name	eel_qdrv_3
Drive Type	1/4" Cartridge (qscsi)
Path Information	[5,0,2,0]
Drive is in a Robotic Library	No

---

## Add Drive Dialog Entries (Drive3)

---

Device Host	eel
Drive Name	eel_4mm_drv_4
Drive Type	4mm Cartridge (4mm)
Path Information	[5,0,1,0]
Cleaning Frequency	0 (hours)
Drive is in a Robotic Library	No

---

If eel was a UNIX server you would complete the following dialog entries.

## Add Drive Dialog Entries (Drive1)

---

Device Host	eel
Drive Name	eel_qdrv_2
Drive Type	1/4" Cartridge (qscsi)
No Rewind Device	/dev/rmt/2cbn
Drive Status	UP
Drive is in a Robotic Library	No

---



Add Drive Dialog Entries (Drive2)

---

Device Host	eel
Drive Name	eel_qdrv_3
Drive Type	1/4" Cartridge (qscsi)
No Rewind Device	/dev/rmt/3cbn
Drive Status	UP
Drive is in a Robotic Library	No

---

Add Drive Dialog Entries (Drive3)

---

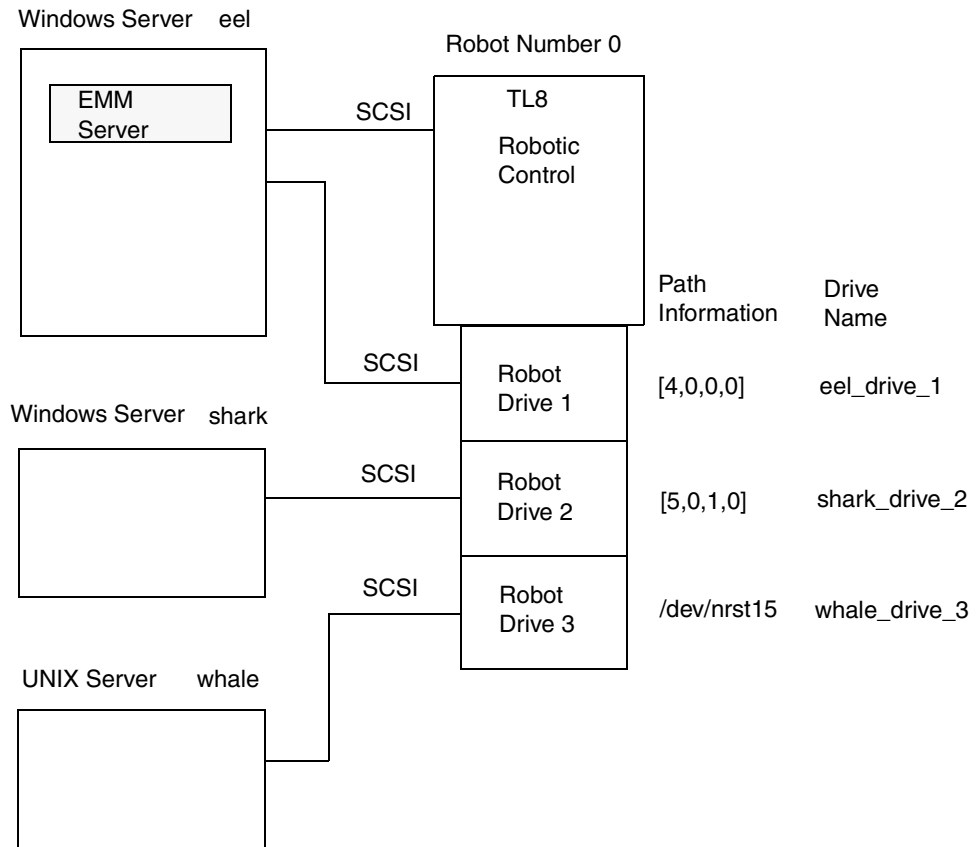
Device Host	eel
Drive Name	eel_4mm_drv_4
Drive Type	4mm Cartridge (4mm)
No Rewind Device	/dev/rmt/4cbn
Cleaning Frequency	25 (hours)
Drive Status	UP
Drive is in a Robotic Library	No

---



## 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. Some things to note when reviewing this example follow:

- ◆ Media for all devices is configured in an EMM server, 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 EMM server 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 (local host)

---

Device Host	eel
Robot Type	TL8 (Tape Library 8MM)
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.

---

### Add Drive Dialog Entries (Drive 1)

---

Device Host	eel
Drive Name	eel_drive_1
Drive Type	8mm Cartridge (8mm)
Path Information	[4,0,0,0]
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 (remote host)

---

Device Host	shark
-------------	-------

---



---

Add Robot Dialog Entries (remote host) (continued)

---

Robot Type	TL8 (Tape Library 8MM)
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)
Path Information	[5,0,1,0]
Cleaning Frequency	0 (hours)
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 (remote host)

---

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

---



Add Drive Dialog Entries (Drive 3)

---

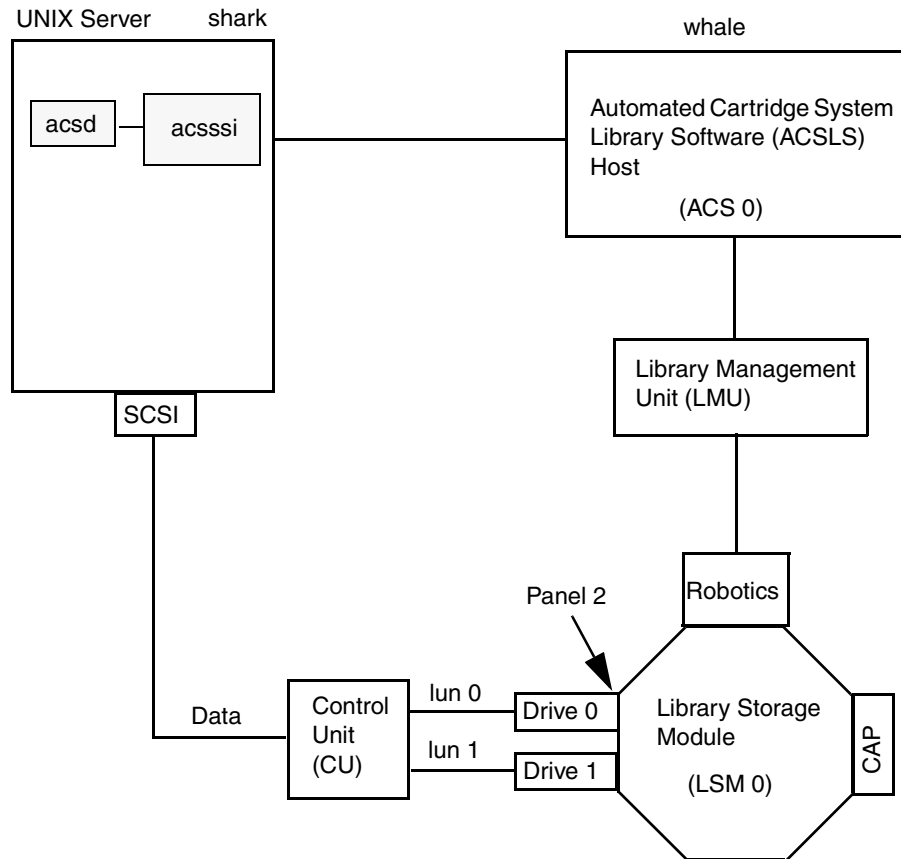
Device Host	whale
Drive Name	whale_drive_3
Drive Type	8mm Cartridge (8mm)
No Rewind Device	/dev/nrst15
Cleaning Frequency	20 (hours)
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TL8(0) - eel
Robot Drive Number	3

---



## Example 4: Configuring an ACS Robot on a UNIX Server

*The following example applies only to NetBackup Enterprise Server.*



This configuration uses an Automated Cartridge System (ACS) robot for storage. Host shark can be a UNIX NetBackup master server or media server. Some items to note when reviewing this example follow:

- ◆ The ACSLS host (in the Add Robot dialog) is server whale, where the ACS library software resides. In this example, Automated Cartridge System Library Software (ACSLs) 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, PANEL, LSM, and DRIVE numbers are part of the ACS library software configuration and must be obtained from that system.



- ◆ 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 server is over the network using ACS Storage Server Interface (acsssi).

See the appendix, “STK Automated Cartridge System (ACS)” on page 483 for more information.

Add Robot Dialog Entries (remote host)

---

Device Host	shark
Robot Type	ACS (Automated Cartridge System)
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 Name	shark_drive_0
Drive Type	1/2" Cartridge (hcart)
No Rewind Device	/dev/rmt1.1
Drive is in a Robotic Library	Yes
Robotic Library	ACS(0) - whale

---





---

**Add Drive Dialog Entries (Drive 0) (continued)**

---

ACS	ACS Number: 0
	LSM Number: 2
	PANEL Number: 0
	DRIVE Number: 0

---

---

**Add Drive Dialog Entries (Drive 1)**

---

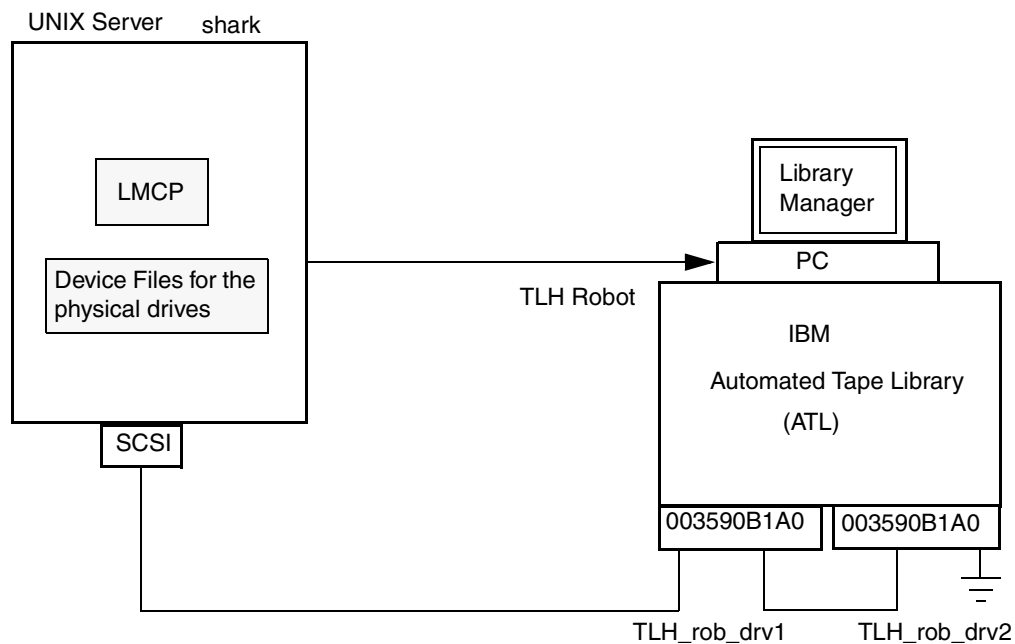
Device Host	shark
Drive Name	shark_drive_1
Drive Type	1/2" Cartridge (hcart)
No Rewind Device	/dev/rmt1.1
Drive is in a Robotic Library	Yes
Robotic Library	ACS(0) - whale
ACS	ACS Number: 0
	LSM Number: 2
	PANEL Number: 0
	DRIVE Number: 1

---



## Example 5: Configuring a TLH Robot on a UNIX Server

*The following example applies only to NetBackup Enterprise Server.*



This configuration adds a TLH robot to the configuration. The server shark can be a UNIX (AIX, Solaris, HP-UX), Linux, or Windows server, and can be a NetBackup master server or media server. Some things to note when reviewing this example follow:

- ◆ The robot control host is the server shark. Note that it is also possible to have the robotic control (`tlhcd`) on a different server.
- ◆ The main difference between configuring a TLH robot and other robot types is the robotic device file. The robotic device file is the Library Manager Control Point (LMCP) file on AIX systems and is the library name on non-AIX systems.

In this example, shark is a AIX server, so the LMCP file is specified for the robotic device file.

If shark was a UNIX server that was not AIX or a Windows server, you would specify the library name (for example 3494AH).

See the appendix, “IBM Automated Tape Library (ATL)” on page 505 for more information.

- ◆ The drive configuration uses the IBM device number. A cleaning frequency cannot be assigned using Media Manager.

---

**Add Robot Dialog Entries (local host)**

---

Device Host	shark
Robot Type	TLH (Tape Library Half-inch)
Robot Number	0
Robot is controlled locally by this device host	Set
LMCP Device File	/dev/lmcp0

---

---

**Add Drive Dialog Entries (Drive 1)**

---

Device Host	shark
Drive Name	TLH_rob_drv1
Drive Type	1/2" Cartridge (hcart)
No Rewind Device	/dev/rmt4.1
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TLH(0) - shark
Vendor Drive Identifier	003590B1A00

---



**Add Drive Dialog Entries (Drive 2)**

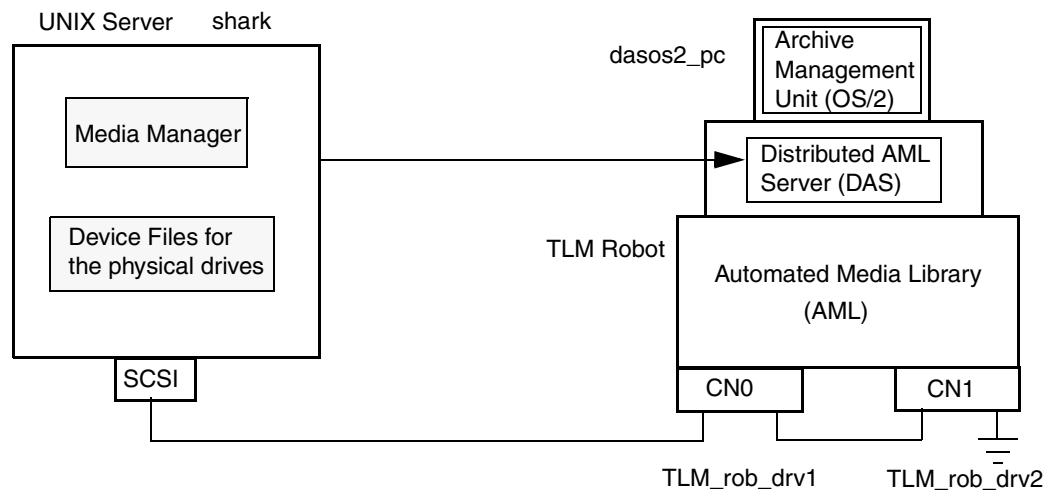
---

Device Host	shark
Drive Name	TLH_rob_drv2
Drive Type	1/2" Cartridge (hcart)
No Rewind Device	/dev/rmt1.1
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TLH(0) - shark
Vendor Drive Identifier	003590B1A01

---

## Example 6: Configuring a TLM Robot on a UNIX Server

*The following example applies only to NetBackup Enterprise Server.*



This configuration adds a TLM robot. The device configuration for this robot is similar to the TL8 robot explained in “Example 1: Configuring a Robot on a Server” on page 85.

However with a TLM robot, you specify the DAS/SDLC server instead of a robot control host. This server may reside on an IBM OS/2 system, usually in or near the robot cabinet, or on a Windows server.

In this example, the DAS Server entry is `dasos2_pc`. It is also necessary to verify that the DAS/SDLC server is configured to recognize server shark as a client and that the AML drives are allocated to shark.

See the appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 519 for further information.

---

**Add Robot Dialog Entries (remote host)**

---

Device Host	shark
Robot Type	TLM (Tape Library Multimedia)
Robot Number	0
Robot control is handled by a remote host	Set (cannot be changed for this robot type)
DAS Server	dasos2_pc

---

---

**Add Drive Dialog Entries (Drive 1)**

---

Device Host	shark
Drive Name	TLM_rob_drv1
Drive Type	1/2" Cartridge (hcart)
No Rewind Device	/dev/rmt/rmt0h
Cleaning Frequency	25 (hours)
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TLM(0) - shark
Vendor Drive Identifier	CN0

---



Add Drive Dialog Entries (Drive 2)

---

Device Host	shark
Drive Name	TLM_rob_drv2
Drive Type	1/2" Cartridge (hcart)
No Rewind Device	/dev/rmt/rmt1h
Cleaning Frequency	25 (hours)
Drive Status	UP
Drive is in a Robotic Library	Yes
Robotic Library	TLM(0) - shark
Vendor Drive Identifier	CN1

---



This chapter explains how to use the NetBackup 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 (Robot Inventory)” on page 175 explains how to use the robot inventory functions to manage media in robots.

See the following related topics:

- ◆ “Starting Media Management” on page 104
- ◆ “Using the Media Management Window” on page 105
- ◆ “Adding New Volumes” on page 123
- ◆ “Using the Volume Configuration Wizard” on page 134
- ◆ “Configuring Volume Pools” on page 135
- ◆ “Using WORM Media” on page 141
- ◆ “Methods Available for Injecting and Ejecting Volumes” on page 146
- ◆ “Rescanning and Updating Barcodes for a Robot” on page 149
- ◆ “Ejecting Volumes From Robots (Actions Menu Command)” on page 148
- ◆ “Moving Volumes” on page 151
- ◆ “When to Delete Volumes” on page 155
- ◆ “Labeling Media” on page 157
- ◆ “Erasing Media Functions” on page 159
- ◆ “Deassigning Volumes” on page 161
- ◆ “Changing the Attributes for a Volume” on page 163
- ◆ “Changing the Volume Group of a Volume” on page 168
- ◆ “Moving A Volume Group” on page 169
- ◆ “Exchanging Volumes” on page 170



- ◆ “Recycling Volumes” on page 172

*The following topic applies only to NetBackup Enterprise Server.*

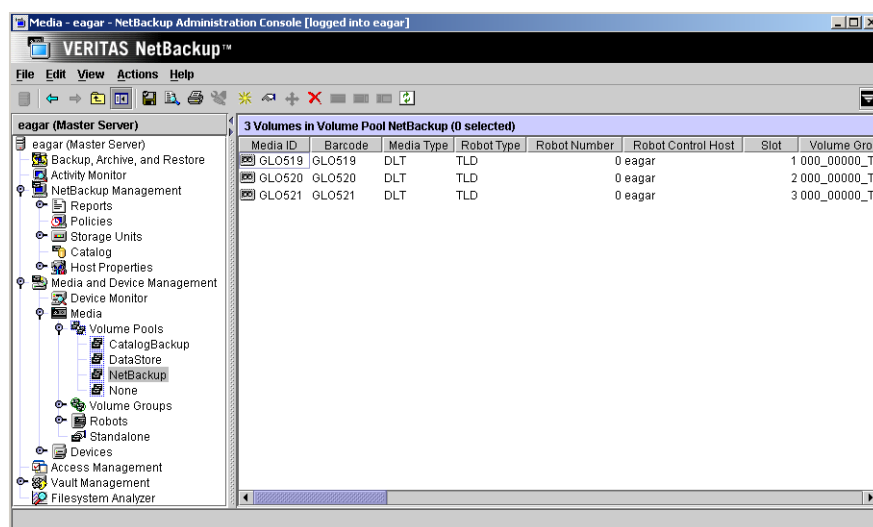
- ◆ “Administering Media on Other Servers” on page 122

Note the following special cases:

- ◆ If you have Backup Exec volumes to manage, see the Backup Exec Tape Reader topics in the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I*.
- ◆ If you have volumes without barcodes to manage, see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354.

## Starting Media Management

In the NetBackup Administration Console, select **Media and Device Management > Media**. A 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. A third pane for task progress messages is displayed when needed.



## Using the Media Management Window

The following topics in this section describe the menus and commands available in the media management window:

- ◆ “Menus and Commands” on page 105
- ◆ “Toolbars” on page 107
- ◆ “Tree Pane” on page 108
- ◆ “Volumes Pane” on page 109
- ◆ “Messages Pane” on page 120
- ◆ “Shortcut Menus and Commands” on page 120
- ◆ “Customizing the Window” on page 121

### 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
<b>File</b>	<p><b>Change Server</b> - Displays a dialog that allows you to change to a different host that is running NetBackup. See “Managing Media on Other Servers” on page 122 for details.</p> <p><b>New Console</b> - Starts another instance of NetBackup Administration Console.</p> <p><b>New Window from Here</b> - Starts another instance of the NetBackup Administration Console node that was active.</p> <p><b>Adjust Application Time Zone</b> - Displays a dialog that allows you to manage the timezone. NetBackup Console can execute in a different timezone than the timezone of the server on which it was initiated. See the <i>VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I</i> for more information.</p> <p><b>Export</b> - Saves configuration information or data about the selected device monitor to a file.</p> <p><b>Page Setup</b> - Displays a setup dialog for printing.</p> <p><b>Print Preview</b> - Previews the print image.</p> <p><b>Print</b> - Prints the contents of the volumes pane.</p> <p><b>Close Window</b> - Closes the current window.</p> <p><b>Exit</b> - Closes all open windows.</p>
<b>Edit</b>	<p><b>Change</b> - Displays a dialog for changing the configuration of the selected items.</p> <p><b>Delete</b> - Deletes selected items from the configuration.</p> <p><b>Find</b> - Command for finding items in the display lists.</p>
<b>View</b>	<p>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 121.</p>

---



## Media Management Menus and Commands (continued)

Menu	Commands
<b>Actions</b>	<p><b>New</b> - Displays a dialog for adding volumes or volume pools to a configuration.</p> <p><b>Change Volume Group</b> - Displays a dialog for changing the volume group for selected volumes.</p> <p><b>Move</b> - Displays a dialog for moving volumes.</p> <p><b>Rescan/Update Barcodes</b> - Rescans the barcodes in the selected robotic library and updates the barcodes for the selected volumes, as necessary.</p> <p><b>Eject Volumes From Robot</b> - Ejects selected single or multiple volumes to the robot's media access port.</p> <p><b>Label</b> - Displays a dialog for labeling unassigned media.</p> <p><b>Long Erase</b> - Displays a dialog to perform a full erase of unassigned media.</p> <p><b>Quick Erase</b> - Displays a dialog to perform a short erase of unassigned media.</p> <p><b>Inventory Robot</b> - 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.</p> <p><b>Stop/Restart Media Manager Device Daemon</b> - Controls the Media Manager device daemon.</p>
<b>Help</b>	<p><b>Help Topics</b> - Provides online help information for the NetBackup Console.</p> <p><b>Troubleshooter</b> - Helps you to debug errors.</p> <p><b>License Keys</b> - Provides information about your active and registered license keys.</p> <p><b>Current NBAC User</b> - Provides NetBackup Access Control information for the current user. Gives the permissions for the user that you are currently logged in as.</p> <p><b>About NetBackup Administration Console</b> - Displays program information, version number, and copyright information.</p>

## Toolbars

The toolbar buttons of the Media window provide shortcuts for commands that are on the menus. Also see "Customizing the Window" on page 121.

### ▼ To show or hide the toolbar buttons

1. In the NetBackup Administration Console, select **Media and Device Management > Media**.
2. Select **View > Show Toolbar**.



## Tree Pane

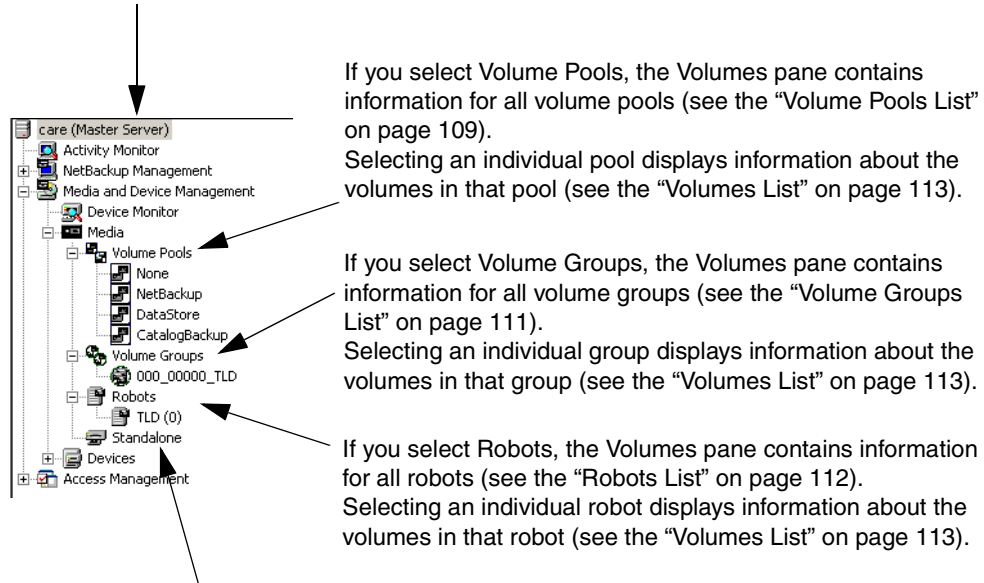
The tree pane for **Media** contains entries for **Volume Pools**, **Volume Groups**, **Robots**, and **Standalone**.

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

If there are no volumes configured in the EMM 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 (see the "Volumes List" on page 113).

*The following point applies to NetBackup Enterprise Server.*

You can view or configure volumes on another master or media server. See "Administering Media on Other Servers" on page 122 for more information.

## Volumes Pane

This pane lists the volumes in the EMM database.

### ▼ 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 > Column 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 109
- ◆ “Volume Groups List” on page 111
- ◆ “Robots List” on page 112
- ◆ “Volumes List” on page 113

## 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"><li>◆ None is the default pool for users of applications, other than NetBackup and Storage Migrator.</li><li>◆ NetBackup is the default pool name for NetBackup.</li><li>◆ DataStore is the default pool name for DataStore.</li><li>◆ CatalogBackup is the default pool name for volume pools used for storing NetBackup hot, online catalog backups of policy type NBU-Catalog.</li><li>◆ HSM is the default pool name for VERITAS Storage Migrator.</li><li>◆ RemoteStorage-media_density is the default pool name created by Data Lifecycle Manager.</li><li>◆ WORMxxxx where xxxx are any additional valid media manager characters used to identify the pool. When the first four characters of a volume pool name are WORM (upper-case letters), Media Manager handles media in the pool as WORM media. See “Using WORM Media” on page 141 for more information about using WORM volume pools.</li></ul>
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"><li>◆ 0 is the None (default) pool.</li><li>◆ 1 is the NetBackup pool.</li></ul> <p>The DataStore pool and CatalogBackup pool are assigned the next available pool number.</p>
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.

## Volume Pools List (continued)

Column	Description
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.
CatalogBackup	Contains Yes, if the volume pool is a CatalogBackup volume pool. Otherwise, contains No.

## 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.
Robot Number	Number of the robot that contains this volume group. If the robot type is NONE, this column is blank.
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 is blank.



## Volume Groups List (continued)

Column	Description
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 309 for a list of supported robot types.	
Robot Number	Number of the robot.	
Robotic Path	Contains the path of the robot or is blank for remote robots.	
NDMP Host	Contains the name of the NDMP control host.	Requires NDMP license.
Enabled	Contains Yes if the path to the robot is enabled. Contains No if the path is not enabled.	
Port	The SCSI port number of the robot. This column may be blank if there is a changer path configured for the robot.	Applies only to NetBackup Windows servers.
Bus	The SCSI bus number of the robot.	Applies only to NetBackup Windows servers.





## Robots List (continued)

Column	Description	Note
Target	The SCSI target number (or SCSI ID) of the robot.	Applies only to NetBackup Windows servers.
LUN	The logical unit number of the robot.	Applies only to NetBackup Windows servers.
Serial Number	The serial number of the robot.	
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.	



## Volumes List (continued)

Column	Description	Note
Media Type	Media type of the volume. See “Media Manager Media Types” on page 310 for a list of the supported media types.	
Robot Type	Type of robot that contains this volume. See “Media Manager Robot Types” on page 309 for a list of supported robot types. NONE in this column means a standalone volume.	
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 is blank.	
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 tracks the slot information. This column is also blank for standalone volumes.	
Volume Group	Name of the volume group for this volume. See “Volume Groups List” on page 111 for more information.	



## Volumes List (continued)

Column	Description	Note
Volume Pool	<p>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 109 for more information.</p> <p>None is the default pool name for users of applications. The following volume pool names are reserved:</p> <ul style="list-style-type: none"> <li>None is the default pool for users of applications.</li> <li>NetBackup is the default pool name for NetBackup.</li> <li>DataStore is the default pool name for DataStore.</li> <li>CatalogBackup is the default pool name for volume pools used for storing NetBackup hot, online catalog backups of policy type NBU-Catalog.</li> <li>HSM is the default pool name for VERITAS Storage Migrator.</li> <li>RemoteStorage-<i>media_density</i> is the default pool name created by Data Lifecycle Manager.</li> <li>WORMxxxx where xxxx are any additional valid media manager characters used to identify the pool. When the first four characters of a volume pool name are WORM (upper-case letters), Media Manager handles media in the pool as WORM media. See “Using WORM Media” on page 141 for more information about using WORM volume pools.</li> </ul>	
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
Application	<p>Application applies only to volumes that are assigned to NetBackup, Storage Migrator, or Data Lifecycle Manager. 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"><li>♦ 0 - NetBackup The volume is assigned to NetBackup regular backups.</li><li>♦ 1 - Catalog The volume is assigned to NetBackup catalog (database) backups.</li><li>♦ 2 - Storage Migrator The volume is assigned to Storage Migrator for UNIX.</li><li>♦ 3 - Data Lifecycle The volume is assigned to Data Lifecycle Manager.</li></ul>	
Side	<p>Optical platter side.</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. For any other media type, this column is blank.</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 is blank. 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
Volume Expiration	Indicates the age of the volume. If the volume 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.	
	<b>Note</b> This is the expiration date for the media itself, not the expiration date of any images stored on the media.	
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 <b>Edit &gt; Change</b> .	
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.



## Volumes List (continued)

Column	Description	Note
Vault Container ID	Contains the ID of the container where this volume is stored.	Applies only to the NetBackup Vault option.
Data Expiration	Date when the backups on the volume expire.	
Last Written	Last time the volume was used for backups.	
Last Read	Last time a restore was done from this volume.	
Kilobytes	Total number of kilobytes on this volume.	
Images	Total number of backups on the volume.	
Valid Images	Number of nonexpired backups on the volume. For example, if the volume has 50 backups but only 10 are valid, then the other 40 have expired. If the volume has any multiplexed backups, this field contains MPX	
Retention Period	How long the backups will be considered valid.	
Number of Restores	Number of times this volume has been used for restores.	
Conflicts	Conflicts can be detected when NetBackup back-level servers are updated to NetBackup 6.0. The messages that commonly appear here are the following:  <b>Media ID:</b> More than one volume sharing an identical media ID.  <b>Barcode:</b> More than one volume sharing an identical barcode.  <b>Residence:</b> More than one volume sharing an identical residence in a robotic library.  <b>RSM GUID:</b> More than one volume sharing an identical RSM GUID.  <b>ADAMM GUID:</b> More than one volume sharing an identical ADAMM GUID.	



## Volumes List (continued)

Column	Description	Note
Origin Host	Original volume database host from which the volumes were imported.	
Media Server	Server where the volumes reside.	
	It is possible to have more than one if the master server has media servers and ALL was selected for the server.	Applies only to NetBackup Enterprise Server.
Media Status	<p>The messages that commonly appear here are the following:</p> <p><b>Active:</b> The volume is currently in use.</p> <p><b>Frozen:</b> The volume is unavailable for future backups. A frozen volume never expires, even after the retention period ends for all backups on the media. This means that the media ID is never deleted from the NetBackup media catalog and remains assigned to NetBackup. (The <code>bpmedia</code> command can also be used to manually freeze or unfreeze volumes.)</p> <p>A frozen volume is available for restores. If the backups have expired, the backups first require importing.</p> <p><b>Suspended:</b> The volume cannot be used for further backups until retention periods for all backups on it have expired. At that time, the suspended volume is deleted from the NetBackup media catalog and unassigned from NetBackup. (The <code>bpmedia</code> command can also be used to manually suspend or unsuspend volumes.)</p> <p>A suspended volume is available for restores. If the backups have expired, the backups first require importing.</p> <p><b>Full:</b> The volume is full and no more backups are written to it. NetBackup sets FULL status if it encounters an end of media (EOM) during a backup.</p> <p>A full volume is unavailable for future backups until the retention period expires for all backups that are on it. At that time, the volume is deleted from the NetBackup media catalog and unassigned from NetBackup.</p> <p><b>Multi-Retlev:</b> (Multiple Retention Level) The volume contains backups of more than one retention level.</p>	



## Volumes List (continued)

Column	Description	Note
	<b>Imported:</b> The backup was imported to this server. The volume cannot be used for further backups until retention periods for all backups on it have expired. At that time, the imported volume is deleted from the NetBackup media catalog and unassigned from NetBackup. An imported volume is available for restores. If the backups have expired, the backups first require importing.	
	<b>MPX_MEDIA:</b> The media contains multiplexed images.	
	<b>WORM:</b> The volume is a WORM volume. See “Using WORM Media” on page 141 for more information about WORM volumes.	
	<b>BE:</b> The volume contains Backup Exec images.	

## Messages Pane

The **Messages** pane appears in the lower right below the Volumes pane, and is used to display messages about a task that is running as a background process. This pane is displayed only if there is an informative message or error message for the task. If the task completes normally, the pane is not displayed.

## Shortcut Menus and Commands

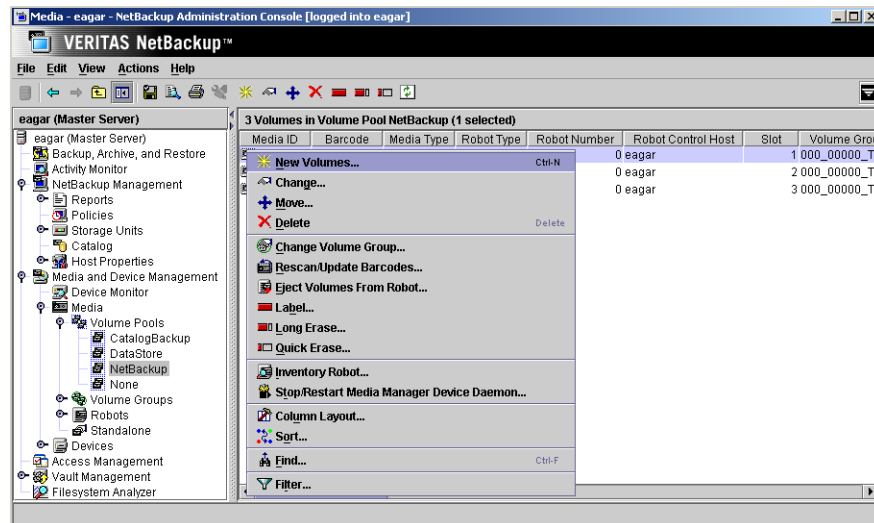
Shortcut menus work in the context of what object is currently selected in a pane. Shortcut commands are also available on the menus or toolbars.

### ▼ To display a shortcut menu

- ❖ Right click on any object or section in the pane



## Shortcut Menu



## Customizing the Window

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

See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* for more details.

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

Select **View > Column Layout**.



## Administering Media on Other Servers

For recommended practices, see “Enterprise Media Manager Domain Management” on page 305.

### 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 is shown at the top of the tree pane, for example, spain (Master Server)

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

You cannot access a NetBackup Enterprise Server from a NetBackup Server.

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

1. In the NetBackup Administration Console, select the server name shown at the top of the tree.
2. Select **File > Change Server**.
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.

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 server. This information is obtained from the EMM database for the server.

You can specify a different server when logging into NetBackup. The name of the UNIX host that you specify in the Login box, when starting the NetBackup Administration interface, must be in the NetBackup `bp.conf` file on the remote UNIX host where you want to monitor devices.

If you encounter problems or for more information on managing media on other servers, see the following topics:

- ◆ “Remote Administration of Other UNIX Servers” on page 42.



- ◆ “Media Manager Security” on page 44.

## 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 EMM database. The attributes in the 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.

---

**Note** When you add a new volume, there is no default volume expiration date.

---

See the following topics:

- ◆ “Methods Available for Adding Volumes” on page 123
- ◆ “Adding Volumes Using a Robot Inventory Update” on page 125
- ◆ “Adding Volumes Using the Actions Menu” on page 126
- ◆ “Dialog Entries for New Volumes” on page 128

## Methods Available for Adding Volumes

The methods available to add volumes depend on how the volume will be used. See the following related topics:

- ◆ “Robotic Volumes (Volumes Located in a Robot)” on page 123
- ◆ “Standalone Volumes (Volumes To Be Used in Standalone Drives)” on page 124
- ◆ “NetBackup Catalog Backup Volumes” on page 124
- ◆ “Notes on Labeling NetBackup Volumes” on page 124

### 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 134 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 125.

- ◆ To add volumes using the menu, see “Adding Volumes Using the Actions Menu” on page 126.



## 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 134 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` option of the `nbemmcmd` command can turn off NetBackup’s automatic use of standalone volumes. See the *VERITAS NetBackup Commands for UNIX and Linux* or the *VERITAS NetBackup Commands for Windows* 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 126. See the *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for Windows* 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 first add them in Media Manager as with any other volumes. You can use any of the methods described in “Methods Available for Adding Volumes” on page 123 to add the volumes. After adding volumes, use the NetBackup Catalog Backup wizard to configure a volume for use with catalogs.

## Notes on Labeling NetBackup Volumes

Labeling volumes is controlled by the application. See the *VERITAS NetBackup System Administrator’s Guide for UNIX and Linux, Volume I*, the *VERITAS NetBackup System Administrator’s Guide for Windows, Volume I*, or the *VERITAS Storage Migrator System Administrator’s Guide for UNIX* 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 207).
- ◆ An optical disk platter must be formatted, have an external media ID, and a volume label before you can use it with Media Manager. Use the **Media** portion of the NetBackup Administration Console, `vmadm`, or `vmadm` with the `tpformat` command to add an optical disk volume. When using **Media** or `vmadm`, you can choose the label option, making it unnecessary to use `tpformat` from the command line.

See “Label Optical Media” on page 134, “Using the Media Management Utility (`vmadm`)” on page 419, or `tpformat (1M)` in the *VERITAS NetBackup Commands for UNIX and Linux* for more information.

## Adding Volumes Using a Robot Inventory Update

A robot inventory update will generate 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 184 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, select **Media and Device Management > Media > Robots**.
3. Select the robotic library where you inserted the volume.
4. Select **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

VERITAS recommends using the Volume Configuration wizard or a robot inventory to add volumes. See “Methods Available for Adding Volumes” on page 123.

### ▼ 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, select **Media and Device Management > Media**.

3. Select **Actions > New > Volumes**.

4. Specify the properties for the volumes as explained in “Dialog Entries for New Volumes” on page 128.

**Note** Be careful when specifying properties, since you cannot change some properties (such as the media ID or media type) later. To change these properties, you need to delete the volumes and add them again.

5. Click **OK** to execute the add.

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 EMM database, using the specified media ID.
- ◆ Reads the barcode of each new volume.
- ◆ Adds the barcodes as attributes in the EMM 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

The following topics explain the dialog properties that you specify when adding new volumes.

- ◆ “Media Type” on page 128
- ◆ “Volume Is In a Robotic Library” on page 128
- ◆ “Select Robot Section of the Dialog” on page 129
- ◆ “Device Host” on page 129
- ◆ “Robot” on page 129
- ◆ “Number of Volumes (or Number of platters)” on page 129
- ◆ “Media ID Naming Style” on page 130
- ◆ “Media ID or First Media ID” on page 130
- ◆ “Partner ID” on page 131
- ◆ “Media Description” on page 131
- ◆ “First Slot Number” on page 131
- ◆ “Maximum Mounts or Maximum Cleanings” on page 132
- ◆ “Volume Group” on page 132
- ◆ “Volume Pool” on page 134
- ◆ “Label Optical Media” on page 134

### 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.

### Volume Is In a Robotic Library

#### ▼ To specify that the volume is in a robot

- ❖ Select **Volume is in a robotic library**.





The **Select robot** section of the dialog is then enabled (see the next topic).

## Select Robot Section of the Dialog

In this section you specify the device host and the robot.

### Device Host

Specifies the name of the device host where the robot is defined.

*The following procedure applies only to NetBackup Enterprise Server.*

#### ▼ To select a robot on another device host

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

### 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 robots on the selected host that can contain volumes of the selected media type.

## Number of Volumes (or Number of platters)

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	<b>Media ID</b>	"Media ID or First Media ID" on page 130
More than one volume	<b>First Media ID</b>	"Media ID or First Media ID" on page 130
	<b>Media ID naming style</b>	"Media ID Naming Style" on page 130



Depending on the number of platters you are adding, you must also specify additional information as shown in the following table:

<b>If You Are Adding</b>	<b>You Must Also Specify</b>	<b>See</b>
One platter	<b>Media ID</b> <b>Partner ID</b>	"Media ID or First Media ID" on page 130 "Partner ID" on page 131
More than one platter	<b>First Media ID</b> <b>Media ID naming style</b>	"Media ID or First Media ID" on page 130 "Media ID Naming Style" on page 130

▼ **To specify the number of volumes (or platters)**

- ❖ Click an arrow and select a number for the volumes.

If you are adding optical volumes, specify the number of platters.

## **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.

If you are adding optical volumes, there are style choices for naming platters.

## **Media ID or First Media ID**

Media IDs can be from 1 to 6 characters in length. See "Allowable Media Manager Characters" on page 308.

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.

**Partner ID**

If you are adding one optical volume, you can specify a partner ID. This ID is the media ID of the volume on the other side of the optical platter.

**▼ To specify a partner ID**

- ❖ Enter a 1 to 6-character ID for the partner ID.

**Media Description**

Enter a 1 to 25 ASCII character description of the media that you are adding. See “Allowable Media Manager Characters” on page 308.

**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 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. Specifying 0 indicates unlimited mounts. If you enter a value larger than 99999, it may be displayed by Media Manager as 0. For example, the output of the `vmrule` command will display 0 for values larger than 99999. However, Media Manager will correctly interpret the actual value.

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 339 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 344 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.

---

If You Leave the Volume Group Blank for	Media Manager
Robotic volumes	Generates a name using the robot number and type. For example, if the robot is a TL8 and has a robot number of 50, the group name will be 000_00050_TL8.

### 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.  
See “Allowable Media Manager Characters” on page 308.

#### ▼ 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.
CatalogBackup	For storing NetBackup hot, online catalog backups of policy type NBU-Catalog.
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 135.)

## Label Optical Media

Before using optical volumes for backups, they must be formatted and labeled. The media will be labeled when it is added, but it is not formatted. If you need to format your optical media, refer to the `tpformat` command in the *VERITAS NetBackup Commands for UNIX and Linux*.

### ▼ To label optical media

- ❖ Click the arrow and select one of the three choices for how you want the media labeled (**Yes, but do not overwrite old labels** - **Yes, overwrite as needed** - **No**).

Click the arrow to select from the list of available choices. The default choice does not overwrite any old labels.

## 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 Enterprise Media Manager (EMM) database.

After running this wizard to configure media, each media will have a unique media ID in the EMM database that is used in Media Manager and NetBackup to track 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 135).
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, select **Media and Device Management > Configure Volumes**.

## 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 109):

- ◆ NetBackup, created by Media Manager, for NetBackup use.
- ◆ DataStore, created by NetBackup, for DataStore use.
- ◆ CatalogBackup, created by NetBackup, for NetBackup catalog backups.
- ◆ On UNIX hosts, a pool is also created for VERITAS Storage Migrator volumes.

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.

If the volume pool will contain WORM media, see “Using WORM Volume Pools to Manage WORM Media” on page 143 for more information.

For background information, see “Volume Pools” on page 344 and “Scratch Volume Pools” on page 347.

The following topics explain volume pool configuration:

- ◆ “Adding a New Volume Pool or Scratch Volume Pool” on page 136
- ◆ “Changing the Attributes of a Volume Pool” on page 139
- ◆ “Changing the Volume Pool Assignment for a Volume” on page 167
- ◆ “Deleting a Volume Pool” on page 141

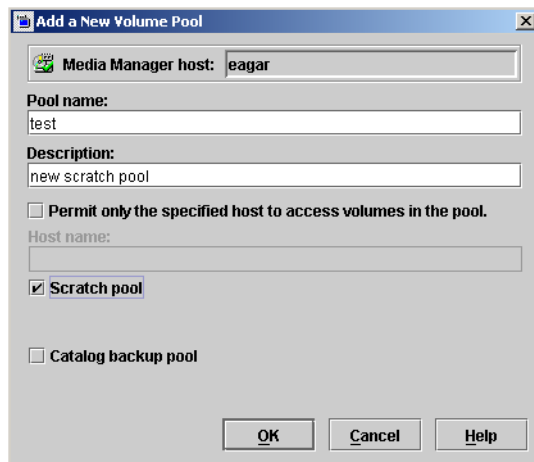
## Adding a New Volume Pool or Scratch Volume Pool

### ▼ To add a volume pool

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



To add a scratch volume pool, see the following topic “Adding a Scratch Volume Pool” on page 138.



3. In the **Pool name** text box, enter a name for the new volume pool.  
Volume pool names are case sensitive. The name must be 20 characters or less, and cannot contain any spaces or special characters. See “Allowable Media Manager Characters” on page 308.
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.

---



6. Select the **Catalog backup pool** check box if you will use this volume pool for hot, online backups of the NetBackup catalog. This check box creates a dedicated catalog backup pool to be used for NBU-Catalog policies. A dedicated catalog volume pool facilitates quicker catalog restore times. Multiple CatalogBackup volume pools are permitted.

See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* for more information about backing up your NetBackup catalog data.

## 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
<b>Pool Name</b>	Enter any pool name, except the following names: NetBackup, DataStore, CatalogBackup, or None. It is recommended to use a descriptive name, like scratchpool, as the pool name.	
<b>Description</b>	It is recommended to include "scratch pool" in the description.	
<b>Permit only the specified host to access volumes in the pool</b>	When creating a scratch volume pool, do not select this check box to specify a specific host. Use the default value, ANYHOST.	Applies only to NetBackup Enterprise Server.
<b>Scratch Pool</b>	Select this check box.	

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

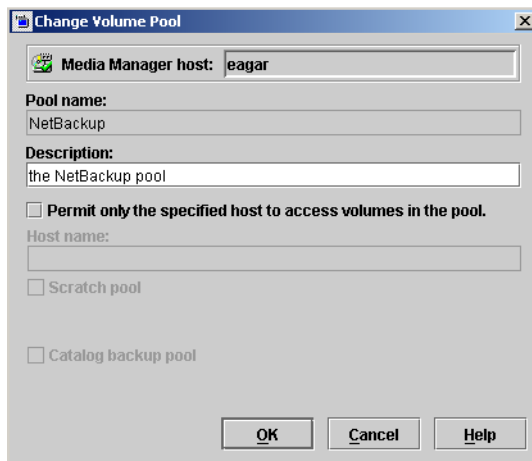
Follow the steps for adding other volumes to pools (see "Adding New Volumes" on page 123). In this case, select the pool name of the scratch pool you created as the volume pool.



## Changing the Attributes of a Volume Pool

### ▼ To change a volume pool

1. In the NetBackup Administration Console, select **Media and Device Management > Media > Volume Pools**.
2. Select a pool from the pools shown under **Volume Pools** in the tree pane.
3. Select **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 140. You cannot change the NetBackup or DataStore pools to be scratch volume pools.
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.

---

6. To change the pool to a CatalogBackup pool, select the **Catalog backup pool** check box. Selecting this check box creates a dedicated catalog backup pool to be used for NBU-Catalog policies. A dedicated catalog volume pool facilitates quicker catalog restore times. Multiple CatalogBackup volume pools are permitted.

See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* for more information about backing up your NetBackup catalog data.

## Changing a Volume Pool To be a Scratch Volume Pool

Also see “Adding a Scratch Volume Pool” on page 138.

### ▼ 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	When creating a scratch volume pool, do not select this check box to specify a specific host. Use the default value, ANYHOST.	Applies only to NetBackup Enterprise Server.
Scratch Pool	Select this check box. You cannot change the NetBackup or DataStore pools to be scratch volume pools.	

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 123). In this case, select the name of the scratch pool as the volume pool.



## Deleting a Volume Pool

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

- ◆ A volume pool that contains volumes
- ◆ The NetBackup volume pool
- ◆ The None volume pool
- ◆ The default CatalogBackup 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, select **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. Select **Edit > Delete**.  
Answer the confirmation dialog.

## Using WORM Media

WORM (Write-Once-Read-Many) media is used to protect key data from unwanted modification or tampering, or to meet compliance regulations.

The NetBackup QIC/WORM tape format is used for WORM media. This format allows appending images to WORM tape, as can be done with standard tape. See “QIC/WORM Tape Format” on page 376.

A SCSI pass-thru path is required to use WORM tape drives. NetBackup software queries the drive to verify it is a WORM-capable drive and that the media in the drive is WORM media. These queries are done using SCSI commands. SCSI pass-thru paths are provided on the server platforms supported by NetBackup. Setting up SCSI pass-thru paths may require special operating system configuration changes. See the appropriate chapter of the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for your particular server platform.

The ability to use WORM tape with NetBackup is available by default. To disable this capability see “Disabling WORM Tape Support” on page 145.



Tape error recovery is disabled when using WORM media. NetBackup has resume logic which will typically attempt to resume a job that has been interrupted (for example, an interruption on the fibre channel). When using WORM media with NetBackup, the job will fail instead of being resumed. NetBackup will then retry the failed job. The use of checkpoint/restart for backups is recommended because files backed up prior to the last checkpoint will not need to be backed up again.

`bplabel` will label only LTO-3 WORM tapes. All other WORM media cannot be labeled, as this label cannot be overwritten when the media is used.

## Supported Drives

The following table lists the drives that have been tested with NetBackup and WORM media. All of these vendors, except Quantum, require the use of special WORM media. The table also shows the firmware required and the supported operating systems.

Quantum allows standard tape media to be converted to WORM media by NetBackup. Use of Quantum drives for WORM media requires an `st.conf` entry on Solaris. See the Sun4/SPARC chapter of the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for information on configuring nonstandard tape drives, and editing the `st.conf` file.

Vendor Drive	Supported Interface	Minimum Firmware Level Required	Supported OS Platforms
StorageTek 9840A	SCSI and FC	R1.34.158	Solaris, Windows, AIX, HP-UX, and Linux
StorageTek 9840B	SCSI and FC	R1.34.358	Solaris, Windows, AIX, HP-UX, and Linux
StorageTek 9840C	FC	R1.34.358	Solaris, Windows, AIX, HP-UX, and Linux
StorageTek 9940B	FC	R1.32.427	Solaris, Windows, AIX, HP-UX, and Linux
Sony S-AIT	SCSI and FC	0200	Solaris, Windows, HP-UX, and Linux
Sony AIT-2 (SDX-500V)	SCSI	0101	Solaris, Windows, HP-UX, and Linux

Vendor Drive	Supported Interface	Minimum Firmware Level Required	Supported OS Platforms
Sony AIT-2 (SDX-500C)	SCSI	0200	Solaris, Windows, HP-UX, and Linux
Sony AIT-3 (SDX-700V)	SCSI	0100	Solaris, Windows, HP-UX, and Linux
Sony AIT-3 (SDX-700C)	SCSI	0200	Solaris, Windows, HP-UX, and Linux
IBM 3592J	FC	D3I0_4B5	Solaris, Windows, AIX, HP-UX, and Linux
Quantum SDLT 600	SCSI	v30	Windows, AIX, HP-UX, and Linux 2.4.15 and above (including 2.6)
HP LTO-3	SCSI	G27D	Windows, HP-UX, and Linux 2.4.15 and above (including 2.6)
	FC	L21D	Solaris, Windows, HP-UX, and Linux 2.4.15 and above (including 2.6)

## Managing Your WORM Media in Media Manager

There are two methods for using WORM tape with NetBackup to ensure that data that is intended for WORM media is written on WORM media.

- ◆ See “Using WORM Volume Pools to Manage WORM Media” on page 143
- ◆ See “Using Unique Drive and Media Types to Manage WORM Media” on page 145

### Using WORM Volume Pools to Manage WORM Media

You can use volume pools that are dedicated for your WORM media. This method allows a WORM-capable tape drive to back up and restore standard and WORM media.

Create a new volume pool and specify WORM (upper-case letters) as the first four characters of the pool name. See “Configuring Volume Pools” on page 135.



The first four characters of the volume pool name are compared against the characters WORM to determine if it is a volume pool containing WORM media. This check on the volume pool name is disabled if the file `/usr/opensv/netbackup/db/config/DISABLE_WORM_POOLCHECK` is present on the media server.

Note the following cases:

- ◆ If the drive contains WORM media and the media is in a WORM volume pool, the media will be written as WORM.
- ◆ If the drive contains WORM media and the media is not in a WORM volume pool, the media will be frozen.
- ◆ If the drive contains standard media and the media is in a WORM volume pool, the media will be frozen. The media will be used if it is Quantum media which has never been used or has had all of its NetBackup images expired.

### Using A Scratch Pool

For all WORM-capable drives listed in the table (except the Quantum drive), the scratch pool must only contain one type of media. It is a good practice to put the most commonly used media in the scratch pool. For example, if most NetBackup jobs use standard media, put standard media in the scratch pool.

Care must be taken to ensure that the volume pool does not run out of the appropriate media type (WORM or standard) to complete requested backup jobs. For example, if a WORM volume pool runs out of media, and the scratch pool contains standard media, then standard media will be moved from the scratch pool into the WORM pool. The standard media will be loaded into a WORM-capable drive, and will then be frozen. This process is repeated until all standard media in the scratch pool has been frozen.

The opposite case is also true. If a standard volume pool runs out of media and the scratch pool contains WORM media, standard backups may not complete due to a lack of available media.

### Using the Quantum Drive

When using the Quantum drive, only one kind of media exists which can be used as standard media or WORM media.

If a WORM volume pool runs out of media, media is moved from the scratch volume pool into the WORM pool. NetBackup determines whether the media is configured as standard or WORM media. If it is standard media, NetBackup will read the tape label, verify the media is unused or all images are expired, and verify that the media is not currently assigned to a server. After verification, NetBackup will configure the media as WORM media and continue with the NetBackup job.



## Using Unique Drive and Media Types to Manage WORM Media

You can assign a different drive and media type to all WORM drives and media. For example, standard drives and media could be configured as HCART and WORM-capable drives and media could be configured as HCART2.

This method allows both types of media to be put in the scratch pool since NetBackup will select the proper media type for the drive type.

A limitation to using this method is that each drive is limited to backup and restores with a specific type of media, so optimal usage of the drives will not likely be achieved. So, even though no WORM backups are in process, the WORM-capable drives will not be able to be used for backups with standard media.

If you are not using WORM volume pools to manage WORM media, you should disable the WORM volume pool check. To do this ensure that the file `/usr/opensv/netbackup/db/config/DISABLE_WORM_POOLCHECK` is present.

### Using the Quantum drive

Since Quantum drives use only a single media type, there is no reason to use this method for managing your WORM media.

## Disabling WORM Tape Support

The ability to use WORM tape with NetBackup is available by default. To disable this capability, a special file is required on each media server (`/usr/opensv/netbackup/db/config/DISABLE_WORM_TAPE`).

The existence of this file removes the requirement to have pass-thru paths to all tape drives. If the file exists, NetBackup will not check for WORM media and will write to WORM media with the standard tape format. This will cause append operations to WORM media to fail.

## WORM Tape Limitations

The following are the current limitations when using WORM tape.

- ◆ Third-Party Copy backups are not supported with WORM media.
- ◆ Resume logic is not supported with WORM tape. Backups will fail and be retried, or restarted from the last checkpoint, if checkpoint/restart is being used.
- ◆ WORM tape is not supported with NetWare media servers.



## 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 related topics for more information:

- ◆ “Performing a Volume Configuration Update Using Robot Inventory” on page 146
- ◆ “Using the Eject Volumes From Robot Command” on page 147
- ◆ “Media Ejection Timeout Periods” on page 147

## 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** *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 184 for complete instructions.

## Using the Eject Volumes From Robot Command

Select **Actions > Eject Volumes From Robot** to eject one or more selected volumes from a robotic library.

You cannot eject volumes that reside in multiple robots.

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 147.

See “Ejecting Volumes From Robots (Actions Menu Command)” on page 148 for complete instructions.

## 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 (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.

---

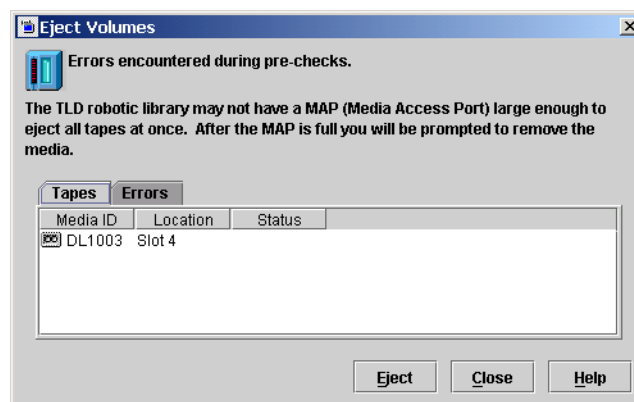


## Ejecting Volumes From Robots (Actions Menu Command)

You can eject single or multiple volumes.

### ▼ To eject volumes

1. In the NetBackup Administration Console, select **Media and Device Management > Media**.
2. In the volumes pane, select one or more volumes that you want to eject.
3. Select **Actions > Eject Volumes From Robot**.



4. In normal cases after the pre-checks for the eject are complete, the **Tapes** 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.

5. *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.

6. 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.

## Rescanning and Updating Barcodes for a Robot

Use the **Rescan/Update Barcodes** command to check the barcodes attached to volumes in robotic libraries, and update the EMM 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 311 lists the robots that support barcodes.

See the following related topics:

- ◆ “When to Use Rescan/Update” on page 149
- ◆ “When Not to Use Rescan/Update” on page 149
- ◆ “Rescanning/Updating Barcodes” on page 150

### When to Use Rescan/Update

Use **Rescan/Update Barcodes** only to fill in barcodes that are missing from the EMM 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 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 184.
- ◆ Physically move the volume into the correct slot to agree with the EMM database.



To obtain an inventory of the robotic library without updating the barcode information in the database, select **Show contents** in the Robot Inventory dialog. See “Showing the Contents of a Robot” on page 179 for more information.

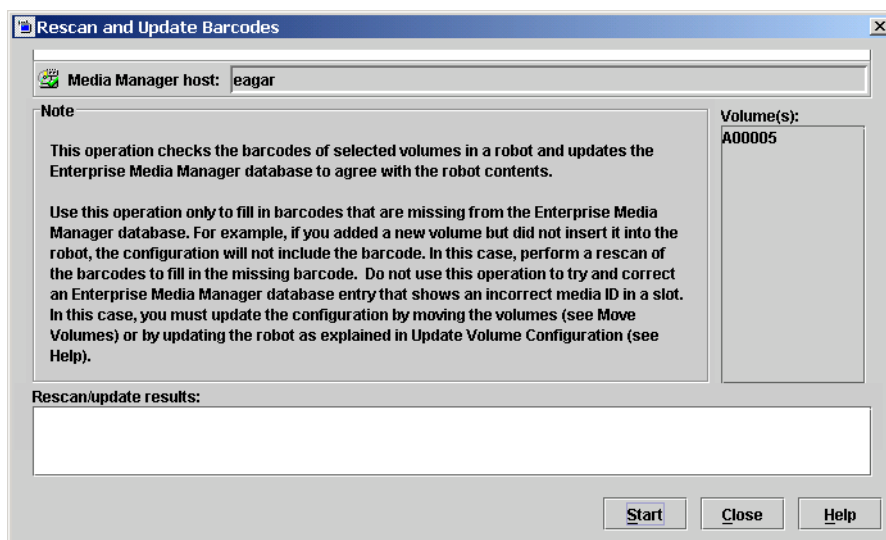
## Rescanning/Updating Barcodes

### ▼ To check barcodes and update the EMM database

1. In the NetBackup Administration Console, select **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. Select **Actions > Rescan/Update Barcodes**.

A dialog appears listing the volumes you selected for the rescan operation.

Click **Start** to continue or **Close** to quit. If you select **Start**, the results of the update are displayed in the output section of the dialog.



## 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 349.

You can move volumes using one of the following methods:

- ◆ “Moving Volumes Using the Robot Inventory Update Option” on page 151
- ◆ “Moving Volumes Using the Actions Menu” on page 151

### 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. Select **Actions > Inventory Robot** to update the EMM database to agree with the contents of the robot.

See “Updating the Volume Configuration for a Robot” on page 184 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 EMM database to show the correct barcode for the volume.

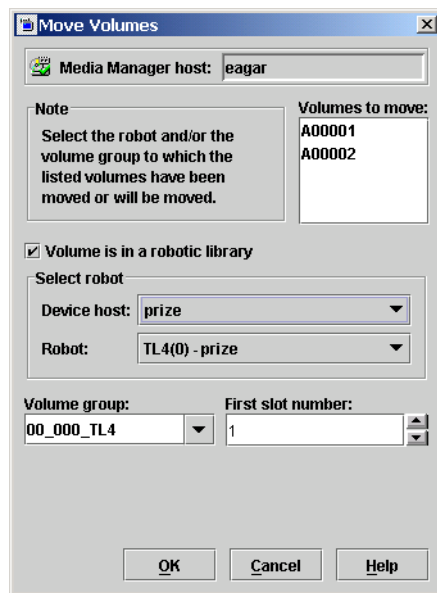
When moving volumes from one robotic library to another, you must move the volumes to standalone as an intermediate step and then to the new robotic library.

#### ▼ To move volumes using the Actions menu

1. Physically move the volumes to their new location.
2. In the NetBackup Administration Console, select **Media and Device Management > Media**.



3. In the volumes pane, select the volumes you want to move.
4. Select **Actions > Move**.



5. Specify the properties for the move as explained in “Dialog Entries for Move Volumes” on page 153.

---

**Note** If you are moving a single volume, the dialog entries are set to show the current location of the volume.

---

6. Click **OK** to execute the move.



## Dialog Entries for Move Volumes

The following topics explain the properties of the dialog:

- ◆ “Volumes to Move” on page 153
- ◆ “Volume Is In a Robotic Library” on page 153
- ◆ “Select Robot Section of the Dialog” on page 153
- ◆ “Device Host” on page 154
- ◆ “Robot” on page 154
- ◆ “Volume Group” on page 154
- ◆ “First Slot Number” on page 155

### 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.

### Volume Is In a Robotic Library

#### ▼ To inject a volume into a robotic library

- ❖ Select **Volume is in a robotic library**.

The **Select robot** section of the dialog is now available. Specify the robot (see “Robot” on page 154) and the slot number for the volume (see “First Slot Number” on page 155).

#### ▼ To eject a volume from a robot

- ❖ Clear **Volume is in a robotic library**

### Select Robot Section of the Dialog

If you are moving a single volume, the **Select robot** section initially shows the current location of the volume.



## Device Host

Specifies the name of the device host where the robot is defined.

*The following procedure applies only to NetBackup Enterprise Server.*

### ▼ To select a robot on another device host

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

## Robot

**Robot** specifies the robotic library where you are moving the volumes. You can specify a different robot.

### ▼ To specify a different robot

- ❖ Click the arrow and select from the list to specify the robot to which you are moving the volumes.

The list shows robots on the selected device host that can contain volumes of the selected media type.

## 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 TL8 and has a robot number of 50, the group name will be 000_00050_TL8.

---

### 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 tracks the slot locations for these robot types.

---

▼ **To specify the first slot number**

- ❖ Click an arrow and specify the number.

## **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 EMM 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 161.

See the following related topics for more information:

- ◆ “Deleting Volumes” on page 156
- ◆ “Deleting a Volume Group” on page 156

## Deleting Volumes

### ▼ To delete volumes

1. In the NetBackup Administration Console, select **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. Select **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, select **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.

The Time Assigned column is hidden by default. To display this column, see “Customizing the Window” on page 121.

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 161).

Use the procedure (“Deleting Volumes” on page 156) to delete individual volumes that are unassigned.

3. Select a volume group in the tree pane.
4. Select **Edit > Delete**.  
A dialog appears asking you to confirm the action.
5. Remove the deleted volumes from the storage device.

## 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 (see “Deassigning Volumes” on page 161).

---

**Caution** If you use this function, any data written on the media will no longer be available for a NetBackup restore or import.

---

### ▼ To label or relabel media

1. In the NetBackup Administration Console, select **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.



3. Select **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** For many types of drives it may not be possible to cancel a label or relabel job from the Activity Monitor.

---

## 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 (see “Deassigning Volumes” on page 161). 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.

---

See the following related topics:

- ◆ “SCSI Quick Erase” on page 159
- ◆ “SCSI Long Erase” on page 160
- ◆ “Erasing Media” on page 160

### 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.

---

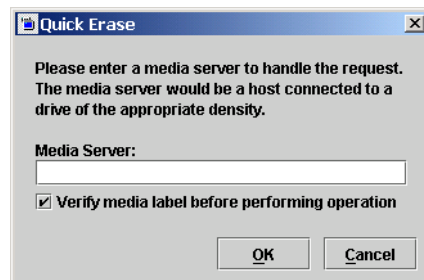
**Caution** A long erase is a time-consuming operation and can take as long as 2 to 3 hours. For example, it takes about 45 minutes to erase a 4mm tape on a standalone drive

---

## Erasing Media

### ▼ To erase media

1. In the NetBackup Administration Console, select **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.
3. For a short erase, select **Actions > Quick Erase**.  
For a long erase, select **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 **Application** column of the Volumes list (see “Volumes Pane” on page 109).

## 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 `/usr/opensv/netbackup/bin/admincmd` directory and has the following format:

```
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:

```
/usr/opensv/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 and typically held in the CatalogBackup volume pool.

To deassign these volumes (assuming they do not contain any important data), specify the CatalogBackup volume pool for catalog backups. The media is available to be reassigned or deleted, or its volume pool can be changed.

See the *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* 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 *VERITAS Storage Migrator System Administrator's Guide for UNIX*.

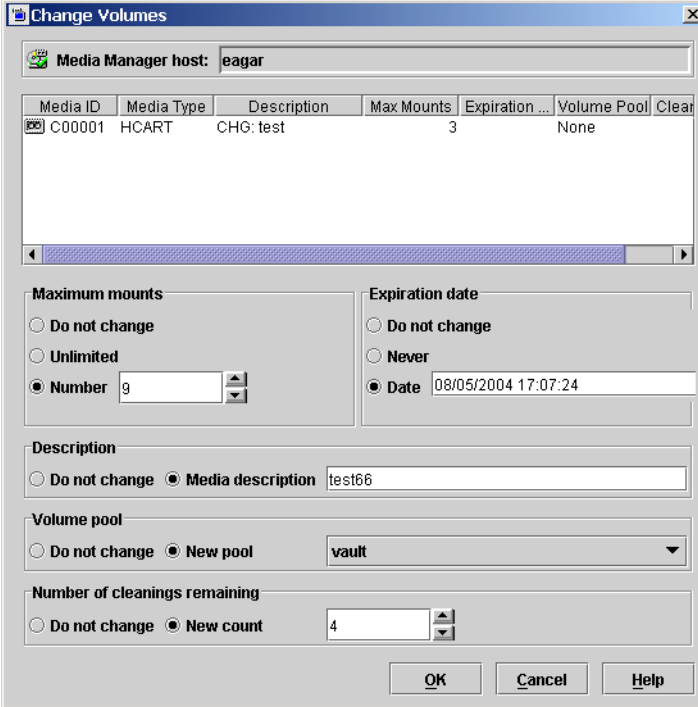
## Changing the Attributes for a Volume

### ▼ To change volume attributes

1. In the NetBackup Administration Console, select **Media and Device Management > Media**.
2. In the volumes pane, select a volume or volumes.
3. Select **Edit > Change**.



A dialog appears and shows the media ID and other attributes for each selected volume.



The "Change Volumes" dialog box is shown. It has a title bar with a close button. Below the title bar is a field for "Media Manager host:" with the value "eagar". Below that is a table with columns: Media ID, Media Type, Description, Max Mounts, Expiration ..., Volume Pool, and Clear. The table contains one row with the following values: C00001, HCART, CHG: test, 3, None, and a clear button. Below the table is a horizontal scrollbar. Below the scrollbar are several sections: "Maximum mounts" with radio buttons for "Do not change", "Unlimited", and "Number" (selected), and a spin box with the value 9; "Expiration date" with radio buttons for "Do not change", "Never", and "Date" (selected), and a date field showing "08/05/2004 17:07:24"; "Description" with radio buttons for "Do not change" and "Media description" (selected), and a text field with the value "test66"; "Volume pool" with radio buttons for "Do not change" and "New pool" (selected), and a dropdown menu showing "vault"; and "Number of cleanings remaining" with radio buttons for "Do not change" and "New count" (selected), and a spin box with the value 4. At the bottom are three buttons: "OK", "Cancel", and "Help".

Media ID	Media Type	Description	Max Mounts	Expiration ...	Volume Pool	Clear
C00001	HCART	CHG: test	3	None		

4. In the dialog, change the attributes for the volume as explained in "Dialog Entries for Change Volumes" on page 164.
5. Click **OK** to apply the changes to the selected volumes.

## Dialog Entries for Change Volumes

The following topics explain the properties of the dialog:

- ◆ "Maximum Mounts" on page 165
- ◆ "Expiration Date" on page 165
- ◆ "Description" on page 166
- ◆ "Volume Pool" on page 166
- ◆ "Number of Cleanings Remaining" on page 167

## 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 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.

Media descriptions can be from 1 to 25 characters in length. See “Allowable Media Manager Characters” on page 308.

▼ **To not make any changes to Description**

- ❖ Select **Do not change**.

▼ **To add a description**

1. Click **Media 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 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, select **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 161).

---

3. Select **Edit > Change**.



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

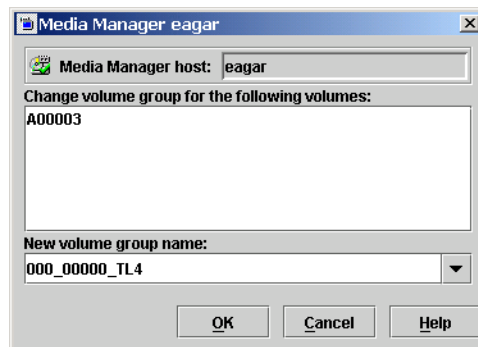
See “Changing the Attributes for a Volume” on page 163 for more information.

4. In the Volume Pool section, click **New Pool**.
5. Click the arrow to view a list of the available volume pools and select a volume pool from the list.
6. Click **OK**.

## Changing the Volume Group of a Volume

### ▼ To change the volume group

1. In the NetBackup Administration Console, select **Media and Device Management > Media**.
2. In the volume list, select the volumes that you want to change the volume group assignment for.
3. Select **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.



## Moving A Volume Group

In addition to moving individual volumes, you can move an entire volume group. This move can be one of the following:

- ◆ From a robotic library to standalone
- ◆ From standalone to a robotic library

### ▼ To move a volume group

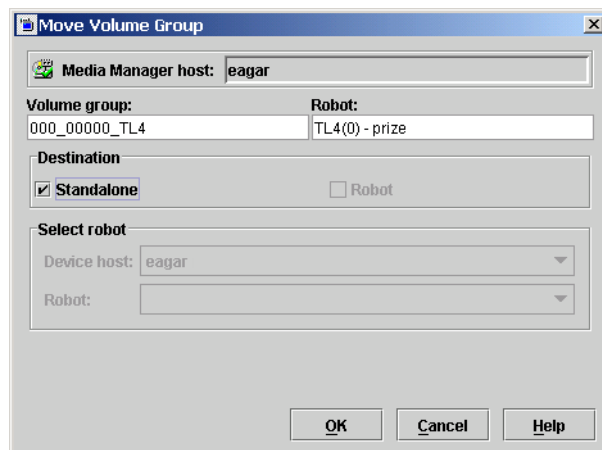
1. In the NetBackup Administration Console, select **Media and Device Management > Media**.

2. In the tree pane, select the volume group that you want to move.

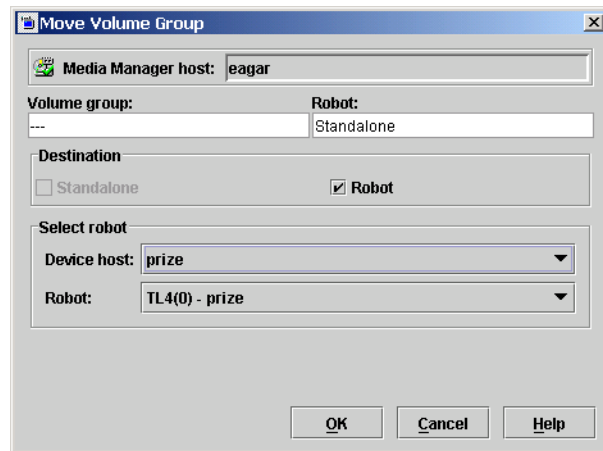
3. Select **Actions > Move**.

In the dialog that appears, the current attributes of the volume group you selected are displayed. These fields cannot be changed.

4. If you are moving the volume group from a robotic library to standalone, **Standalone** is pre-selected as the destination. For this type of move, fields that are not used cannot be selected.



5. If you are moving the volume group from standalone to a robotic library, **Robot** is pre-selected as the destination.



- a. *This step applies only to NetBackup Enterprise Server.*  
Select the device host that controls the robotic library, by clicking the arrow and selecting from the list of hosts shown.
  - b. Select the destination robotic library, by clicking the arrow and selecting from the list of robots.
6. Click **OK**.
  7. Physically move the volumes to their new location.

Moving a volume group in Media Manager changes only their residence information in the EMM database. The volumes must also be physically moved.

## 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 151).  
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 123.
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 155.
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 123.
4. Set a new Expiration Date for this volume. See “Changing the Attributes for a Volume” on page 163.
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 161.

### 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 151.
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 155.
5. Add a new volume entry, and physically add the volume to the storage device. See “Adding New Volumes” on page 123.
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:  
$$value = (\text{number of mounts that the manufacturer recommends}) - (\text{the value that you recorded in step 3})$$

This is necessary because the count will start from zero for the new volume entry.
7. Set the number of mounts to the value you recorded in step 3 by using the following command:  

```
/usr/opensv/volmgr/bin/vmchange -m media_id -n number_of_mounts
```
8. Set the expiration date to the value you recorded in step 3.





# Managing Media in Robots (Robot Inventory)

4

The operations used to manage media in robots described in this chapter are done using the Robot Inventory dialog (see “Accessing the Robot Inventory Dialog” on page 177).

See “Starting Media Management” on page 104 for an explanation of the NetBackup **Media** window that you use to initiate a robot inventory operation.

Note the following special cases:

- ◆ If you have Backup Exec volumes to manage, see the Backup Exec Tape Reader topics in the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I*.
- ◆ If you have volumes without barcodes to manage, see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354.

## Overview of Robot Inventory 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 EMM 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.
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 179.



◆ **Compare contents with volume configuration**

Compares the contents of a robotic library with the contents of the EMM database. Regardless of the result the 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 182.

◆ **Preview volume configuration changes**

Inventories the selected robotic library and compares the results with the contents of the EMM database. If there are differences, the results section shows a list of recommended changes. A preview allows you to ensure that all new media have barcodes before they are added to the EMM database.

After checking the results of a preview, you can perform a volume configuration update operation to update the database to agree with the contents of the robot.

For instructions on performing a preview, see “Procedure To Update the Volume Configuration” on page 187.

◆ **Update volume configuration**

Inventories the selected robotic library and compares the results with the contents of the EMM database. If there are differences, Media Manager updates the database to match the contents of the robot.

For detailed instructions, see “Procedure To Update the Volume Configuration” on page 187.

If you select **Update volume configuration** (or **Preview volume configuration changes**), 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.

- ◆ **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

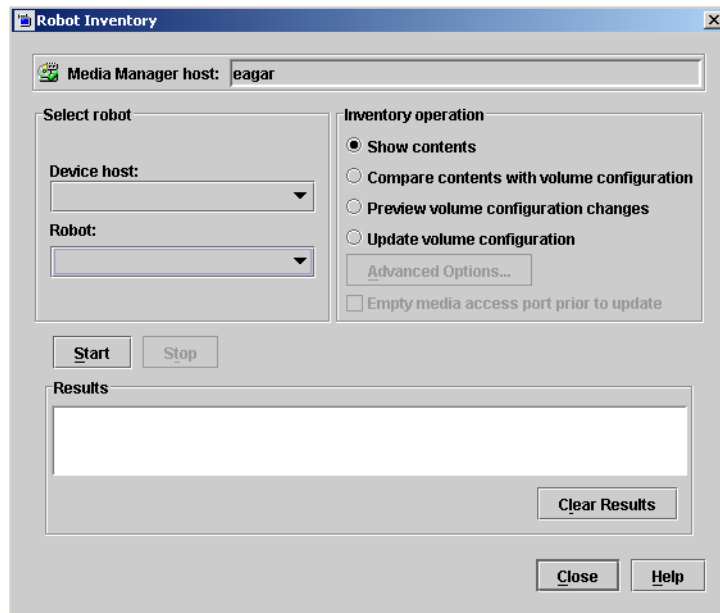
To use the Robot Inventory dialog for robot management tasks (for example, “Comparing Robot Contents with the Volume Configuration” on page 182), you will first need to perform the following set of common steps to access the Robot Inventory dialog. These steps are always required, but are not repeated in the task descriptions in this chapter.

- ▼ **To access the Robot Inventory dialog**

1. In the NetBackup Administration Console, select **Media and Device Management > Media > Robots**.
2. Select the robot you want to inventory.



3. Select **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 177.
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)

The screenshot shows the 'Robot Inventory' dialog box. At the top, 'Media Manager host' is set to 'eagar'. Under 'Select robot', 'Device host' is 'eagar' and 'Robot' is 'TLD(0) - eagar'. In the 'Inventory operation' section, 'Show contents' is selected. Below this are buttons for 'Advanced Options...' and a checkbox for 'Empty media access port prior to update'. At the bottom left are 'Start' and 'Stop' buttons. The 'Results' section displays a text report with a table of robot contents.

Media Manager host: eagar

Select robot

Device host: eagar

Robot: TLD(0) - eagar

Inventory operation

☒ Show contents

☐ Compare contents with volume configuration

☐ Preview volume configuration changes

☐ Update volume configuration

Advanced Options...

☐ Empty media access port prior to update

Start Stop

Results

```

04/20/2005 11:03:14
Robot: TLD(0) on eagar
Operation: Inventory
  
```

Robot Contents

Slot	Tape	Barcode
1	Yes	GL0519
2	Yes	GL0520
3	Yes	GL0521
4	No	
5	No	

Clear Results

Close Help



**Note** If a volume is mounted in a drive, the inventory report lists the slot that it was in before it was moved to the drive.

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.

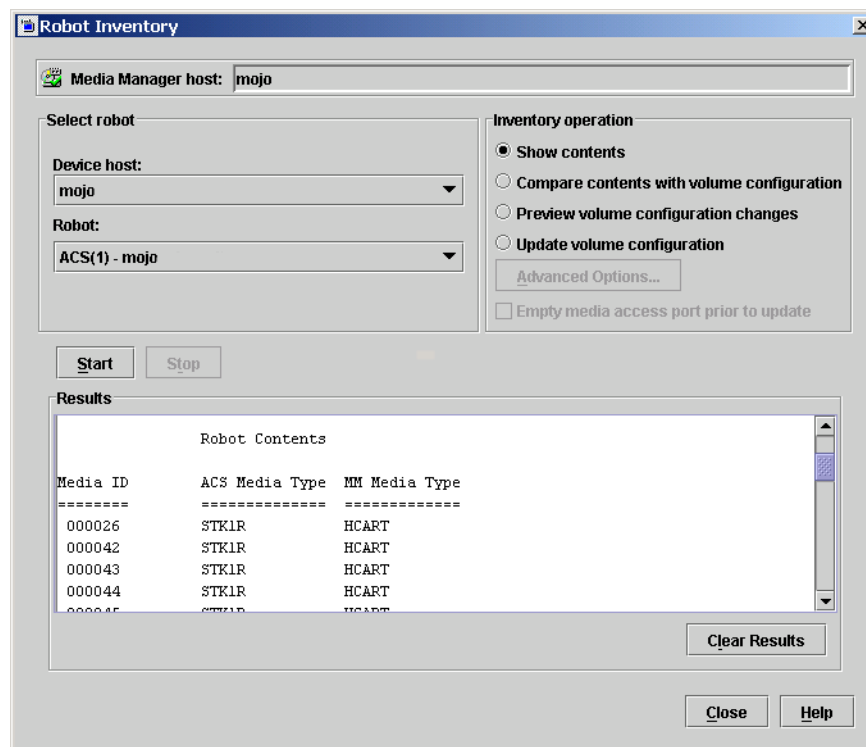
See “Robot Attributes” on page 311 for information on the robots that support barcode readers and the supported barcode length.

See “How Contents Reports for API Robots are Generated” on page 180 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)



Depending on your type of API robot, see the following topics:

- ◆ “ACS Robots” on page 181
- ◆ “TLH Robots” on page 181
- ◆ “TLM Robots” on page 181

## 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 492 for more information on how Media Manager reports what it receives from ACS library software.

## 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 505 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 the 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 519 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 177.
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 EMM database.

See “Compare Volume Configuration Reports” on page 182 for information on the reports that are generated.

4. If the report shows that the EMM 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 187.

## 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 311), the report includes barcode information. Media Manager determines if the barcodes in the robot match those in the EMM 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)

The screenshot shows the 'Robot Inventory' window. At the top, 'Media Manager host' is set to 'eagar'. Under 'Select robot', 'Device host' is 'eagar' and 'Robot' is 'TLD(0) - eagar'. In the 'Inventory operation' section, 'Compare contents with volume configuration' is selected. Below this are buttons for 'Start', 'Stop', 'Advanced Options...', and a checkbox for 'Empty media access port prior to update'. The 'Results' section contains a table comparing robot contents with volume configuration.

Robot Contents			Volume Configuration		
Slot	Tape	Barcode	Media ID	Barcode	Mismatch Detected
1	Yes	GL0519	GL0519	GL0519	
2	Yes	GL0520	GL0520	GL0520	
3	Yes	GL0521	GL0521	GL0521	
4	No				
5	No				
6	No				
7	No				
8	No				

Buttons at the bottom include 'Clear Results', 'Close', and 'Help'.

- ◆ For API robots, Media Manager determines whether the media ID and media type in the EMM database matches what it receives from the vendor's robotic library software.

The following figure shows example results for an ACS robot. Results for other API robots are similar to this report.

See "Robot Inventory Operations" on page 492 for more information on what Media Manager receives from ACS library software.



### Compare Contents Report (API Robot)

The screenshot shows the 'Robot Inventory' window. At the top, 'Media Manager host' is set to 'mojo'. Under 'Select robot', 'Device host' is 'mojo' and 'Robot' is 'ACS(1) - mojo'. In the 'Inventory operation' section, 'Compare contents with volume configuration' is selected. Below this are buttons for 'Start', 'Stop', 'Advanced Options...', and a checkbox for 'Empty media access port prior to update'. The 'Results' section contains a table comparing 'Robot Contents' and 'Volume Configuration'.

Robot Contents			Volume Configuration		
Media ID	ACS Media Type	MM Media Type	Media ID	Media Type	Mismatch?
000026	STKLR	HCART	000026	HCART	
000042	STKLR	HCART	000042	HCART	
000043	STKLR	HCART	000043	HCART	
000044	STKLR	HCART	000044	HCART	
000045	STKLR	HCART	000045	HCART	

- ◆ If the robotic library cannot read barcodes, Media Manager verifies only whether the EMM 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 EMM database to match the contents of the robotic library.

- ◆ “When to Use Update Volume Configuration” on page 185
- ◆ “When Not to Use Update Volume Configuration” on page 186
- ◆ “Updating the Volume Configuration for Non-Barcoded Media” on page 187
- ◆ “Procedure To Update the Volume Configuration” on page 187
- ◆ “Media Settings Tab (Advanced Options)” on page 190
- ◆ “Properties for the Media Settings Tab” on page 191
- ◆ “Barcode Rules Tab (Advanced Options)” on page 202



- ◆ “Media ID Generation Tab (Advanced Options)” on page 207
- ◆ “Media Type Mappings Tab (Advanced Options)” on page 211

## 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 configuration information (or media information) that is stored in the EMM database, after performing one of the following tasks:

- ◆ Removing existing volumes from a robotic library.

This operation updates the residence information in the EMM 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 202.

If the robotic library supports barcodes and the volume has readable barcode labels, the operation creates new volume entries in the EMM 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 207).

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 123.

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 EMM 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 EMM database to show the new slot location.



- ◆ Physically moving volumes between robotic and standalone.  
The operation updates the residence information in the EMM database to show the new robotic or standalone location.
- ◆ Physically moving volumes from one robotic library to another.  
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 226.

## 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 187), 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 EMM 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 EMM 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 227.

## 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. `vmphysinv`, 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 EMM database.

See “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354 for more information.

## Procedure To Update the Volume Configuration

*The following point applies only to NetBackup Enterprise Server.*

### ▼ 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 182.

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 187).

### ▼ To update the volume configuration for a robot

1. Perform the steps described in “Accessing the Robot Inventory Dialog” on page 177.
2. In the Inventory operation section of the Robot Inventory dialog, select **Update volume configuration**.

To preview the update without making any changes to the EMM database, select **Preview volume configuration changes**.



**Caution** If you preview the configuration changes first and then update the EMM database, the update results may not match the results of the preview operation. This can be caused by the state of the robot, EMM database, barcode rules, media type mappings and so on, that may have changed between the preview and the update.

---

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 190.
Create barcode rules.	See “Barcode Rules Tab (Advanced Options)” on page 202.
Create media ID generation rules.	See “Media ID Generation Tab (Advanced Options)” on page 207.
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 211.

---

4. 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 “Performing a Volume Configuration Update Using Robot Inventory” on page 146 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 command, 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.

---

5. To clear any previous display in the Results section, click **Clear Results**.

Click **Start** to start the update (or the preview).

## Example Update Volume Configuration Reports

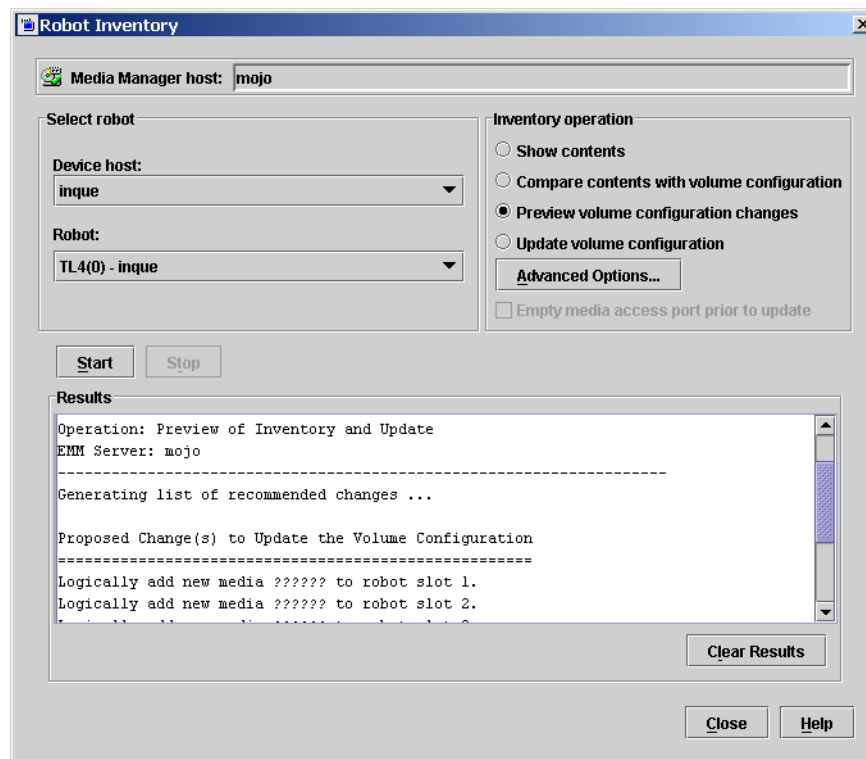
The following figure shows example results for a robotic library that is not an API robot.

---

**Note** *Selecting a device host applies only to NetBackup Enterprise Server.*

---

Update Volume Configuration Report (Not an API Robot)

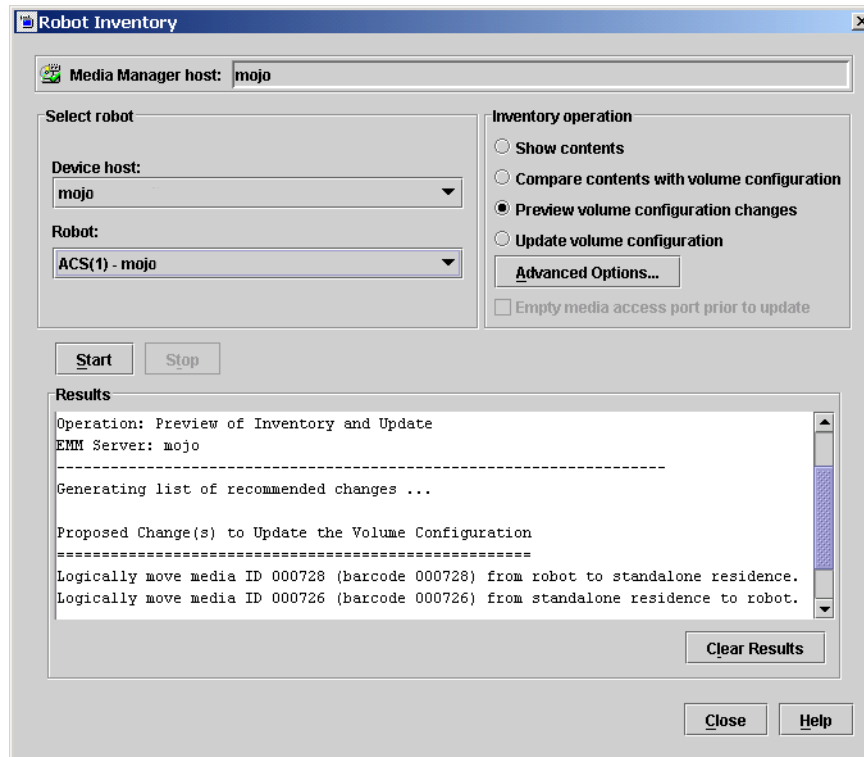


The following figure shows example results for an ACS robot. Results for other API robots are similar to this report.

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)



The screenshot shows the 'Robot Inventory' window. At the top, the 'Media Manager host' is set to 'mojo'. Under 'Select robot', the 'Device host' is 'mojo' and the 'Robot' is 'ACS(1) - mojo'. In the 'Inventory operation' section, the 'Preview volume configuration changes' radio button is selected. Below this is an 'Advanced Options...' button and a checkbox for 'Empty media access port prior to update'. At the bottom left are 'Start' and 'Stop' buttons. The 'Results' pane shows the following text:

```
Operation: Preview of Inventory and Update
EMM Server: mojo
-----
Generating list of recommended changes ...

Proposed Change(s) to Update the Volume Configuration
-----
Logically move media ID 000728 (barcode 000728) from robot to standalone residence.
Logically move media ID 000726 (barcode 000726) from standalone residence to robot.
```

Buttons for 'Clear Results', 'Close', and 'Help' are located at the bottom right of the window.

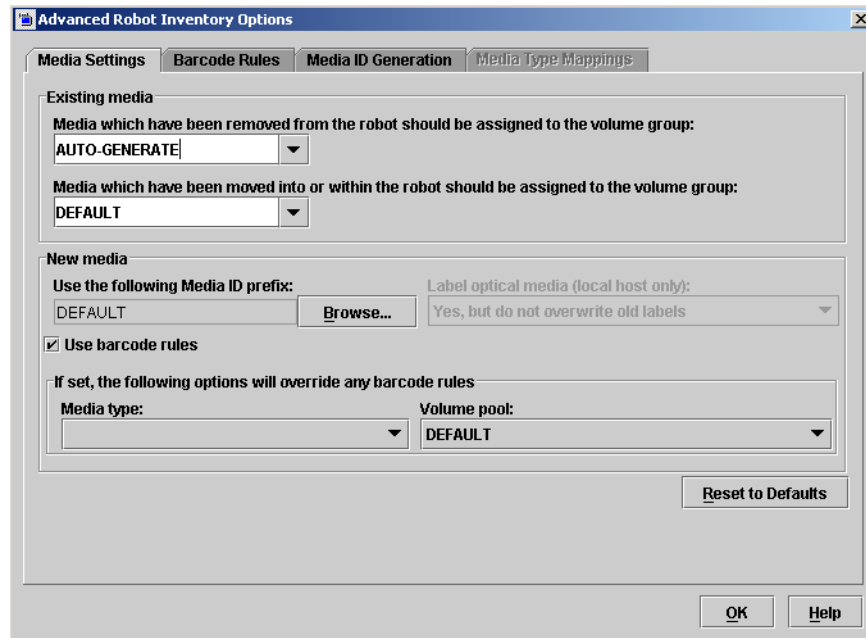
## Media Settings Tab (Advanced Options)

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 191.

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 192
- ◆ “Media Which Have Been Moved Into or Within the Robot” on page 193
- ◆ “Use the Following Media ID Prefix” on page 194
- ◆ “Label Optical Media (Local Host Only)” on page 195



- ◆ “Use Barcode Rules” on page 196
- ◆ “Media Type” on page 197
- ◆ “Volume Pool” on page 201

## 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 197.

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 198).
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 197.

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 198).
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 207.

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

See “The Media Manager Configuration File (`vm.conf`)” on page 387 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.

---

### ▼ To specify a media ID prefix

- ❖ Click **Browse** if you want media IDs for media generated based on a specific prefix. You then specify a media ID prefix using either of the following methods:

▼ **To specify a media ID prefix by entering a new value**

1. Click **Specify the media ID prefix for current session only**.

2. Enter a new value for the prefix in the text box.

The prefix 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.

3. Click **OK** to return to the **Media Settings** tab.

▼ **To specify a media ID prefix by selecting from the list**

1. Click **Choose from the media ID prefix list (stored in vm.conf file)**.

2. You can optionally add a new prefix to the list (you can also remove prefixes).

- a. Enter a prefix in the text box.

- b. Click **Add**.

3. Select a choice for the prefix from the list (does not have to be a prefix that was just added).

4. Click **OK** to return to the **Media Settings** tab.

### **Label Optical Media (Local Host Only)**

**Label optical media (local host only)** is enabled only if you selected an optical robot to inventory. The media labeling will only be done if the robot is attached to the local host specified during the NetBackup Java login.

---

**Note** The media is labeled, but is not formatted.

---

▼ **To label optical media**

- ❖ Click the arrow **a** and select one of the three choices for how you want the media labeled (**Yes, but do not overwrite old labels** - **Yes, overwrite as needed** - **No**).



## 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 <b>Use barcode rules</b>	Searches existing barcode rules and applies the rules to new volumes that have been inserted into a robot.
Clear <b>Use barcode rules</b>	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). Media type is always set to DEFAULT for API robots. See “Media Type Mappings Tab (Advanced Options)” on page 211 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 198.
Yes	“Specifying Media Type (when using barcode rules)” on page 199.



**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	<b>DEFAULT.</b> If <i>all</i> of the drives in the robotic library (configured on this robot host) are <ul style="list-style-type: none"><li>• 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.</li><li>• <i>Not</i> the same type, then Media Manager uses the default media type for the robotic library.</li></ul>
A media type other than the default media type	A media type from the list. 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. <i>The following point applies only to NetBackup Enterprise Server.</i> 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.

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)	Rewritable optical disk. Also supports write-once read-many (WORM) operations.
Tape Library 4MM (TL4)	4MM cartridge tape.
Tape Library 8MM (TL8)	8MM cartridge tape. Also supports 8MM cartridge tape 2 and 8MM cartridge tape 3.

## 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 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 225.





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
CatalogBackup
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 196).

The following topics explain how to manage barcode rules:

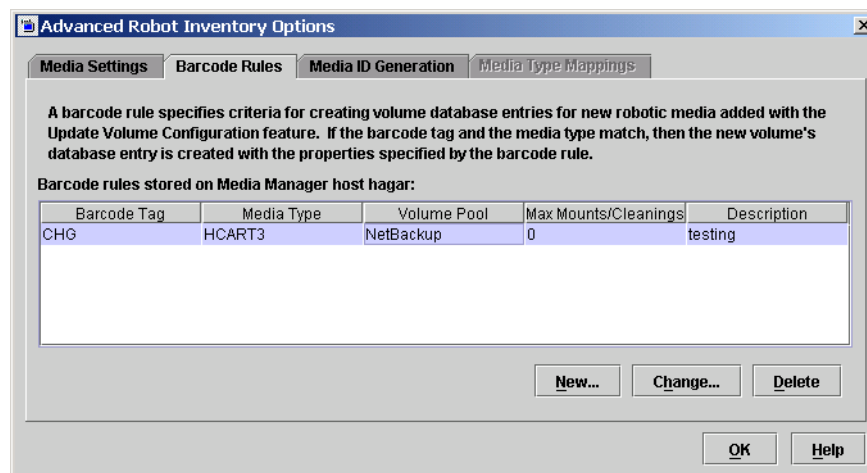
- ◆ “Adding a New Barcode Rule” on page 202
- ◆ “Changing a Barcode Rule” on page 203
- ◆ “Deleting a Barcode Rule” on page 204
- ◆ “Dialog Properties for Adding or Changing Barcode Rules” on page 204

For background information, see “Barcode Rules” on page 352.

### 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 204 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 204 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 204
- ◆ “Maximum Mounts” on page 205
- ◆ “Media Type” on page 205
- ◆ “Volume Pool” on page 207
- ◆ “Description” on page 207

### Barcode Tag

The barcode tag can have from 1 to 16 characters, but cannot contain any spaces (see “Allowable Media Manager Characters” on page 308). A barcode tag can have a maximum of 16 characters. But in the EMM 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 311 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 190).



▼ **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 EMM 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. 0 indicates unlimited mounts.
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 211 for more information.



---

**Note** For API robots, barcode rules that contain media types incompatible with vendor media types may lead to a Robot Inventory update adding media with media types not consistent with the vendor media types. Avoid this by using barcode rules that are grouped by media type.

---

See “Specifying Media Type (when using barcode rules)” on page 199 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
<i>Any</i> 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.
<i>Only</i> 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.

Select the following media type for the barcode rule	Resulting media type that is used
--	-----------------------------------

A specific media type.	The media type that you select for the barcode rule.
------------------------	--

**Note** When a media type is selected, the **Maximum Mounts** value, if previously set, may revert to the default value for the specified media type. For example, to 0 for unlimited when a non-cleaning media type has been selected.

### 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 208

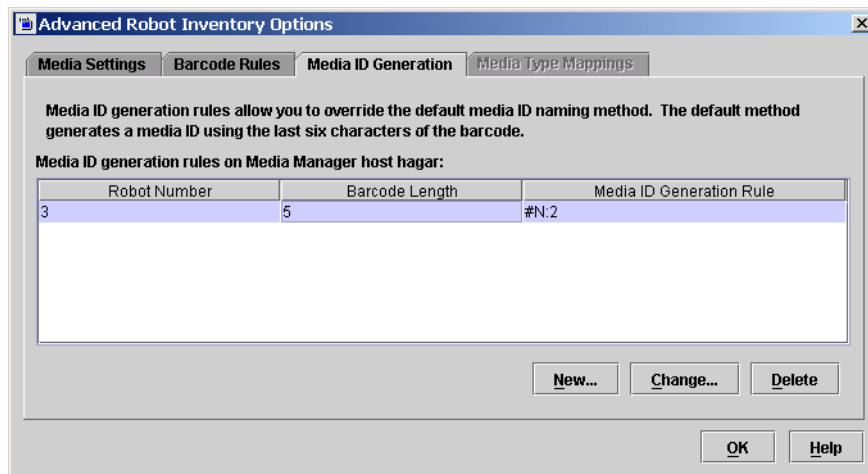


- ◆ “Changing a Media ID Generation Rule” on page 209
  - ◆ “Deleting a Media ID Generation Rule” on page 210
  - ◆ “Dialog Properties for Adding or Changing Media ID Generation Rules” on page 210
- For background information see “Media ID Generation Rules” on page 354.

## Adding a New Media ID Generation Rule

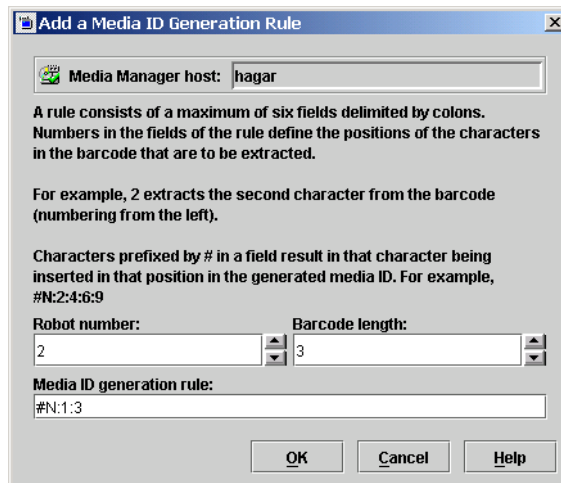
### ▼ To add a rule

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 210 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 or rules from the list of rules.
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 210 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.

<b>Eight-character Tape Barcode</b>	<b>Media ID Generation Rule</b>	<b>Generated Media Manager Media ID</b>
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
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, TLH, or TLM robot types on NetBackup Enterprise Server.*

For API robots, the Media type setting on the **Media Settings** tab is always set to DEFAULT (see “Media Type” on page 197). 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 211
- ◆ “Using the Tab to Change Media Type Mappings” on page 212
- ◆ “Adding Mapping Entries to vm.conf” on page 213
- ◆ “Default and Allowable Media Types for API Robots” on page 214

### How the Mapping Defaults Shown on the Tab are Determined

The default media types shown on the **Media Type Mappings** tab are the media types shown in the second column of the API robot tables (see “Default and Allowable Media Types for API Robots” on page 214).



**Note** The update operation also uses any robot-specific media mappings you have added to the Media Manager configuration file (see “Adding Mapping Entries to `vm.conf`” on page 213).

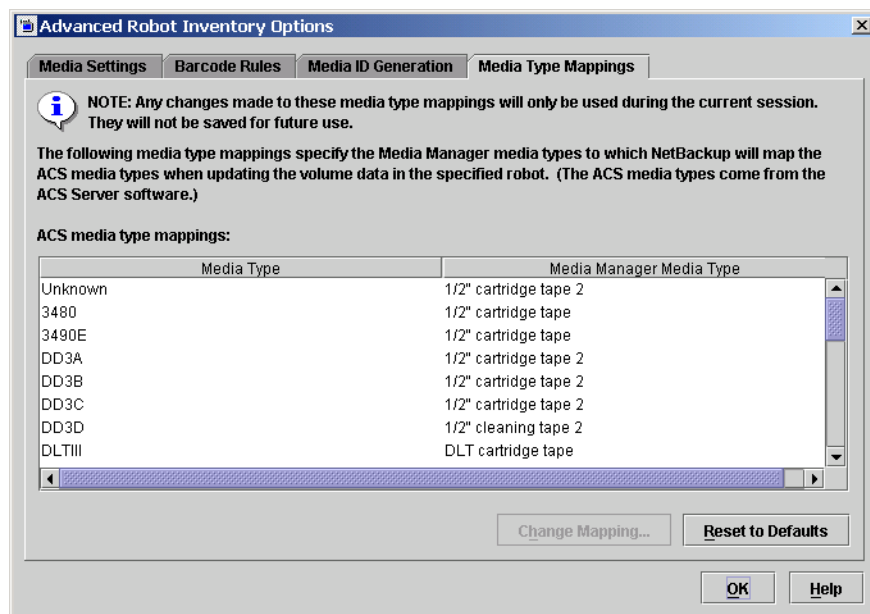
If the `vm.conf` file does not exist or it does not contain media mapping entries for that robot and media type, the update operation uses the default media types and any mappings that you have set on the **Media Type Mappings** tab.

## Using the Tab to Change Media Type Mappings

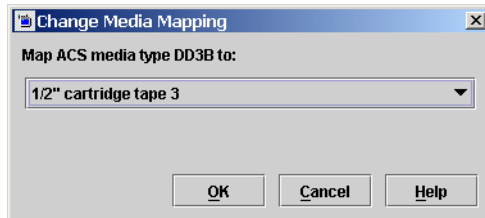
On the **Media Type Mappings** tab you can map the media types for a particular robot vendor that is shown, to one of the allowable Media Manager types for that robot vendor. Media Manager uses any mappings that you have set on this tab for this update. Your mapping changes apply only to the current 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**.

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 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.
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 387 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



Default and Allowable Media Types for ACS Robots (continued)

ACS Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
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
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
SDLT_2	Digital Linear Tape (DLT)	DLT, DLT2, DLT3
T10000T1	1/2-inch cartridge tape 3(HCART3)	HCART, HCART2, HCART3
T10000TS	1/2-inch cartridge tape 3(HCART3)	HCART, HCART2, HCART3



## Default and Allowable Media Types for ACS Robots (continued)

ACS Media Type	Default Media Manager Media Type	Allowable Media Types Through Mappings
T10000CT	1/2-inch cartridge tape 3(HCART3)	HCART, HCART2, HCART3
LTO_400G	1/2-inch cartridge tape 3(HCART3)	HCART, HCART2, HCART3
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 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
3592JA	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
3592JW	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
3592JJ	1/2-inch cartridge tape 2 (HCART2)	HCART, HCART2, HCART3
3592JR	1/2-inch cartridge tape 2 (HCART2)	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.

**Note** For API robots, barcode rules that contain media types incompatible with vendor media types may lead to a Robot Inventory update adding media with media types not consistent with the vendor media types. Avoid this by using barcode rules that are grouped by media type.



## 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 EMM 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 226.

---



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 EMM 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 EMM 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 186 and “Example 7: Adding Existing Volumes when Barcodes are Not Used” on page 227).

---

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 EMM 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 EMM 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 227.

---

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 187.





The NetBackup Device Monitor provides menus and commands that are used to manage drives, device paths, and service requests for operators. The following topics provide information on using the Device Monitor window:

- ◆ “Starting the Device Monitor” on page 232
- ◆ “Using the Device Monitor Window” on page 232
- ◆ “Controlling the Media Manager Device Daemon” on page 247
- ◆ “Monitoring Devices on Other Servers” on page 248
- ◆ “Changing the Operating Mode of a Drive” on page 249
- ◆ “Resetting a Drive” on page 250
- ◆ “Drive Cleaning Functions” on page 251
- ◆ “Adding or Changing a Drive Comment” on page 253
- ◆ “Obtaining Information About a Drive” on page 253
- ◆ “Managing Drive Paths” on page 254
- ◆ “Handling Pending Requests and Pending Actions” on page 254
- ◆ “Resolving Pending Requests” on page 256
- ◆ “Resolving Pending Actions” on page 259
- ◆ “Resubmitting Requests” on page 259
- ◆ “Denying Requests” on page 260

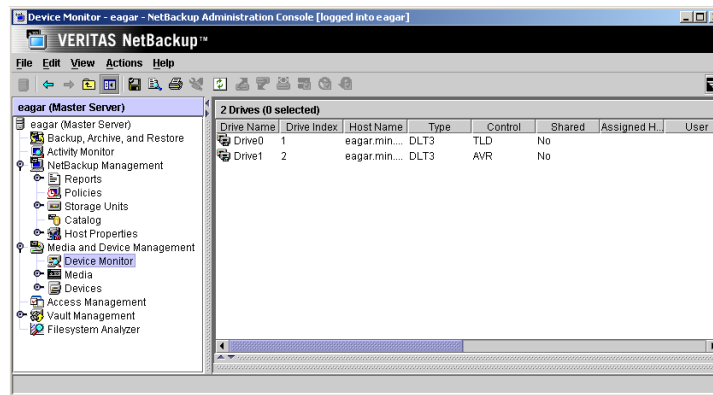
*The following topic applies only to NetBackup Enterprise Server.*

- ◆ “Shared Storage Option Summary Reports” on page 261



## 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, a pane showing drive information is displayed on the right when you start the Device Monitor. Also the following panes are displayed on the right as needed:

- ◆ A pane showing path information for drives. This pane appears only if a drive is configured as a shared drive or there are multiple paths to a drive.
- ◆ A pane for pending requests (or pending actions). This pane appears if there is a pending request or pending action that is active.
- ◆ A pane for task progress messages.

## Using the Device Monitor Window

The following topics provide an overview of the Device Monitor window:

- ◆ “Menus and Commands” on page 233
- ◆ “Toolbars” on page 236
- ◆ “Drive Status Pane” on page 236
- ◆ “Drive Paths Pane” on page 240
- ◆ “Pending Requests Pane” on page 243
- ◆ “Messages Pane” on page 246
- ◆ “Shortcut Menus and Commands” on page 246





- ◆ “Customizing the Window” on page 246

## 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 drive status or pending requests panes. For example if a drive is selected in the drive status pane, **Up Drive** is enabled on the **Actions** menu.

Device Monitor Menus and Commands

Menu	Commands	Note
<b>File</b>	<p><b>Change Server</b> - 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 248 for details</p> <p><b>New Console</b> - Starts another instance of NetBackup Administration Console.</p> <p><b>New Window from Here</b> - Starts another instance of the NetBackup Administration Console node that was active.</p> <p><b>Adjust Application Time Zone</b> - Displays a dialog that allows you to manage the time zone. NetBackup Console can execute in a different time zone than the time zone of the server on which it was initiated. See the <i>VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I</i> for more information.</p> <p><b>Export</b> - Saves configuration information or data about the selected device monitor to a file.</p> <p><b>Page Setup</b> - Displays a setup dialog for printing.</p> <p><b>Print Preview</b> - Previews the print image.</p> <p><b>Print</b> - Prints the drive status, drive paths, or pending requests pane (when one of these panes is selected).</p> <p><b>Close Window</b> - Closes the current window.</p> <p><b>Exit</b> - Closes all open windows.</p>	
<b>Edit</b>	<p><b>Find</b> - Command for finding items in the display lists.</p>	
<b>View</b>	<p>Contains commands for specifying your viewing preferences for the Device Monitor, including showing and hiding the toolbar or tree, and refreshing the display. See “Customizing the Window” on page 246.</p>	



## Device Monitor Menus and Commands (continued)

Menu	Commands	Note
<b>Actions</b>	<p><b>Up Drive</b> - 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.</p> <p>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.</p> <p>For standalone drives using unlabeled volumes, you assign tape drives to requests using <b>Actions &gt; Assign Request</b>.</p> <p><b>Up Drive, Operator Control</b> - Sets the operating mode of a standalone drive to up in operator control mode (OPR). Do not use this mode for drives that are being used by NetBackup.</p> <p>In NetBackup 6.0, drive paths in OPR mode are eligible for auto-assignment if they satisfy the mount request. There is no distinction between AVR mode and OPR mode relating to auto-assignment of mount requests.</p> <p>This command appears on the menu only if it has been enabled. To enable this command, select <b>View &gt; Options &gt; Device Monitor</b> and select <b>Show 'Up, Operator Control'</b>.</p> <p><b>Down Drive</b> - 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.</p> <p>When changing the operating mode of drives in SSO configurations, also see "Changing the Operating Mode of a Drive" on page 249.</p> <p><b>Reset Drive</b> - Resets the specified drive, terminating the drive assignment and taking control away from the assigned user.</p> <p>For SSO configurations with multiple hosts, the drive is only reset on the device host being managed.</p> <p>For more information, see "Resetting a Drive" on page 250.</p> <p><b>Drive Cleaning</b> - Displays a sub-menu with choices for performing drive cleaning functions.</p>	<p>Applies only to NetBackup Enterprise Server.</p>



## Device Monitor Menus and Commands (continued)

Menu	Commands	Note
	<p><b>Change Drive Comment</b> - Displays a dialog for changing the comment for the selected drive. The comment is applied across all hosts sharing the drive.</p> <p>For SSO configurations also see “Adding or Changing a Drive Comment” on page 253.</p> <p><b>Drive Details</b> - Displays a dialog with information about the selected drive, including drive properties, drive status, and robotic library information.</p> <p><b>Assign Request</b> - Assigns a drive to a pending request.</p> <p><b>Deny Request</b> - Denies a pending request.</p> <p><b>Resubmit Request</b> - Resubmits a pending request.</p> <p><b>Display Pending Action</b> - Displays information about the pending action.</p> <p><b>Stop/Restart Media Manager Device Daemon</b> - Controls the Media Manager device daemon.</p> <p><b>View Status of Shared Drives</b> - Displays a dialog that allows you to display device allocation information about SSO configurations. See “Shared Storage Option Summary Reports” on page 261.</p>	
Help	<p><b>Help Topics</b> - Provides online help information for the NetBackup Console.</p> <p><b>Troubleshooter</b> - Helps you to debug errors.</p> <p><b>License Keys</b> - Provides information about your active and registered license keys.</p> <p><b>Current NBAC User</b> - Provides NetBackup Access Control information for the current user. Gives the permissions for the user that you are currently logged in as.</p> <p><b>About NetBackup Administration Console</b> - Displays program information, version number, and copyright information.</p>	



## 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 246.

### ▼ To show or hide the toolbar buttons

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. Select **View > Show Toolbar**.

## Drive Status Pane

This pane shows the status of the drives that Media Manager controls on this server. The following table describes the columns displayed in this pane. Check the Note column for any restrictions.

Drive Status Pane

Column	Description	Note
Drive Name	Drive name assigned to the drive during configuration.	
Drive Type	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: 4MM (4mm cartridge) 8MM (8mm cartridge) 8MM2 (8mm cartridge 2) 8MM3 (8mm cartridge 3) DLT (DLT cartridge) DLT2 (DLT cartridge 2) DLT3 (DLT cartridge 3) DTF (DTF cartridge) HCART (1/2-inch cartridge) HCART2 (1/2-inch cartridge 2) HCART3 (1/2-inch cartridge 3) ODISK (optical disk) QSCSI (1/4-inch cartridge)	



## Drive Status Pane

Column	Description	Note
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).	Applies only to robotic drives.
	DOWN- <i>robot_designation</i> . For example, DOWN-TLD. The drive is in an unusable state because it was downed by an operator or by NetBackup; or when the drive was configured, it was added as a down drive.	Applies only to robotic drives.
	DOWN. In this mode, the drive is not available to Media Manager.	Applies only to standalone drives.
	A drive can be in a DOWN mode because of problems or because it was set to that mode using <b>Actions &gt; Down Drive</b> .	
	AVR 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.	Applies only to robotic drives.
	AVR The drive is running with automatic volume recognition enabled.	Applies only to standalone drives.
	OPR The drive is running in OPR mode. In NetBackup 6.0, drive paths in OPR mode are eligible for auto-assignment if they satisfy the mount request. There is no distinction between AVR mode and OPR mode relating to auto-assignment of mount requests.	Applies only to standalone drives.



## Drive Status Pane

Column	Description	Note
	<p>SCAN.</p> <p>A drive is configured for SSO, but has no available scan host (to be considered available, a host must have an SSO_SCAN_ABILITY factor of non-zero and have the drive in the UP state).</p> <p>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 have a scan factor of zero. The drive is unusable by NetBackup until a scan host is assigned.</p>	Applies only to NetBackup Enterprise Server.
	<p>&lt;Mixed&gt;.</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. The status of individual paths to the drive is displayed in the <b>Drive Path</b> column. If the control modes <i>are</i> all the same, that mode is displayed.</p>	Applies only to NetBackup Enterprise Server.
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	<p>Status of the drive, indicating if it is ready to perform an operation on the loaded volume. Yes, means ready. No, means not ready.</p> <p>See the vendor's manual for the drive for instructions to make it ready, if the drive does not become ready automatically.</p>	
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.	
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.	
Request ID	If this drive is assigned to a request, this column contains the ID of the request.	



## Drive Status Pane

Column	Description	Note
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.	
Drive Comment	Comments that have been added for this drive. See “Adding or Changing a Drive Comment” on page 253.	
Shared	Yes, means this drive is configured as a shared drive. No, means the drive is not a shared drive.	
Device Host	The name of the device host where the drive is connected.  If a drive is configured as shared, this column contains <Multiple>.	
Drive Path	The device path to the drive.  If a drive is configured with multiple paths to it, this column contains <Multiple>. See “Drive Paths Pane” on page 240 for detailed path information for drives that are shared or have multiple paths configured.	
Port	This column contains the SCSI port number of the drive.	Applies only to NetBackup Windows servers.
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.



## Drive Status Pane

Column	Description	Note
NDMP Host	Contains the name of the NDMP control host. If the drive has multiple paths configured, this column contains Multiple.	Requires NDMP license.
	If the drive is configured as a shared drive (SSO), this column contains Multiple.	Applies only to NetBackup Enterprise Server.
Drive Index	Drive index assigned to the drive during configuration.  This column contains <Multiple> for shared drives.	
Cluster Name	For a Virtual Cluster, displays the cluster name. See the <i>NetBackup High Availability System Administrator's Guide for Windows, UNIX, and Linux</i> for more information.	Applies only to supported cluster environments.

## Drive Paths Pane

This pane shows path information for drives. This pane is displayed only if a drive is configured as a shared drive, or if there are multiple paths to a drive configured.

The following table describes the columns displayed in this pane. Review the Note column for any restrictions. All columns in this table also appear in the Drive Status table (see “Drive Status Pane” on page 236).

## Drive Paths Pane

Column	Description	Note
Drive Name	Contains the configured name of the drive.	
Device Host	The name of the device host that has the drive.	
NDMP Host	If NDMP-attached, contains the name of the NDMP control host.	Requires an NDMP license.





## Drive Paths Pane

Column	Description	Note
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 Itid (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 unusable 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 <b>Actions &gt; Down Drive</b> .  PEND- <i>robot_designation</i> . For example, PEND-TLD.  PEND  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. Some server operating systems (Windows, Tru64, and HP-UX) may report PEND if the drive reports Busy when opened. You can use the AVRD_PEND_DELAY entry in the Media Manager configuration file to filter out these reports.	Applies only to robotic drives.  Applies only to robotic drives.  Applies only to standalone drives.  Applies only to robotic drives.  Applies only to standalone drives.



## Drive Paths Pane

Column	Description	Note
	<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>	Applies only to robotic drives.
	<p>AVR</p> <p>The drive is running with automatic volume recognition enabled.</p>	Applies only to standalone drives.
	<p>OPR</p> <p>The drive is running in OPR mode.</p> <p>In NetBackup 6.0, drive paths in OPR mode are eligible for auto-assignment if they satisfy the mount request. There is no distinction between AVR mode and OPR mode relating to auto-assignment of mount requests.</p>	Applies only to standalone drives.
	<p>SCAN</p> <p>A drive is configured for SSO, but has no available scan host (to be considered available, a host must have an SSO_SCAN_ABILITY factor of non-zero and have the drive in the UP state).</p> <p>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 have a scan factor of zero. The drive is unusable by NetBackup until a scan host is assigned.</p>	Applies only to NetBackup Enterprise Server.
	<p>&lt;Mixed&gt;</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. The status of individual paths to the drive is displayed in the <b>Drive Path</b> column. If the control modes are all the same, that mode is displayed.</p>	Applies only to NetBackup Enterprise Server.
Cluster Name	For a Virtual Cluster, displays the cluster name. See the <i>NetBackup High Availability System Administrator's Guide for Windows, UNIX, and Linux</i> for more information.	Applies only to supported cluster environments.
Drive Path	For a UNIX device host or an NDMP-attached path on an NDMP host, contains the drive path.	



## Drive Paths Pane

Column	Description	Note
Port	For a Windows device host, this column contains the SCSI port number of the drive.	
Bus	For a Windows device host, this column contains the SCSI bus number of the drive	
Target	For a Windows device host, this column contains the SCSI target number (or SCSI ID) of the drive	
LUN	For a Windows device host, this column contains the SCSI logical unit number of the drive	
NDMP Host	Contains the name of the NDMP control host. If the drive has multiple paths configured, this column contains Multiple.	Requires NDMP license.
	If the drive is configured as a shared drive (SSO), this column contains Multiple.	Applies only to NetBackup Enterprise Server.
Drive Index	Drive index assigned to the drive during configuration.	

## 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 254 for more information.



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. <b>Note</b> A pending action is indicated by a media icon depicting a human hand, located to the left of the Request ID.
Host Name	The name of the device host that has the pending 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 stored in the EMM 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. Note that for some densities, the mapping to the drive type is not identical. For example, the density ODISKWM is drive type ODISK.</p> <p>4MM (4mm cartridge)        8MM (8mm cartridge)        8MM2 (8mm cartridge 2)        8MM3 (8mm cartridge 3)        DLT (DLT cartridge)        DLT2 (DLT cartridge 2)        DLT3 (DLT cartridge 3)        DTF (DTF cartridge)        HCART (1/2-inch cartridge)        HCART2 (1/2-inch cartridge 2)        HCART3 (1/2-inch cartridge 3)        ODISKWM (optical disk-write many)        ODISKWO (optical disk-write once)        QSCSI (1/4-inch cartridge)</p>
Mode	Specifies whether the volume should be write-enabled. Write in this column means you must write-enable the volume. Read 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.
Time	Time of day the user made the request for access.
Barcode	Alphanumeric representation of the barcode label on the volume that was requested by the user.
Volume Group	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.
Media Description	Describes the media in 25 or less alphanumeric characters. You create the description when you configure volumes.



## Messages Pane

The **Messages** pane may appear in the lower right below the status of drives pane, and is used to display messages about a task that is running as a background process. This pane is displayed only if there is an informative message or error message for the task. If the task completes normally, the pane is not displayed.

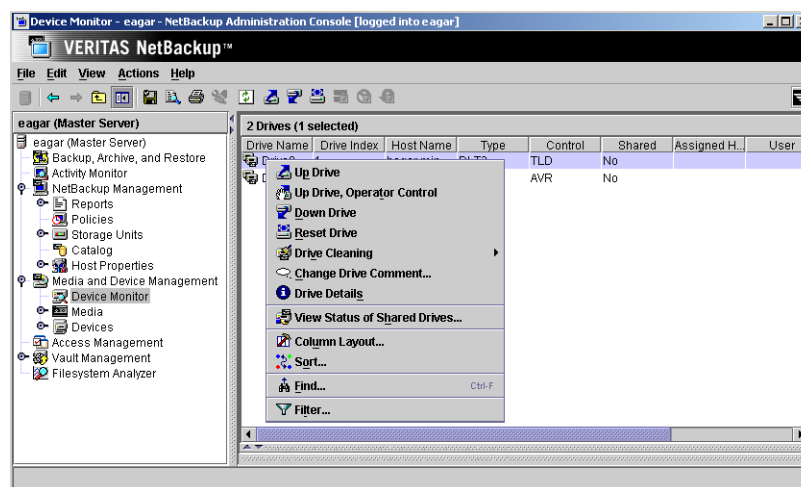
## Shortcut Menus and Commands

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

### ▼ To display a shortcut menu

- ❖ Right click on any object or section in the pane

Shortcut 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

- ❖ Select **View > Column Layout**.

▼ **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. Initially, screen refresh is enabled and the default rate is 60 seconds.

1. Select **View > Options > Device Monitor**.

2. Set the desired refresh rate.

It may be necessary to scroll the Device Monitor window to see any newly arrived jobs after a screen refresh.

To disable screen refresh, unselect **Automatically refresh display every**. The Device Monitor saves the setting of **Automatically refresh display every** when you exit.

## Controlling the Media Manager Device Daemon

The Media Manager device daemon must be running on the host being monitored or the lists in the Device Monitor panes will be blank.

If the daemon is not running when you start the Device Monitor, NetBackup prompts you so you can start it at that time.

---

**Note** If the device host you want to monitor is a Windows host, this procedure controls the NetBackup Device Manager service on that Windows host.

---

▼ **To manage this daemon**

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.

2. Select **Actions > Stop/Restart Media Manager Device Daemon**.

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

Select a device host. The dialog also shows the current status of this daemon.

If the device host is known to NetBackup to be a Backup Exec server, the server does not appear in the list.

The current status field shows the status of this daemon.

4. The dialog allows you to start, stop, or stop/restart the daemon 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**.

---

**Note** *This note applies only to NetBackup Enterprise Server.*

By using **Apply**, you can select device hosts and actions for more than one device host before clicking **OK** to close the dialog.

---

## 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 is shown at the top of the tree pane. For example: spain (Master Server).

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.

You cannot change from a NetBackup Server to a NetBackup Enterprise Server.

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

1. In the NetBackup Administration Console, select the server name shown at the top of the tree.
2. Select **File > Change Server**.
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.

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.

The Media Manager device daemon 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 daemon. Click **OK** in this box.



In addition to using **File > Change Server** to monitor devices on other servers, you can specify a different server when logging into NetBackup.

The name of the UNIX server that you specify in the Login box, when starting the NetBackup Administration interface, must be in the NetBackup `bp.conf` file on the remote UNIX host where you want to monitor devices.

If you encounter problems or for more information on remote administration, see the following topics:

- ◆ “Remote Administration of Other UNIX Servers” on page 42.
- ◆ “Media Manager Security” on page 44.

## 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.

### ▼ To change the mode of a drive

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. In the Drive status pane, select a drive or multiple drives.
3. From the **Actions** menu, choose the command for the new drive operating mode.  
**Up Drive, Operator control** applies only to standalone drives. See the **Actions** menu in “Menus and Commands” on page 233 for an explanation of the operating mode commands.
4. If the selected drive is configured with multiple device paths, a dialog appears containing a list of all device paths to the drive. You can select any number of paths where the mode change will apply.
5. If the selected drive is a shared drive (SSO option), a dialog appears containing a list of all host/device paths to the drive. You can select any number of host/device paths 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 “Drive Status Pane” on page 236 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 Drive status pane *before* changing the drive mode. Notice that the Control column contains AVR and the Ready column contains Yes.

Drive Name	Drive Type	Control	Recorded Media ID	External Media ID	Ready	Writable	Drive
 SEAGATE.ULTRIUM06242-XXX.000	HCART	AVR	000061	000061	Yes	Yes	

The following display shows the Drive 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	Drive Type	Control	Recorded Media ID	External Media ID	Ready	Writable	Drive
 SEAGATE.ULTRIUM06242-XXX.000	HCART	DOWN-TLD			No	No	

## Resetting a Drive

Resetting a drive changes the state of the drive. The actions that result from resetting a drive depend on whether the drive is currently allocated to a user or application.

---

Drive State	Reset Action
In use by NetBackup	The reset action fails.
Not in use by NetBackup	Media Manager attempts to unload the drive and set its runtime attributes to default values.

---

A situation where resetting a drive might be desirable is when the state of the drive is unknown. The drive state can become unknown if the drive has been used by an application other than NetBackup. Resetting the drive returns the drive to a known state prior to use with NetBackup. If a drive is SCSI-reserved by a host, resetting it from that host may help clear the SCSI reservation from that host.

---

**Note** Resetting a drive does not perform any SCSI bus or SCSI device resets.

---

▼ **To reset a drive**

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. In the Drive status pane, select a drive or multiple drives.
3. Select **Actions > Reset Drive**.

▼ **If the drive is in use by NetBackup and cannot be reset**

1. Determine which job is using the drive. In the NetBackup Administration Console, select **Activity Monitor**. From the **Jobs** tab, cancel the job.

See the *NetBackup System Administrator's Guide for Windows, Volume I* or the *NetBackup System Administrator's Guide for UNIX and Linux, Volume I* for more information about using the Activity Monitor.

2. Restart the NetBackup Job Manager using the **Activity Monitor**. You can also restart NetBackup using the `netbackup -stop/-start` command on UNIX or Linux or the `bpdown/bpup` commands on Windows. Note that restarting the NetBackup Job Manager cancels all NetBackup jobs in process.

See *NetBackup Commands for UNIX and Linux* or *NetBackup Commands for Windows* for more information.

## Drive Cleaning Functions

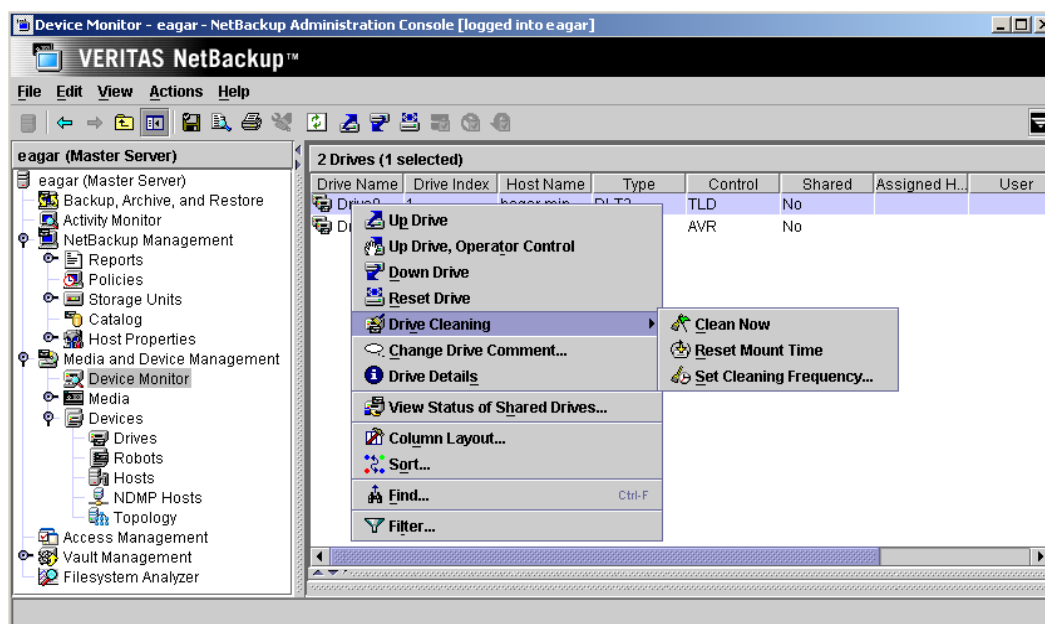
See “Drive Cleaning” on page 339 for background information on types of drive cleaning and cleaning tapes.

▼ **To perform drive cleaning functions**

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. In the Drive status pane, select a drive.



### 3. Select Actions > Drive Cleaning.



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

Select	To
<b>Clean Now</b>	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. <b>Clean Now</b> resets the mount time to zero, but the cleaning frequency value remains the same.
<b>Reset Mount Time</b>	Reset the mount time for the selected drive to zero. Use <b>Reset Mount Time</b> to reset the mount time after doing a manual cleaning of a drive.
<b>Set Cleaning Frequency</b>	Set the desired number of mount hours between each drive cleaning. <b>Set Cleaning Frequency</b> is not available for robots that do not support frequency-based cleaning.

### 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

You may want to add a comment explaining how a drive is used. Any comment for a drive appears in the drive status pane (see “Drive Status Pane” on page 236).

### ▼ To add or change a drive comment

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. In the Drive status pane, select a drive or multiple drives.
3. Select **Actions > Change Drive Comment**.  
The dialog shows the current comment (if any is currently configured).
4. Enter a comment or change the current drive comment.  
See “Allowable Media Manager Characters” on page 308 for a list of allowable characters.
5. Click **OK**.

## Obtaining Information About a Drive

You can obtain detailed information about drives (or shared drives), including drive cleaning, drive properties, drive status, host, and robotic library information.

### ▼ To obtain drive details

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. In the Drive Status pane, select a drive.
3. Select **Actions > Drive Details**.

*The following applies only to NetBackup Enterprise Server.*

For shared drives you can view the drive control mode and drive index for each host that is sharing a drive, and view a list of hosts that are sharing a drive.



## Managing Drive Paths

The Drive Paths pane shows path information for drives. This pane is displayed only if a drive is configured as a shared drive (SSO option), or if there are multiple (redundant) paths to a drive configured (see “Drive Paths Pane” on page 240). From this pane you can manage your drive paths.

### ▼ To manage paths from the Drive Paths pane

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. In the Drive Paths pane, select a host/device path or multiple paths.
3. From the **Actions** menu, choose a command for the path action. Commands applicable for paths are the following: **Up Path**, **Down Path**, **Reset Path**.

## Handling Pending Requests and Pending Actions

In normal operating situations, NetBackup is able to resolve most requests automatically and quickly. In some situations, NetBackup may be not be able to immediately resolve a request. For example, 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 254.
- ◆ 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 255.

### 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 will not automatically complete the request and the request remains in the Pending Requests pane until resolved. NetBackup pends a mount request when it cannot determine which standalone drive, or drive in a robot whose drives are in AVR mode, to use for the job.



To resolve the request, proceed as explained in “Resolving Pending Requests” on page 256.

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 243 for an explanation of the columns in a pending request display.

## Pending Requests (Storage Unit Specific)

**Note** The following information applies only to storage unit specific mount requests (backups, write side of duplicates). Media-specific mount requests (including restores, imports, tpreq, etc.) are not storage unit related and will pend if the robot drives are in AVR mode. Media-specific mount requests can be auto-assigned by NetBackup and manually assigned to any compatible drive

NetBackup will not pend mount requests to robots whose drives are in AVR mode for storage unit related requests. NetBackup will try and pick another storage unit that has a working robot. If NetBackup cannot find a storage unit for the job, NetBackup will queue the job and a **Queued** state will be displayed in the Activity Monitor.

If the robot must be operated in manual mode, set the robot to operate in Pend If Robot Down (PIRD) mode. Use the `tpconfig` command to set the robot in PIRD mode. See *NetBackup Commands for UNIX and Linux* or *NetBackup Commands for Windows* for more information about the `tpconfig` command.

If a robot is operating in PIRD mode, pending requests will appear in the device monitor, and you can manually assign these mount requests to drives. NetBackup will not auto-assign, and it is not possible to manually assign, a mount request targeted to one storage unit to drives of another storage unit.

## 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 a media icon (the icon has a human hand on it depicting that a manual action is required), located 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 259.

---

**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 243 for an explanation of the columns in a pending action (or pending request) display.

## Resolving Pending Requests

### ▼ To assign a drive to a pending request

1. In the NetBackup Administration Console, select **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 Drive 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 243 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. Select **Actions > Assign Request**.  
Verify that the request is cleared from the Pending Requests pane.
7. In the Drive 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 “Drive Status Pane” on page 236 and “Pending Requests Pane” on page 243 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 Drive 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 Drive 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 `tpumount` 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, select **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
 *D 000062	000062	000062	NetBackup	hcart	R	2/5/2003 1:01:23 PM	000062	00_000_TLD

3. Select **Actions > Display Pending Action** (or double-click on the 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 259.
  - or
  - b. Select **Actions > Deny Request** to deny the request. See “Denying Requests” on page 260.

## Resubmitting Requests

### ▼ To resubmit a request

1. In the NetBackup Administration Console, select **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. Select **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 184 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, select **Media and Device Management > Device Monitor**.
2. In the Pending Requests pane, select the request.
3. Select **Actions > Deny Request**.

The request is removed from the Pending Requests pane.



## Shared Storage Option Summary Reports

These two reports contain Media Manager information about your SSO configuration and include the following information about the drives and hosts.

This Report	Contains the Following SSO Information
Shared Drive Summary	Drive name, device allocation host, the number of registered hosts, drive reservation status, hosts reserving this drive, and the current scan host.
Device Allocation Host Summary	The device allocation host, host name of the registered host, the number of registered and reserved drives, availability status, the scan ability factor, and scanning status.

See “Shared Storage Option (SSO) Topics” on page 279 for background, installation, configuration, and verification information for shared drives.

### ▼ To view summary reports

1. In the NetBackup Administration Console, select **Media and Device Management > Device Monitor**.
2. Select **Actions > View Status of Shared Drives**.
3. In the **Status of Shared Drives** dialog, select a device allocation host (or hosts) from the list.
4. Use **Add >>** to move the host to the list of hosts that will be scanned.
5. Click **OK**.

The **Shared Drive Summary** and **Device Allocation Host Summary** appear in the two lower panes of the dialog.





## Managing the Media Manager Daemons

---

## 6

This chapter includes the following Media Manager daemon topics:

- ◆ Overview of Media Manager Daemons
- ◆ Media Manager Device Daemon (ltid)
- ◆ Automatic Volume Recognition Daemon (avrd)
- ◆ Enterprise Media Manager (nbemm)
- ◆ Media Manager Volume Daemon (vmd)
- ◆ Media Manager Status Collection Daemon (vmgcd)
- ◆ Robotic Daemons
- ◆ Displaying Process Status using the vmgs Script
- ◆ Logging of Errors

### Overview of Media Manager Daemons

The following daemons manage the assignment and scanning of devices:

- ◆ `ltid` - The Media Manager device daemon.
- ◆ `avrd` - The automatic volume recognition daemon.
- ◆ `vmd` - The Media Manager volume daemon enables remote device management and enables access to `nbemm` for NetBackup 5.x media servers.
- ◆ `vmgcd` - The Media Manager status collection daemon. `vmgcd` communicates with NetBackup 5.x servers.
- ◆ `nbemm` - The Enterprise Media Manager manages volumes, volume pools, barcode rules and devices. `nbemm` performs media, drive, drive path, and storage unit selection. `nbemm` also acts as the Device Allocator in SSO environments.



## Robotic Daemons and Robotic Control Daemons

A Media Manager robotic daemon (and possibly a robotic control daemon) exist for each robot that you configure on a host where Media Manager is installed.

Every host that has a drive in a robot, has a robotic daemon for that robot. The robotic daemon receives requests from the Media Manager device daemon and sends necessary information directly to the robotics or to a robotic control daemon.

### Library Sharing (or Robot Sharing)

*This is a NetBackup Enterprise Server topic.*

Robotic control daemons also exist for robot types where drives can optionally attach to hosts other than the host with direct robotic control.

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` daemon. The robotics are controlled by a single host and only that host has the robotic control daemon, `tlcdc` installed. This is true even when the robotic control path could be available on multiple hosts in a Shared Storage Option configuration.

When it is necessary to mount a tape, the robotic daemon on the host with the drive sends control information to the robotic control daemon on the host controlling the robotics.

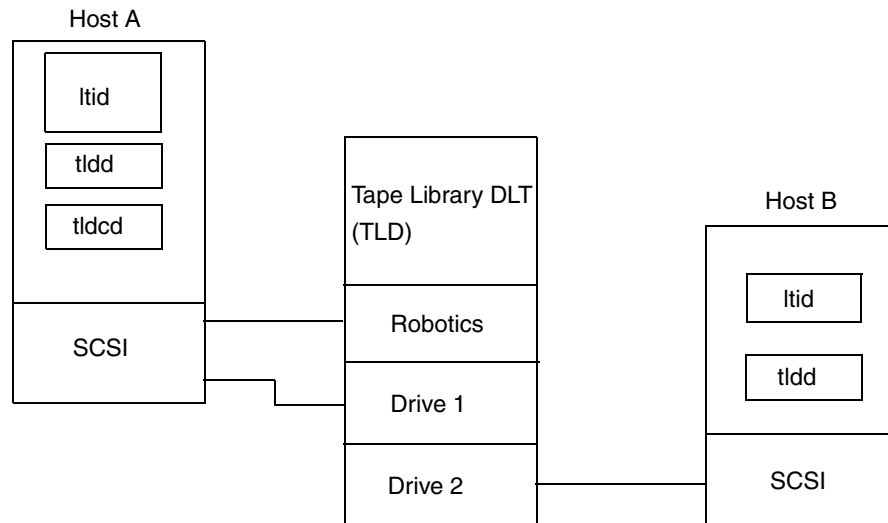
The following figure shows the daemons for a Tape Library DLT robot. In this figure note the following points:

- ◆ Each host connects to one drive and has a robotic daemon, `tldd`.
- ◆ The robotic control and the robotic control daemon, `tlcdc`, is on Host A.

The Media Manager device daemons on host A and B start `tldd`. The `tldd` daemon 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.



## Example TLD Robot and Host Configuration



## Media Manager Device Daemon (ltid)

`ltid` is the interface between Media Manager commands and device control. When a tape request is issued, `ltid` passes the request for the volume to the appropriate robotic daemon to mount the volume.

### Starting the Device Daemon

Starting `ltid` also starts `vmd`, `avrd` and the daemons for any robots with defined drives.

#### ▼ To start ltid from a command line

- ❖ Enter `/usr/opensv/volmgr/bin/ltid`.

To start `ltid` and the robotic daemons in verbose mode and log debug information through `syslogd`, use the `-v` option. This option should only be used when needed for debugging, since it can use large amounts of disk space to save extra information.

#### ▼ To start ltid from the NetBackup Administration Console

1. Use **Actions > Stop/Restart Media Manager Device Daemon**.
2. *This step applies only to NetBackup Enterprise Server.*



In the dialog, the button 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.

Select a host.

3. Click **Start** and **OK**, when ready. This also starts the daemons for any robot that is configured.

## Stopping the Device Daemon

Stopping `ltid`, also stops robotic daemons, but `vmd` continues to run.

---

**Note** *This note applies only to NetBackup Enterprise Server.*

The ACS robotic processes (`acsssi` and `acssel`) also continue to run, since they are used by the ACS test utility and do not normally need to be stopped.

---

### ▼ To stop `ltid` from the NetBackup Administration Console

1. Notify users and operators that the system will be unavailable.
2. Check the Pending Requests list to ensure that no tapes are currently assigned. If any tapes are assigned, you should not stop the daemons.
3. Use **Actions > Stop/Restart Media Manager Device Daemon**.
4. *This step applies only to NetBackup Enterprise Server.*

In the dialog, the button 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.

Select a host.

5. Click **Stop** and **OK**.

## Automatic Volume Recognition Daemon (avrd)

This daemon handles automatic volume recognition and label scanning. This allows Media Manager to read labeled tape and optical disk volumes and assign the associated removable media requests to drives.

`avrd` is started when you start `ltid` and stops when you stop `ltid`. You do not have to start and stop it at any other times.

## Enterprise Media Manager (nbemm)

nbemm must be active to change the volume configuration, device configuration, storage unit configuration, and for any tape mount activity.

### ▼ To start nbemm

❖ Enter `/usr/opensv/netbackup/bin/nbemm`.

### ▼ To stop nbemm

❖ Enter `/usr/opensv/netbackup/bin/nbemm -terminate`.

## Media Manager Volume Daemon (vmd)

vmd enables remote device configuration and it is required for NetBackup 5.x servers to access nbemm running on a NetBackup 6.0 server.

### ▼ To start vmd

❖ Enter `/usr/opensv/volmgr/bin/vmd`.

### ▼ To stop vmd

❖ Enter `/usr/opensv/volmgr/bin/vmctrldbm -t`.

## Media Manager Status Collection Daemon (vmgcd)

vmgcd maintains a persistent connection with 5.x servers and communicates with them using Media Manager protocols. The main purpose of vmgcd is to keep the EMM database up-to-date with the actual status of drives attached to NetBackup 5.x servers.

vmgcd is started by nbemm on the same host as the EMM server if and only if there are one or more NetBackup 5.x servers present in the configuration.

vmgcd performs the following tasks:

- ◆ Collects the drive status of NetBackup 5.x servers and updates the EMM database if required.
- ◆ Accepts commands from the EMM server and sends them to NetBackup 5.x servers. Examples of these commands are DA reserve/release drive, assign/de-assign drive, DA re-register, and stop local scan.



- ◆ Allocates/de-allocates the drives attached to NetBackup 5.x servers in the EMM database whenever they get assigned/de-assigned.
- ◆ Updates the robot state in the EMM database whenever the robot state changes.

## Robotic Daemons

The following table lists the robotic daemons and robotic control daemons (if applicable) for each robot type. For more information about these daemons, see the *VERITAS NetBackup Commands for UNIX and Linux*.

Robotic and Robotic Control Daemons

Robot	Daemon	Description	Note
Automated Cartridge System (ACS)	acsd	This daemon runs on a Media Manager server and communicates mount, unmount, and robot inventory requests to the ACS Storage Server Interface process. This process communicates with the ACS library software server that controls the ACS robotics.	Applies only to NetBackup Enterprise Server.
Optical Disk Library (ODL)	odld	This daemon runs on a Media Manager server that has an Optical Disk Library. odld receives requests to mount and unmount volumes, or for robot inventory, and communicates these requests to the robotics through a SCSI interface.	ODL is supported only on UNIX servers.
Tape Library DLT (TLD)	tldd tldcd	<p>The robotic daemon (tldd) runs on each Media Manager server that has a drive in a Tape Library DLT. This daemon receives requests to mount and unmount volumes and sends these requests to the robotic control daemon (tldcd).</p> <p>tldcd runs on the Media Manager server that has the robotic control, accepts mount, dismount, and robot inventory requests and communicates with the Tape Library DLT robotics through a SCSI interface.</p>	

## Robotic and Robotic Control Daemons (continued)

Robot	Daemon	Description	Note
		Drives in the same robot may be configured on different hosts.	Applies only to NetBackup Enterprise Server.
Tape Library 4MM (TL4)	tl4d	This daemon runs on a host that has a Tape Library 4MM. tl4d receives requests to mount and unmount volumes, or for robot inventory, and communicates these requests to the robotics through a SCSI interface.	
Tape Library 8MM (TL8)	tl8d tl8cd	The robotic daemon (tl8d) runs on each Media Manager server that has a drive in a Tape Library 8MM. This daemon receives requests to mount and unmount volumes and sends these requests to the robotic control daemon (tl8cd).  tl8cd runs on the Media Manager server that has the robotic control, accepts mount, dismount, and robot inventory requests and communicates with the Tape Library 8MM robotics through a SCSI interface.	
		Drives in the same robot may be configured on different hosts.	Applies only to NetBackup Enterprise Server.
Tape Library Half-inch (TLH)	tlhd tlhcd	The robotic daemon (tlhd) runs on each Media Manager server that has a drive in a Tape Library Half-inch. This daemon receives requests to mount and unmount volumes and sends these requests to the robotic control daemon (tlhcd).  tlhcd runs only on the Media Manager server that has the robotic control, receives mount or dismount requests from tlhd, and communicates with the IBM Automated Tape Library Software, which controls a library, such as an IBM 3494.	Applies only to NetBackup Enterprise Server.



## Robotic and Robotic Control Daemons (continued)

Robot	Daemon	Description	Note
Tape Library Multimedia (TLM)	tlmd	This daemon runs on a Media Manager server and communicates mount, unmount, and robot inventory requests to an ADIC DAS/SDLC server, which controls the robotics, such as a Grau Automated Media Library (AML).	Applies only to NetBackup Enterprise Server.
Tape Stacker Half-inch (TSH)	tshd	This daemon runs on a Media Manager server that has a Tape Stacker Half-inch. tshd receives requests to mount and unmount volumes, or for robot inventory, and communicates these requests to the robotics through a SCSI interface.	

## Starting and Stopping Robotic Daemons

Starting `ltid` (the device daemon) also starts the robotic daemons for all configured robots. Stopping `ltid` also stops robotic daemons.

Once started, a robotic daemon can be in an UP or DOWN state. When a connection is made to the appropriate robot, the corresponding daemon is in the UP state and can mount or unmount tapes (or platters). If the connection cannot be made or if errors exist, the daemon moves to the DOWN state. Even in the DOWN state, the daemon is still running and automatically returns to the UP state when the connection is made or problems no longer exist.

*The following point applies only to NetBackup Enterprise Server.*

The ACS robotic processes (`acsssi` and `acsse1`) continue to run, since they are used by the ACS test facility and do not normally need to be stopped.

### ▼ To start robotic daemons in verbose mode

- ❖ Use the `-v` option on the command for the daemon or start `ltid` with the `-v` option. This option logs debug information through the system log and should only be used when required for debugging, since it can use large amounts of disk space to log the extra information.

### ▼ To start robotic daemons independently of `ltid`

- ❖ Enter `/usr/openv/volmgr/bin/daemon_name [-v] &`.



▼ **To stop a robotic daemon without stopping ltid**

1. Determine the process ID for the daemon using the vmps script.

```
/usr/opensv/volmgr/bin/vmps | grep daemon_name.
```

See “Displaying Process Status using the vmps Script” on page 271” for information on using this script.

2. Use the kill command with the process ID from step 1.

```
kill daemon_pid_#.
```

▼ **To stop robotic control daemons**

Use one of the following commands. You can also stop these daemons using the kill command.

```
❖ /usr/opensv/volmgr/bin/tl8cd -t.
```

```
❖ /usr/opensv/volmgr/bin/tldcd -t.
```

```
❖ /usr/opensv/volmgr/bin/tlhcd -t.
```

## Displaying Process Status using the vmps Script

The vmps script shows the Media Manager daemon processes that are active. You can execute this script using the following command:

```
/usr/opensv/volmgr/bin/vmps
```

In the following sample display, the second column contains the process IDs for the processes.

root	303	0.0	0.2	136	264	?	S	Feb 11	4:32	ltid -v
root	305	0.0	0.0	156	0	?	IW	Feb 11	0:54	vmd -v
root	306	0.0	0.0	104	0	?	IW	Feb 11	0:15	tl8d -v
root	307	0.0	0.0	68	56	?	S	Feb 11	12:16	avrd
root	310	0.0	0.0	116	0	?	IW	Feb 11	0:07	tl8cd -v

**Note** nbemm status is not shown in the output of vmps. nbemm status is shown in the output of the bpps script. Execute the bpps script using the following command:

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



## Logging of Errors

With the exception of nbemm, robotic errors and network errors are logged using syslogd. nbemm logs to VERITAS Unified Logging (VxUL). See the *VERITAS NetBackup Troubleshooting Guide for UNIX, Windows, and Linux* for more information.



If you are not using NetBackup or Storage Migrator, or you want to troubleshoot or test Media Manager, you can manually request Media Manager to mount and remove specific volumes by using the commands found in this chapter.

This chapter includes the following topics:

- ◆ Requesting Tapes
- ◆ Reading and Writing Tape Files
- ◆ Removing Tape Files
- ◆ Using an Optical Disk
- ◆ External Access to Media Manager Controlled Devices
- ◆ User Error Messages

### Requesting Tapes

The `tpreq` command allows you to request a tape of a particular density and specify various options, such as the access mode. This command reserves a single drive and creates a file in the current working directory (unless a full path is specified). The file acts as a symbolic link to the tape and all subsequent access to the tape is through this file name. Users do not have to be concerned with the full path to a specific device file.

The information you supply on the `tpreq` command is required for use by the Media Manager device daemon and used to validate all access requests to the tape file.

For all types of tapes, the tape is actually mounted and assigned when you enter the `tpreq` command.

By default, the drive assigned is one which supports DLT cartridge tapes, using the density `dlt`. You can use the `density` option on `tpreq` to request a drive that supports another density. See the `Density` field in the table in “Pending Requests Pane” on page 243 for a list of supported densities and drive types.



The density for the physical write is not selected automatically on drives. It is requested, so an operator can satisfy the correct drive. Density is determined by the `/dev` device name that was used when the drive was added to the Media Manager configuration or by the buttons selected on the drive.

A `tpreq` command must include a media ID and a file name. If the tape volume is associated with a volume pool (configured using Media Manager), the name of the volume pool may also be specified using the `-p` parameter. If the pool name is specified, the name will be validated against the pool name associated with the media in the EMM database.

See `tpreq` in the *VERITAS NetBackup Commands for UNIX and Linux* for more information.

## drive\_mount\_notify Script

When a `tpreq` command is executed, a call is made to execute the `drive_mount_notify` script immediately after the media has been successfully placed in a pre-selected drive.

This script allows user special-handling to occur at this point. Control is then returned to NetBackup to resume processing. The script is only called from the `tpreq` command for drives that are in robots and is not valid for standalone drives.

This script is located in the `/usr/opensv/volmgr/bin/goodies` directory. If you wish to use this feature, this script should be activated and put into the `/usr/opensv/volmgr/bin` directory.

Usage information is documented within the script.

## tpreq Example

The following sample `tpreq` command reserves a tape drive and creates a symbolic tape file:

```
/usr/opensv/volmgr/bin/tpreq -f tape1 -m jlr01 -a w -d qscsi
```

This command creates a file named `tape1` in the current working directory and links the file to the drive containing the tape volume having the media ID of `JLR01`. The access mode for the tape file is set to write and a 1/4-inch cartridge drive is assigned.

## Reading and Writing Tape Files

Reading or writing tape files involves copying the file from tape to disk or from disk to tape. To perform read or write operations, use one of the UNIX commands that performs input/output operations, for example `tar` or `mt`.



## Positioning Tape Files

The `mt` command positions tape files by skipping forward or backward according to tape marks. The following table shows the options available on the `mt` command for positioning tapes and how they affect tape files.

mt Option	Operation
<code>eof, weof</code>	Writes end-of-file tapemarks at the current position on the tape according to the count option on <code>mt</code> .
<code>fsf, bsf</code>	Spaces forward or backward the number of tapemarks on the count option.
<code>fsr, bsr</code>	Spaces forward and backward the number of records according to the count option on <code>mt</code> . <code>bsr</code> is only supported for the undefined record type.

The following example uses `mt` to skip forward three files on a tape:

```
mt -f tape1 fsf 3
```

## Rewinding Tape Files

When a file is rewound, it is positioned to the beginning of the data. To rewind a tape file, you can use the `mt` command.

The following command causes rewinding of tape file `tape1`. `tape1` is positioned to the beginning of the tape volume associated with the file:

```
mt -f tape1 rewind
```

The count option is not used for the rewind operation. If a count is specified, it is ignored.

## Removing Tape Files

When you have completed reading or writing tape files, use the `/usr/opensv/volmgr/bin/tpunmount` command to end the assignment of the tape file. This command removes from the directory the tape file you created using `tpreq` and causes the tape volume to be removed from the tape drive. Using `tpunmount` is required for each file created by a `tpreq` command.

See `tpunmount` in the *VERITAS NetBackup Commands for UNIX and Linux* for more information.



## drive\_unmount\_notify Script

When a `tpunmount` command is executed, a call is made to execute the `drive_unmount_notify` script.

This script allows user special-handling to occur at this point. Control is then returned to NetBackup to resume processing. The script is only called from the `tpreq` command for drives that are in robots and is not valid for standalone drives.

This script is located in the `/usr/opensv/volmgr/bin/goodies` directory. If you wish to use this feature, this script should be activated and put into the `/usr/opensv/volmgr/bin` directory.

Usage information is documented within the script.

## Using an Optical Disk

An optical disk cannot be used in the same ways that a tape can. It does have many similarities to a tape and takes advantage of the automation provided by Media Manager: optical disks allow automatic volume recognition, and they can be mounted and moved by a robot.

Optical disks work well with VERITAS storage management applications. These applications use databases to handle location information (offsets, capacity, and so forth) that would otherwise have to be done by the user. A user who is willing to keep track of such information can access an optical disk using the following tape commands.

In the following example, a user performs two `tar` operations to an optical disk, then lists the second `tar` image.

1. A rewritable optical disk is requested, as follows.

```
tpreq tape -m XXX01A -d odiskwm -p NetBackup
```

2. The first `tar` is performed, starting at the beginning of the disk.

```
tar -cvf - /home/arh | dd of=tape ibs=10240 obs=10240
0+473 records in
189+0 records out
```

3. The second `tar` is performed, starting at the end of the previous data. The records out information is used for the `oseek` parameter.

```
tar -cvf - /home/arh/.cshrc | dd of=tape ibs=10240 obs=10240
oseek=189
```

4. The disk is unmounted, as follows.

```
tpunmount tape
```

5. The optical disk is requested again.

```
tpreq tape -m XXX01A -d odiskwm
```

6. The second tar image is listed. To access the data, the user must know where it is located for the `iseek` parameter.

```
dd if=tape ibs=10240 obs=10240 iseek=189 | tar -tvf -  
rw-r--r--357/110 2386 Jul 9 14:01 1992  
/home/arh/.cshrc
```

7. The disk is unmounted, as follows.

```
tpunmount tape
```

## External Access to Media Manager Controlled Devices

The device daemon (`ltid`) restricts access to Media Manager controlled drives that are in an up state, by changing the permissions of the device files for those drives. The permissions are changed to 0600 when `ltid` starts and back to their original settings when `ltid` is terminated (or when a drive's state is changed to DOWN).

Do not modify the permissions of these device files when `ltid` is active. To ensure reliable operation, only users that use the `tpreq` and `tpunmount` commands, or the `drive_mount_notify` and `drive_unmount_notify` callout scripts, explained in this chapter can have access to a drive that is up under `ltid` control.

The following example uses `tpreq`:

```
tpreq tape -m xxx -d 4mm -f /tmp/tape  
/bin/tar -cvf /tmp/tape files  
tpunmount /tmp/tape
```

Users that do not use `tpreq` and `tpunmount` or the callout scripts to access drives that are in the up state may encounter both access and data reliability problems. These problems occur because the Media Manager `avrd` daemon periodically attempts to rewind and read data from media in drives that are up and are not currently assigned.

A user that is unable to use `tpreq` and `tpunmount` must do one of the following actions before attempting to access the drive:

- ❖ Down the drive prior to accessing it.



- ❖ Terminate `ltid` by executing `stopltid` and then restart `ltid` after accessing the drive.

## User Error Messages

See the Device Management Status Codes section of the *VERITAS NetBackup Troubleshooting Guide for UNIX, Windows, and Linux* for errors returned from user tape commands.

## Shared Storage Option (SSO) Topics

## 8

The Shared Storage Option (SSO) is a separately licensed and priced VERITAS NetBackup software option. SSO runs on Windows and UNIX (including Linux) media servers (see “Supported Media Servers for SSO” on page 285) that has NetBackup installed.

This software option is the Shared Drives option and the license key used to enable it is the Shared Storage Option key. The Shared Storage Option is available with both NetBackup Server and NetBackup Enterprise Server. SSO is needed in a NetBackup Server environment only if there are shared drives for multiple attach hosts. For example, NDMP attach hosts sharing one or more drives.

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 297).

This chapter contains the following topics:

- ◆ “What is SSO?” on page 279
- ◆ “Configuring and Verifying Your SSO Hardware” on page 281
- ◆ “Installing the Shared Storage Option” on page 284
- ◆ “Configuring SSO in NetBackup” on page 287
- ◆ “Using Media Manager with SSO” on page 292
- ◆ “Troubleshooting SSO Issues” on page 294
- ◆ “SSO Reference Topics” on page 298

### 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 299). 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**

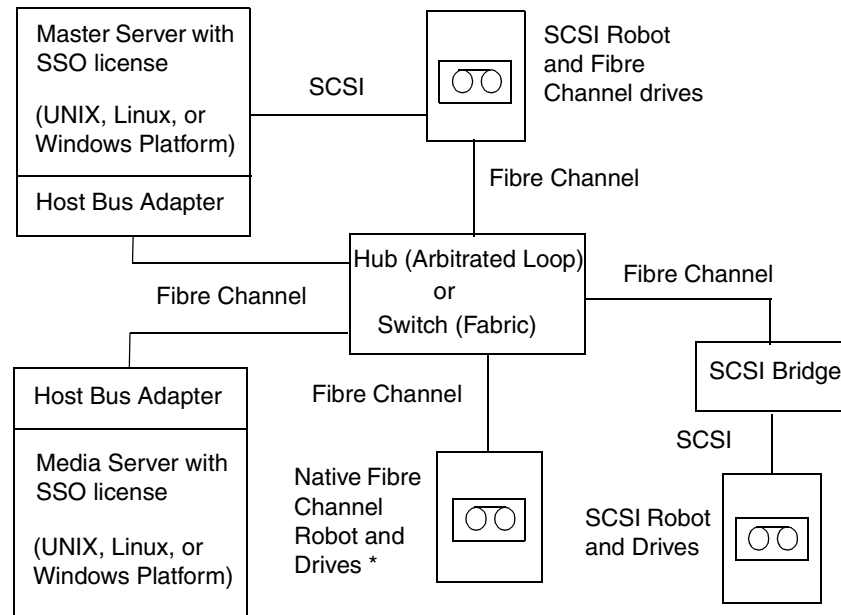
SSO provides the management and coordination tools necessary to effectively share tape resources in a SAN. SSO was designed to work with fibre channel networks, but it can also be applied to environments that use SCSI switches or multi-initiator configurations. SAN fibre is not required to use SSO.

## **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 or Linux 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 363 for information on replacing devices in an existing SSO configuration.



## Using the Media Manager Device Configuration Guide

See the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for information on installing and configuring drivers, and modifying the appropriate system configuration files.

The configuration tasks explained in this 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 or Linux 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* 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 (select **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 `bpc1ntcmd` utility to resolve IP addresses into host names. See the *VERITAS NetBackup Troubleshooting Guide for UNIX, Windows, and Linux* and the *VERITAS NetBackup Commands for UNIX and Linux* or the *VERITAS NetBackup Commands for Windows* 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 286).
- ◆ See the appropriate chapter in the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for more information and examples (the chapters in this 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 284
- ◆ “Enterprise Media Manager (EMM) Device Allocator Requirements” on page 285
- ◆ “Supported Robot Types for SSO” on page 285
- ◆ “Supported Media Servers for SSO” on page 285
- ◆ “SSO Restrictions and Limitations” on page 286
- ◆ “SSO Installation” on page 287

## 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 39 for information about mixed NetBackup server environments.



## Enterprise Media Manager (EMM) Device Allocator Requirements

The host that is defined as the Enterprise Media Manager (EMM) server (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 server.

Host Requirements
It must be network-accessible from all hosts that are sharing drives managed by the device allocation host.
The EMM server must be at the same or greater level of NetBackup as the media servers that it services. However, if there are any NDMP controlled devices in your configuration, then the EMM server and all media servers must be at NetBackup 6.0.
VERITAS Host Recommendations
Use the NetBackup master server as the common EMM server for your configuration.
Configure the EMM server as a Highly Available host.
Use a relatively high-powered server for your EMM server.

## 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* and the NetBackup release notes for information on the supported operating system levels for these server platforms.



- ◆ Sun Solaris
- ◆ IBM AIX
- ◆ Hewlett-Packard HP-UX
- ◆ Hewlett-Packard Tru64
- ◆ Enterprise Linux
- ◆ Microsoft Windows 2000, 2003

## SSO Restrictions and Limitations

- ◆ SSO can be used to share drives which are NDMP-controlled. However, drives which are NDMP-controlled by any host must have all control hosts at NetBackup 6.0 or higher.
- ◆ 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 285 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.
- ◆ 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 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 *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I*.

You can check keys by using the license key dialog 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 287), and also configure storage units and backup policies (see “Configuring NetBackup Storage Units and Backup Policies” on page 288).

### Configuring SSO Devices in Media Manager

Using the Device Configuration wizard is recommended and is the easiest method for configuring shared drives. This wizard guides you through the steps involved in configuring drives that will be shared.

You can only use the Device Configuration wizard to configure devices on the media servers listed in “Supported Media Servers for SSO” on page 285.

See “Why You Should Use the Media Manager Wizards” on page 47 and “Adding Shared Drives” on page 60.



Also see “The Device Configuration Wizard” on page 48 for more information about this wizard.

There are also alternate ways to configuring SSO. See “Using Alternate Interfaces to Configure Shared Drives” on page 61.

## 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 *VERITAS NetBackup System Administrator's Guide for UNIX and Linux, Volume I* or the *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* for more 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. When configuring storage units, you can select a single media server, or you can allow the EMM server to select the media server to use at the time of backup. For example, you can configure a single storage unit that can be used by any media server that shares the storage unit.

### 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 same robot drive 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 a Shared Storage Option (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/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.

1. Execute `tpconfig -d` or `tpconfig -dl` and `scan`. For NDMP devices, use `tpautoconf -probe -ndmp_host_name <host list>`.



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.

Id	DriveName	Type	Residence	Status
	Drive Path			
*****				
0	QUANTUMDLT70000	dlt	TLD(0) DRIVE=5	
	/dev/st/nh3c0t510			UP
1	QUANTUMDLT70001	dlt	TLD(0) DRIVE=6	
	/dev/st/nh3c0t110			UP

Currently defined robotics are:

```
TLD(0)      robotic path = /dev/sg/h3c0t010,
EMM server = norway
```

3. The output from the robot section of `scan` shows the same address for the robot (/dev/sg/h3c0t010), 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/nh3c0t110"
Passthru Name: "/dev/sg/h3c0t110"
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 293.

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 294.



## Using the Device Monitor with SSO

See the following related Device Monitor topics:

- ◆ “The Drive Status Pane” on page 293
- ◆ “Changing the Operating Mode for a Shared Drive” on page 293
- ◆ “Adding or Changing a Comment for a Shared Drive” on page 293
- ◆ “Performing Drive Cleaning Functions for a Shared Drive” on page 293
- ◆ “Shared Storage Option Summary Reports” on page 294

### The Drive Status Pane

This display contains columns that are of note for shared drives. For example, **Control** and **Drive Index**.

See “Drive Status Pane” on page 236 for more details.

### Changing the Operating Mode for a Shared Drive

For a shared drive, the change mode dialog contains a list of all host/device paths to the selected drive. You can choose any number of host/device paths where the mode change will apply.

See “Changing the Operating Mode of a Drive” on page 249 for more details.

### Adding or Changing a Comment for a Shared Drive

For a shared drive, the change drive comment dialog contains a list of all host/device paths to the selected drive and the current drive comment for each combination. You can choose any number of host/device paths where the change will apply.

See “Adding or Changing a Drive Comment” on page 253 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.



Drive Cleaning Function	Shared Drive Usage
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 251 for more details.

## Shared Storage Option Summary Reports

These reports contain Media Manager information about your SSO configuration, including the drives and hosts.

See “Shared Storage Option Summary Reports” on page 261.

## 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 387 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 294 and “Media Manager Configuration Guidelines” on page 295).
- ◆ Operating system references (“Operating System Help” on page 296).
- ◆ Common problems (“Common Configuration Issues with SSO” on page 296).
- ◆ FAQs that may help you resolve any SSO issues (“Frequently Asked Questions About SSO” on page 297).

## 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 Device Configuration wizard to configure SSO.
- ◆ When 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.

## 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 or Linux servers only).
- ◆ The *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

## 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 dialog available from the NetBackup **Help** menu on Windows, UNIX, and Linux 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 robot control host 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 Device Configuration wizard. This wizard has 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, or did not define a storage unit that allows any media servers.
- ◆ 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 or Linux servers only)
- ◆ See the Sun chapter of the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* 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 character.

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 286).

**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 NetBackup SSO use IP protocol or SCSI protocol?**

Both. IP protocol is used to provide coordination between servers. SSO uses SCSI protocol (SCSI reserve/release) as an added layer of protection.

## 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. For drives attached to NDMP hosts, each NDMP attach host is considered an additional host for purposes of SSO.

#### 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.

## Sharing Robotic Libraries Without Using SSO

You can share robotic tape libraries among multiple Media Manager servers using any of the following methods. These capabilities are not related to SSO and should not be confused with SSO.

- ◆ NetBackup allows different drives within the same physical robotic library to be configured on different media servers. This capability is termed *shared library support*. Robot types that support this are ACS, TL8, TLD, TLH, TLM.

TL8 and TLD robots also support library partitioning. One partitioned view of the robotic library includes one set of drives, while the other view has another set of different drives in the library. The partitioning helps two robotic control daemons on different control hosts manage the robotic library—each for a different NetBackup master and media server environment.

- ◆ Use multiple NetBackup master servers that share a common media and device management domain. This means that the master servers are using the same EMM server.

## 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. `nbemm` is the Enterprise Media Manager. A major function of `nbemm` is to manage media information. An additional function that `nbemm` provides is to be the device allocator (DA) for shared drives. In this case, `nbemm` is known as `nbemm/DA`.

### **nbemm/DA**

To coordinate network-wide allocation of tape drives, `nbemm/DA` acts as a central clearing agent for all NetBackup and Storage Migrator shared tape requests in a storage area network. `nbemm/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).

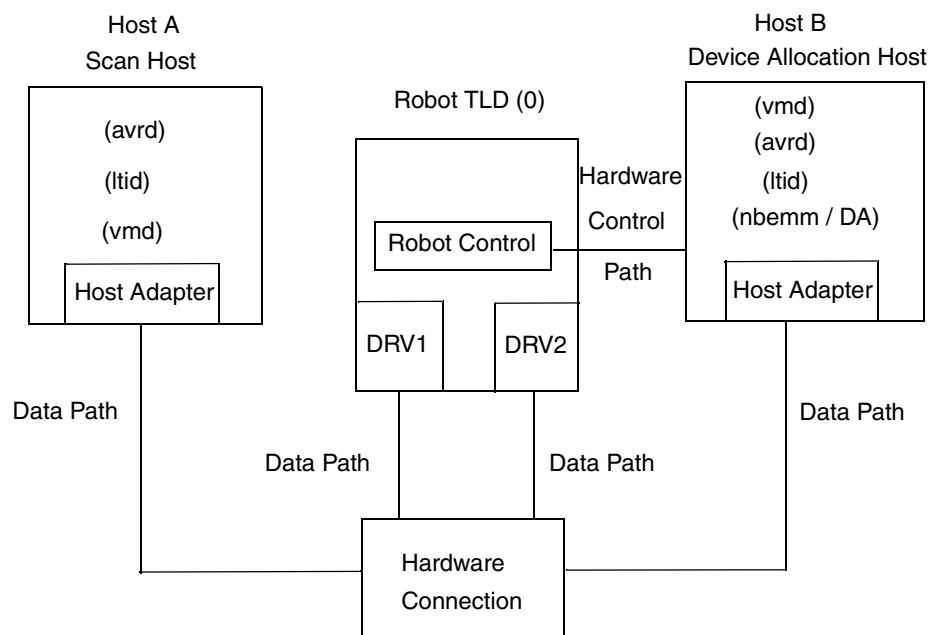


For shared drive configurations, the host that is configured as the EMM server for a drive in a robot or a standalone drive is also known as the device allocation host (see “Device Allocation Host” on page 302). This is the host where `nbemm/DA` resides. Other hosts in the configuration have `nbemm` without device allocator functionality being utilized.

`nbemm/DA` maintains shared drive and host information, such as a list of hosts that are online and available 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).

### Example SSO Configuration Showing Media Manager Components

The following figure shows an example of a shared drive configuration with Media Manager components. See the *VERITAS NetBackup Troubleshooting Guide for UNIX, Windows, and Linux* for a process flow diagram of SSO components.



In this figure, Host A is

- ◆ Connected to drives DRV1 and DRV2 through enabling hardware.
- ◆ The first host in the environment to come online with a non-zero scan ability will be the initial scan host for its drives (see “Scan Host” on page 301).

In this figure, Host B

- ◆ Is connected to drives DRV1 and DRV2 through enabling hardware.



- ◆ Is configured to be the EMM server and by default is also the device allocation host (see “Device Allocation Host” on page 302). `nbemm/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.

Prior to NetBackup release 6.0, instances of `ltid` on hosts that were *not* scan hosts created `rdevmi` (remote device management interface) processes on the scan hosts. These processes communicated with the other hosts sharing the drive, and ran on the scan hosts as slave processes of the non-scan hosts' `ltid`. In NetBackup release 6.0, instances of `rdevmi` running on NetBackup 5.x servers communicate through a proxy with the EMM server. These processes receive drive status information from the EMM server. This status information is used to maintain the shared drive information centrally in the EMM database.

### How the Scan Host is Determined

Any drive that is not being locally scanned has the same scan host, the EMM server.

Scan hosts are determined by `nbemm/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 294) that comes online for each shared drive with `nbemm/DA` becomes the initial scan host for that drive.

All device hosts that register with `nbemm/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, the drive path, or the network goes down.
- ◆ The drive is logically placed in the Down mode.

A new scan host is then chosen by `nbemm/DA`. 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.



### **Drive Paths for the Scan Host**

If a drive has multiple paths configured on the selected scan host, nbemm/DA will select a scan path as follows:

1. The first local device path it finds in its database in the UP state.
2. The first NDMP-attached drive path it finds in its database in the UP state.

### **Device Allocation Host**

The device allocation host is another name for the EMM server, when the EMM server performs tasks in support of SSO. This host is also the host where nbemm/DA runs and manages the following:

- ◆ All drive allocations
- ◆ All configured devices
- ◆ All media servers and their current status (online, offline).

## Media Manager Reference Topics

---

## A

You may find the following reference and conceptual topics useful when using Media Manager:

- ◆ “NetBackup Media Manager Best Practices” on page 304
- ◆ “Allowable Media Manager Characters” on page 308
- ◆ “Robot Overview” on page 308
- ◆ “Frequently Asked Questions About Device Discovery” on page 321
- ◆ “How NetBackup Uses SCSI Reserve/Release” on page 324
- ◆ “Using TapeAlert” on page 332
- ◆ “Correlating Device Files to Physical Drives When Adding Drives” on page 336
- ◆ “Drive Cleaning” on page 339
- ◆ “Volume Pools and Volume Groups” on page 344
- ◆ “Barcodes” on page 350
- ◆ “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354
- ◆ “Making Changes to Your Hardware Configuration” on page 363
- ◆ “Labeling Media” on page 369
- ◆ “Mounting and Unmounting of Media” on page 370
- ◆ “Suspending Media Or Downing Devices” on page 370
- ◆ “How Media Manager Selects a Drive for a Robotic Mount Request” on page 370
- ◆ “How NetBackup Selects Media in Robots” on page 371
- ◆ “How NetBackup Selects Media in Standalone Drives” on page 373
- ◆ “Media Formats” on page 375
- ◆ “Media Manager Security” on page 378
- ◆ “Administrators Quick Reference” on page 383
- ◆ “The Media Manager Configuration File (vm.conf)” on page 387



## 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 304
- ◆ “Enterprise Media Manager Domain Management” on page 305
- ◆ “Media Management” on page 305
- ◆ “Device Management” on page 306
- ◆ “Performance and Troubleshooting” on page 307
- ◆ “Other Best Practices” on page 307

Visit the VERITAS support web site (<http://support.veritas.com>) for a list of supported devices, server platforms, and the latest device mapping file.

### 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 master servers' databases. You may also want to backup the configuration settings stored in the vm.conf and bp.conf files on your media servers.
- ◆ When restoring NetBackup databases (for example, master server databases and the EMM database), the backups must all be from the same point in time.
- ◆ If you want to use devices with some other application and these devices are currently being controlled by Media Manager, you must do one of the following to avoid potential loss of data:
  - ◆ Use the Media Manager commands, `tpreq` to mount media on a drive and `tpunmount` to remove media from the drive. Using these commands will allow you to get control of the device when Media Manager is finished with the device.





- ◆ Down the drive, if the drive is in the Media Manager UP state.

## Enterprise Media Manager Domain Management

- ◆ Users cannot share devices or volumes between EMM Domains.
- ◆ Media IDs must be unique within a given EMM Domain.
- ◆ Barcodes must be unique within a given EMM Domain.
- ◆ Drive Names must be unique within a given EMM Domain and should be descriptive.
- ◆ Robot Numbers must be unique within a given EMM Domain.
- ◆ Host names should be consistent throughout an EMM 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 EMM server should be one of the NetBackup master servers and there should be only one EMM server per domain.
- ◆ 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.*

- ◆ A NetBackup master server running release 6.0 supports media servers running NetBackup release 5.0 and later. NetBackup 5.x media servers communicate with the NetBackup 6.0 master server using proxy services.

---

**Note** Because NetBackup 6.0 allocates drives prior to starting jobs on the media server, it is possible for NetBackup 6.0 media servers to pre-empt drive selections on NetBackup 5.x media servers. To optimize resource allocation in your environment, update all media servers to release 6.0.

---

## 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* before configuring devices on media servers (or SAN media servers).
- ◆ Use only tested robots. See the NetBackup hardware compatibility list on the VERITAS support site.
- ◆ 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 fully-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.
- ◆ Use the device configuration wizard to configure your devices for use with NetBackup.
- ◆ 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 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.

## Performance and Troubleshooting

- ◆ Use the performance-tuning documents available on the VERITAS support web page.
- ◆ Use only a dedicated backup server (not an application or file server) for the Enterprise Media Manager (EMM) server and master servers. Plan periodic maintenance periods for all of your backup servers.
- ◆ Consult the *VERITAS NetBackup Troubleshooting Guide for UNIX, Windows, and Linux* 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 279 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 *VERITAS NetBackup Vault System Administrator's Guide for UNIX, Windows, and Linux*.
- ◆ 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 *VERITAS NetBackup Vault System Administrator's Guide for UNIX, Windows, and Linux* for the best practices for NetBackup Vault.

## Allowable Media Manager Characters

The following set of characters can be used in user-defined names for NetBackup entities. You enter these names when creating these entities.

Some examples of user-defined names are: host names, drive names and comments, volume group names, volume pool names, and media IDs.

These same characters must also be used when specifying these items in languages other than English.

- ◆ Alphabetic (A-Z a-z).
- ◆ Numeric (0-9).
- ◆ Period (.).
- ◆ Plus (+).
- ◆ Minus (-). Do not use a minus as the first character.
- ◆ Underscore (\_).
- ◆ Spaces are only allowed in a comment for a drive.

## 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 related topics:

- ◆ “Media Manager Robot Types” on page 309
- ◆ “Media Manager Media Types” on page 310
- ◆ “Robot Attributes” on page 311
- ◆ “Table-Driven Robotics” on page 320
- ◆ “Robotic Test Utilities” on page 320



## 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.
ODL	Optical Disk Library	12	490	
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.
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.

Also see “Alternate Media Types” on page 311.

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



Media Type	Description
4MM_CLN	4MM cleaning tape
8MM_CLN	8MM cleaning tape
8MM2_CLN	8MM cleaning tape 2
8MM3_CLN	8MM cleaning tape 3
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 Robots

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, UNIX, and Linux. Windows servers require STK LibAttach software. See the VERITAS support web site for the latest compatibility information and obtain the appropriate LibAttach software from STK.





Attribute	NetBackup Server (ACS robots are not supported)	NetBackup Enterprise Server
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.
For More Information		See the ACS appendix, “STK Automated Cartridge System (ACS)” on page 483.

## ODL Robots

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.	



Attribute	NetBackup Server	NetBackup Enterprise Server
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 <i>VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux</i> .	

## TL4 Robots

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.



Attribute	NetBackup Server	NetBackup Enterprise Server
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 <i>VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux</i> .	

## TL8 Robots

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
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.	



Attribute	NetBackup Server	NetBackup Enterprise Server
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 <i>VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux</i> .	

## TLD Robots

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
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, UNIX, and Linux.	Windows, UNIX, and Linux.
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.	



Attribute	NetBackup Server	NetBackup Enterprise Server
Robot Examples	ADIC Scalar 1000 DLT, ATL D7000, STK L Series, and Overland Data Neo series	
For More Information	See the <i>VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux</i> .	

## TLH Robots

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
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, UNIX, and Linux.



Attribute	NetBackup Server (TLH robots are not supported)	NetBackup Enterprise Server
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 505.

## TLM Robots

Attribute	NetBackup Server (TLM robots are not supported)	NetBackup Enterprise Server
API Robot		Yes
SCSI Control		No
LAN Control		Yes
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



Attribute	NetBackup Server (TLM robots are not supported)	NetBackup Enterprise Server
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, UNIX, and Linux.
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 519.

## TSH Robots

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



Attribute	NetBackup Server	NetBackup Enterprise Server
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 <i>VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux</i> .	

## 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 39 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 `/usr/opensv/volmgr/bin/robtest` 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, 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.

## 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).
- ◆ ACS, TLM, and TLH robotics 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 the EMM database, which has data structures that are managed by the following:

- ◆ The NetBackup GUIs - used centrally
- ◆ Device configuration wizards - used centrally
- ◆ The `tpconfig` command - used locally on each media server
- ◆ An internal API

In addition to the primary attribute information needed to use devices, the EMM database contains discovered device attributes that are necessary for automatic correlation and for validation of consistency in the configuration. The EMM data base ensures consistency between drives, robotic libraries, storage units, media, and volume pools across multiple servers. The EMM server is defined at installation time and is unique for all media servers (or SAN media servers) sharing devices in a multiple server configuration. See “Enterprise Media Manager Domain Management” on page 305.

The NetBackup scheduling components use the information stored in the EMM database directly for selecting the server, drive path, and media for jobs. When `ltid` (the Media Manager device daemon on UNIX or the NetBackup Device Manager service on Windows servers) starts up, it reads device information from the EMM 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.

NetBackup can be configured to run an automated form of device discovery during `ltid` startup (which is the default behavior for Windows). This allows for detection and at least partial handling of differences between the actual device configuration and the device configuration as it is defined in the EMM database.

#### **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 without some user intervention. The Media Manager manual-based device configuration interfaces are still used in these cases.

However, with non-discoverable or non-serialized devices, automated device path correction at `ltid` startup time is limited.

#### **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 running the Device Configuration wizard. 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.

#### **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 (DA) manages scan host assignments for shared drives. 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. An alternative approach that leads to polling shared drives from multiple hosts could also become disruptive. The approach used by NetBackup reflects a balanced overall solution.

## 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 324
- ◆ “How NetBackup Uses SCSI Reserve/Release Commands” on page 326
- ◆ “Issuing Reset Commands to Break a Reservation” on page 330
- ◆ “Controlling SCSI Reserve/Release” on page 331
- ◆ “SCSI Reserve/Release Requirements and Limitations” on page 331

## Background Topics

The following topics explain a previous 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, Solaris, AIX, Tru64, Linux, and Windows servers.*

The NetBackup processes (`bptm`, `bprecover`, and `bpbackupdb`) 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 `bpexpdate` 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 or Linux 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* 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 or Linux 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, non-disabled tape device paths 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 `vmoprcmd` command:

```
vmoprcmd -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. The DA host is also the EMM server.

---

**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 *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for 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 328).

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.

## 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 or Linux `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, Linux, 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 > Enable SCSI Reserve/Release**.

## 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* 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 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* for instructions.

This VERITAS implementation using SCSI reserve/release has the following limitations:

- ◆ SCSI reserve/release is not applicable for NDMP drives (the NDMP filer is responsible for providing exclusive device access).
- ◆ 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 Advanced Client System Administrator's Guide*.



- ◆ 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 and those devices that were in use during the fail over must be made available without manual intervention, 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.

## Using TapeAlert

TapeAlert is a tape drive status monitoring and messaging utility. The TapeAlert utility can detect tape quality problems, defects in tape drive hardware, and the need to perform cleaning operations. For drives that support TapeAlert, the TapeAlert firmware monitors the drive hardware and the media. Error, warning, and informational states are logged on a TapeAlert log page. NetBackup writes TapeAlert conditions into the `bptm` log, the error log, the job details log, and the system log.

If you are using TapeAlert for cleaning drives, see “Reactive Cleaning (TapeAlert)” on page 340 for more information.

## Requirements for Using TapeAlert with Media Manager

To use TapeAlert, all of the following conditions must be true. No additional configuration is needed.

- ◆ 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.

- ◆ For drive cleaning using 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*).

## TapeAlert Log Codes

TapeAlert codes are derived from the T10 SCSI-3 Stream Commands standard. Refer to the device-specific SCSI manual for the list of codes supported by the device. TapeAlert checks for errors of the following types:

- ◆ Recoverable read and write drive problems
- ◆ Unrecoverable read and write drive problems
- ◆ Hardware defects
- ◆ Wrong or worn-out media
- ◆ Expired cleaning tapes
- ◆ Abnormal errors

A set of TapeAlert conditions are defined that can cause the media in use to be frozen. An additional set of conditions are defined that can cause a drive to be downed. .

<b>TapeAlert Code</b>	<b>Default Action</b>	<b>Error Type</b>	<b>Error Message</b>
0x01	None	Warning - WRN	READ WARNING
0x02	None	Warning - WRN	WRITE WARNING
0x03	None	Warning - WRN	HARD ERROR
0x04	Freeze media - FRZ	Critical - CRT	MEDIA
0x05	Freeze media - FRZ	Critical - CRT	READ FAILURE
0x06	Freeze media - FRZ	Critical - CRT	WRITE FAILURE
0x07	Freeze media - FRZ	Warning - WRN	MEDIA LIFE
0x08	Freeze media - FRZ	Warning - WRN	NOT DATA GRADE
0x09	None	Critical - CRT	WRITE PROTECT
0x0a	None	Informational - INFO	NO REMOVAL
0x0b	None	Informational - INFO	CLEANING MEDIA



<b>TapeAlert Code</b>	<b>Default Action</b>	<b>Error Type</b>	<b>Error Message</b>
0x0c	None	Informational - INFO	UNSUPPORTED FORMAT
0x0d	Freeze media - FRZ	Critical - CRT	REC. MECH. CARTRIDGE FAILURE
0x0e	Freeze media - FRZ	Critical - CRT	UNREC. MECH. CARTRIDGE FAILURE
0x0f	Freeze media - FRZ	Warning - WRN	MIC FAILURE
0x10	None	Critical - CRT	FORCED EJECT
0x11	None	Warning - WRN	READ ONLY
0x12	None	Warning - WRN	DIRECTORY CORRUPTED ON LOAD
0x13	Freeze media - FRZ	Informational - INFO	NEARING MEDIA LIFE
0x14	Clean drive - CLN	Critical - CRT	CLEAN NOW
0x15	Clean drive - CLN	Critical - CRT	CLEAN PERIODIC
0x16	None	Warning - WRN	EXPIRED CLEANING MEDIA
0x17	None	Warning - WRN	INVALID CLEANING TAPE
0x18	None	Warning - WRN	RETENSION REQUESTED
0x19	None	Warning - WRN	DUAL-PORT ERROR
0x1a	None	Warning - WRN	COOLING FAN FAILURE
0x1b	None	Warning - WRN	POWER SUPPLY FAILURE

<b>TapeAlert Code</b>	<b>Default Action</b>	<b>Error Type</b>	<b>Error Message</b>
0x1c	None	Warning - WRN	POWER CONSUMPTION
0x1d	None	Warning - WRN	DRIVE MAINTENANCE
0x1e	Down drive - DOWN	Critical - CRT	HARDWARE A
0x1f	Down drive - DOWN	Critical - CRT	HARDWARE B
0x20	None	Warning - WRN	INTERFACE
0x21	None	Critical - CRT	EJECT MEDIA
0x22	None	Warning - WRN	DOWNLOAD FAIL
0x23	None	Warning - WRN	DRIVE HUMIDITY
0x24	None	Warning - WRN	DRIVE TEMPERATURE
0x25	None	Warning - WRN	DRIVE VOLTAGE
0x26	None	Critical - CRT	PREDICTIVE FAILURE
0x27	None	Warning - WRN	DIAGNOSTICS REQ.
0x28 - 0x31	None	None	UNDEFINED
0x32	None	Warning - WRN	LOST STATISTICS
0x33	Freeze media - FRZ	Warning - WRN	DIRECTORY INVALID ON UNLOAD
0x34	Freeze media - FRZ	Critical - CRT	SYSTEM AREA WRITE FAILURE
0x35	Freeze media - FRZ	Critical - CRT	SYSTEM AREA READ FAILURE
0x36	Freeze media - FRZ	Critical - CRT	NO START OF DATA
0x37	Freeze media - FRZ	Critical - CRT	LOADING FAILURE



<b>TapeAlert Code</b>	<b>Default Action</b>	<b>Error Type</b>	<b>Error Message</b>
0x38	Freeze media - FRZ	Critical - CRT	UNREC. UNLOAD FAILURE
0x39	None	Critical - CRT	AUTOMATION INTERFACE FAILURE
0x3a	None	Warning - WRN	FIRMWARE FAILURE
0x3b	Freeze media - FRZ	Warning - WRN	WORM MEDIUM - INTEGRITY CHECK FAILED
0x3c	Freeze media - FRZ	Warning - WRN	WORM MEDIUM - OVERWRITE ATTEMPTED
0x3d - 0x40	None	None	UNDEFINED

## 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 279 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 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.
2. Determine the physical drive address (for example, number) by checking labels on the robot.
3. 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 set of SCSI coordinates.
4. 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: [5,0,0,0]

Drive 2: [5,0,1,0]

Drive 3: [5,0,2,0]

Also assume that in step c you requested that the tape be mounted on Drive 1. If the SCSI coordinates for the drive are 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 SCSI coordinates for that drive are 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 SCSI coordinates for Drive 2



are incorrect. Replace the Drive 2 SCSI coordinates [5,0,1,0] with the correct SCSI coordinates [5,0,2,0] for Drive 3. In this case, you also know that the SCSI coordinates for Drive 3 are incorrect. Possibly, the SCSI coordinates 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 contains the following drive cleaning topics:

- ◆ "Available Types of Cleaning" on page 340
- ◆ "Reactive Cleaning (TapeAlert)" on page 340
- ◆ "Library-Based Cleaning" on page 341
- ◆ "Frequency-Based Cleaning" on page 341
- ◆ "Operator-Initiated Cleaning" on page 343
- ◆ "Using a Cleaning Tape" on page 343



## 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 340.
- ◆ 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 341.
- ◆ 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 341.
- ◆ 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 343.

## 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, `bptm` 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 341 and “TapeAlert and Frequency-Based Cleaning” on page 341).

See the following related topics:

- ◆ “Requirements for Using TapeAlert with Media Manager” on page 332
- ◆ “TapeAlert and Media Manager” on page 341
- ◆ “TapeAlert and Frequency-Based Cleaning” on page 341

## 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 bptm 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 EMM 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 311).
- ◆ 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.

### Frequency-Based Cleaning Limitations

*The following applies only to NetBackup Enterprise Server.*

Frequency-based cleaning is *not* supported for drives in ACS 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.

Check the Drive Cleaning Support Attribute of the tables in “Robot Attributes” on page 311.

### 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 251.
- ▼ **To change the number of cleanings allowed for a cleaning tape**
  - ❖ See “Changing the Attributes for a Volume” on page 163 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 EMM 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 or CLEAN\_PERIODIC 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 342.

## 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 342.



## 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 related topics:

- ◆ “Volume Pools” on page 344
- ◆ “Volume Groups” on page 344
- ◆ “Volume Pool and Volume Group Example” on page 345
- ◆ “Scratch Volume Pools” on page 347
- ◆ “Moving Volumes” on page 349

### 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 users, groups, or applications. You can create volume pools for user groups 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 CatalogBackup, 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 None, NetBackup, CatalogBackup 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 347).

### 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:

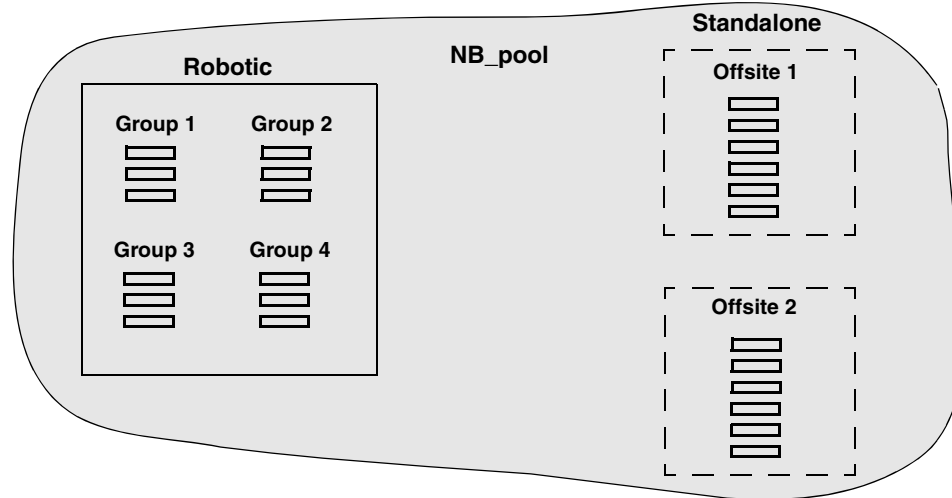
- ◆ All volumes in a group must be the same media type.  
However, a media type and its corresponding cleaning media type are allowed in the same volume group (for example, DLT and DLT\_CLN).
- ◆ All volumes in a robotic library *must* belong to a volume group. You cannot add volumes to a robotic library 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.



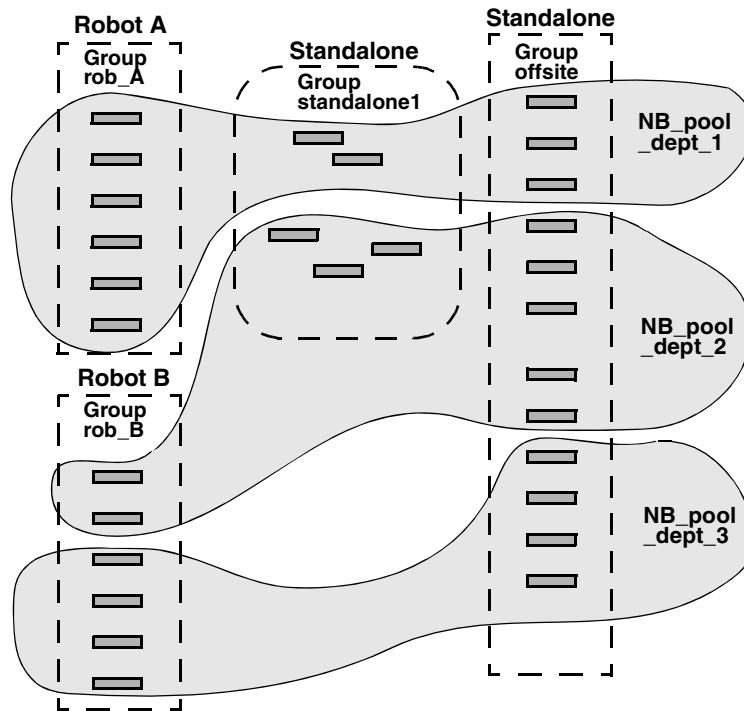
Volume Pool With Multiple Volume Groups



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 347).

## Scratch Volume Pools

The scratch pool is an optional volume pool that you can configure. If a scratch pool is configured, Media Manager moves volumes from that scratch pool to other pools that have do not have volumes available.

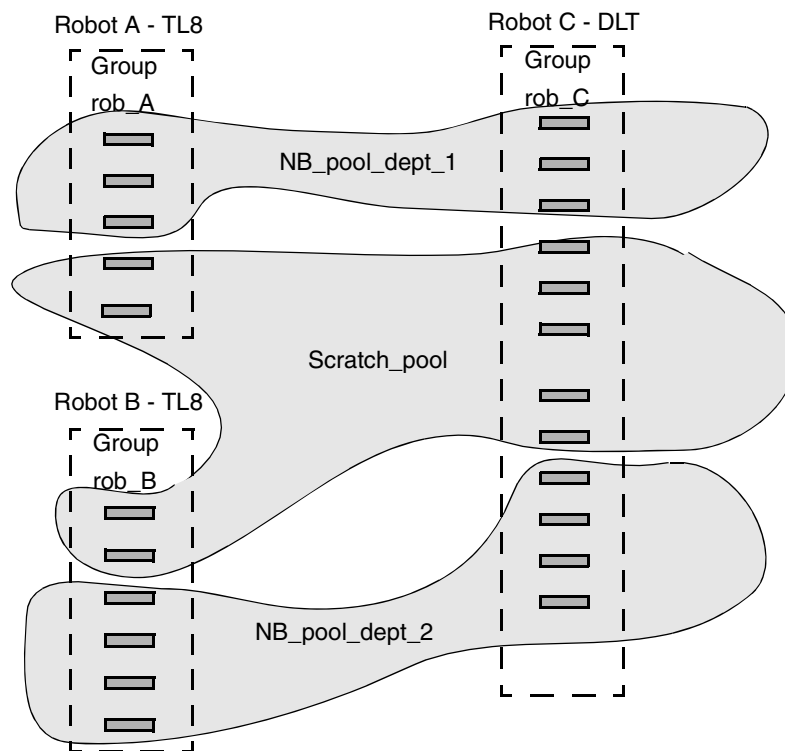
See “Adding a New Volume Pool or Scratch Volume Pool” on page 136 for configuration information.

## 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).

- ◆ 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

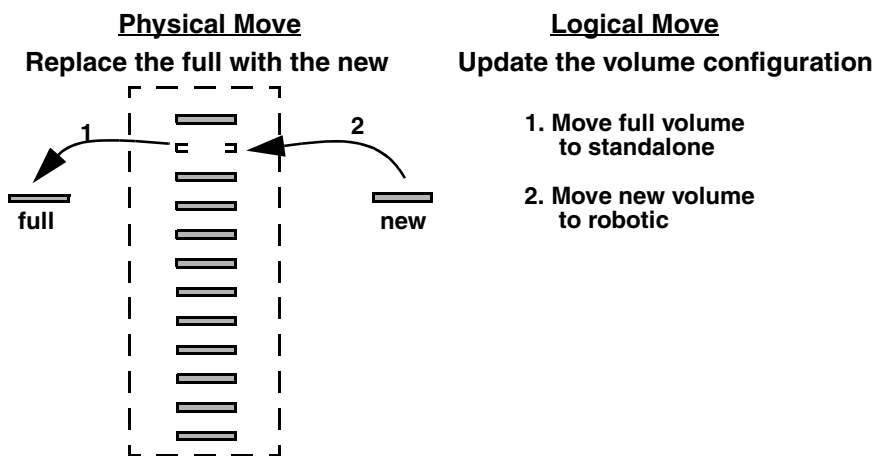
When you move volumes in or out of a robotic library or from one robotic library to another, you must physically and logically move the volume, as follows:

- ◆ 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 EMM 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 related topics:

- ◆ “Barcode Advantages” on page 350
- ◆ “Barcode Best Practices” on page 351
- ◆ “Barcode Rules” on page 352
- ◆ “Media ID Generation Rules” on page 354

## 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 311.
- ◆ 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, TLH, and TLM robots.
- ◆ 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 354). 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 EMM server .

### 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 EMM 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
TL8	8MM	t_pool	0	8 mm backup
TL	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 TL8 robot:

Media Type = 8MM

Volume Group = 00\_000\_TL8

Use Barcode Rules = YES

Volume Pool = DEFAULT

If a new volume in this robotic library has a barcode of TL800001, Media Manager uses the rule with the barcode tag of TL8 and assigns the following attributes for the volume:

Media ID = 800001 (last six characters of barcode)

Volume Group = 00\_000\_TL8

Volume Pool = t\_pool



Max Mounts = 0 (no maximum)

If a new volume has a barcode of TL000001, Media Manager uses the rule with the barcode tag of TL and assigns the following attributes for the volume:

Media ID = 000001 (last six characters of barcode)

Volume Group = 00\_000\_TL8

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 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 EMM 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 EMM database for its media information, and appropriately updates the EMM database to match its contents to that of the robotic library.

## Why Use `vmphyinv`?

For robotic libraries without barcode readers or libraries containing non-barcoded 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 EMM database.

For the complete syntax for the `vmphyinv` command, see `vmphyinv` in *VERITAS NetBackup Commands for UNIX and Linux* or *VERITAS NetBackup Commands for Windows*.

Also see the following related topics:

- ◆ “Features of `vmphyinv`” on page 355
- ◆ “Requirements and Restrictions for `vmphyinv`” on page 356

## Features of `vmphyinv`

`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.
- ◆ 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 for `vmphyinv`

`vmphyinv` has the following requirements and restrictions:

- ◆ 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.
- ◆ The optical disk library (ODL) robot type is not supported.

## When to Use `vmphyinv`

This utility can be used to update the EMM 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 EMM database. For non-barcoded media, the second action is the recommended way to inventory the robot.

- a. Add volume records to the EMM 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 EMM database.

- ◆ Some of the media are misplaced and the EMM 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 EMM 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 EMM 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 EMM 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 EMM 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 backup 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 volume records corresponding to the robot number in the EMM database for the robot. `vmphyinv` obtains a list of volume records belonging to that robot and inventories each of the media in the list.
- ◆ Specify a Media Manager robot number with filtering options



Inventorying 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 EMM 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 EMM 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
-rn 1 -slot_range 2 10 -d dlt	Only media in the slot range 2 to 10 in robot 1.
-rn 0 -slot_list 3:4:5 -d 8mm	Only media in slots 3, 4, and 5 in robot 0.
-rn 2 -slot_range 2 4 -slot_list 5:6:7 -d dlt	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 EMM database. If you want to generate volume records for the media, you should run `vmupdate` to update the EMM 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 EMM 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 EMM 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 EMM database is updated. Until then the EMM 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 the EMM database 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 EMM database checking if the media ID from the tape is present in the media ID field of any record in the EMM database.

---

Media ID Present?	Action
Yes	<code>vmphyinv</code> updates the Media Manager volume record having the media ID accordingly.
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 EMM database checking if the media GUID from the tape is present in the ADAMM\_GUID field of any record in the EMM 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 EMM 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 EMM database (if not already present). Each record is assigned to NetBackup (if not already assigned) and its state is set to FROZEN in the EMM 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 EMM database checking if the media GUID from the tape is present in the `ADAMM_GUID` field of any record in the EMM 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 Storage Migrator for Windows 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.

---

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 EMM 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” on page 363.
- ◆ “Decommissioning a Media Server” on page 365.

### Replacing Devices

If you replace an existing device in your configuration with a new device, the serial number of the device will likely change. If you are swapping a serialized device or updating drive firmware for an existing device, NetBackup can recognize the change and update the EMM database without restarting `ltid`. For devices on NetBackup 5.x hosts, you must restart `ltid` before the new device will be correctly recognized.

NetBackup also has an improved its serial number formatting algorithm in Release 6.0. This serial number formatting change may cause certain devices (tape drives and robotic libraries) to be configured as unserialized or configured with a different serial number.



Devices that are upgraded from pre-NetBackup 6.0 installations will still have the legacy serial numbers in the EMM database. Any runtime integrity checks performed by querying the device serial number and comparing with the configured serial number in the database will fail for those few devices whose legacy serial number in the database differs from what the new serial number formatting algorithm generates. This may lead to the device being unusable (e.g.: the tape drive may be downed). This can happen when `ltid` performs automatic path correction, or when the run-time Plug-n-Play code (Windows only) performs serial number checks. In such cases:

- ◆ Update the serial number or reconfigure the device causing the new serial number to be stored in the EMM database. See “To swap a serialized drive or to update drive firmware on a single host” on page 364, or, for a shared drive, see “To swap a shared serialized drive or to update drive firmware on a shared drive” on page 365
- ◆ Disable runtime serial number checks using the `AUTO_PATH_CORRECTION` `vm.conf` option.

▼ **To swap a serialized drive or to update drive firmware on a single host**

1. Down the drive. In the Device Monitor, select the drive to swap or update. From the **Actions** menu, select **Down Drive**. Alternatively, down the drive using the `vmopr cmd` command with the `-downbyname drive_name` option.
2. Replace the drive or physically update the firmware for the drive. When replacing the drive, specify the same SCSI ID for the new drive as the drive you are replacing.
3. Up the drive. In the Device Monitor, select the swapped or updated drive. From the **Actions** menu, select **Up Drive**. Alternatively, up the drive using `vmopr cmd` with the `-upbyname drive_name` option.

For the complete syntax of the `vmopr cmd` command, see `vmopr cmd` in *VERITAS NetBackup Commands for UNIX* or *VERITAS NetBackup Commands for Windows*.

If you are replacing a drive with a drive of a different type, or replacing a serialized drive with an unserialized drive, configure the new device by running device discovery. 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).

**▼ To swap a shared serialized drive or to update drive firmware on a shared drive**

1. Down the drive. In the Device Monitor, select the drive to swap or update. From the **Actions** menu, select **Down Drive**.
2. Replace the drive or physically update the firmware for the drive. When replacing the drive, specify the same SCSI ID for the new drive as the drive you are replacing.
3. 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.
4. Ensure that all servers that are sharing the new hardware are up and are running NetBackup services.
5. Run `tpautoconf` with the `-replace_drive drive_name -path path_name` options or `-replace_robot robot_number -path robot_path` options.  
  
The serial number is read from the new hardware device and the EMM database is updated.
6. If the new device is an unserialized drive, run the device configuration wizard on all servers that are sharing the drive.  
  
If the new device is a robot, run the device configuration wizard on the server that is the robot control host.
7. Up the drive. In the Device Monitor, select the swapped or updated drive. From the **Actions** menu, select **Up Drive**.

## 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 *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I* or *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* 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 EMM database records, replacing the *old\_server* with the *new\_server*, and updating the images database on the master server.

```
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 151.

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 76.

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 Manually” on page 51 and “Adding Drives” on page 61.
  - 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 policies that explicitly specified any of the storage units on the *old\_server*. These policies 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. Use `nbermmcmd` to remove the host aliases and host names referencing the *old\_server*. Run `nbermmcmd -listhosts` to verify that all references have been removed.
  11. 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.

## Moving the EMM Server

### ▼ Additional considerations when moving an EMM server to a Windows cluster.

1. When you move an EMM server to a NetBackup cluster installation, use the virtual name of the EMM server when configuring NetBackup.
2. Add the NetBackup Enterprise Media Manager service to the `ClusteredServices` entry in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\
Cluster\Instance1
```

This service must be included in the `ClusteredServices` entry so that it will start when a failover occurs.



3. Add the NetBackup Enterprise Media Manager service to the `MonitoredServices` entry in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Cluster\Instance1
```

This service must be included in the `MonitoredServices` entry so that it will be monitored. If it fails, it will be restarted. If it fails too many times, the NetBackup cluster group will fail over to another node.

4. Set the services to **Manual**.

This prevents the NetBackup services from starting on the inactive node if the inactive node is rebooted.

5. Update any paths to shared drives that the EMM server points to.
6. Change the server name to a virtual name and update any databases to reflect the name change.
7. The database also needs to be moved (if it is with the EMM server).

▼ **Additional considerations when moving an EMM server from a Windows cluster**

1. When you move an EMM server from a NetBackup cluster installation, use the virtual name of the EMM server when configuring NetBackup

2. Remove the NetBackup Enterprise Media Manager service from the `ClusteredServices` entry in the following registry key:

```
(HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Cluster\Instance1)
```

This service must be removed from the `ClusteredServices` entry so that it does not start when a failover occurs.

3. Remove the NetBackup Enterprise Media Manager service from the `MonitoredServices` entry in the following registry key:

```
(HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Cluster\Instance1)
```

This service has to be removed from the `MonitoredServices` entry so that it does not get monitored.

4. Set the services to **Manual** or remove them.

This prevents the NetBackup services from starting on the inactive node if the inactive node is rebooted





5. Update or remove any paths to the shared drive that the EMM server points to.
6. Change the server name to a non-virtual name and update any databases to reflect the name change.
7. The database also needs to be moved (if it is with the EMM server).

▼ **Additional considerations when moving an EMM server to/from a Unix cluster**

- ❖ Update the NBU\_RSP file (adding or removing EMM server).

## 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, the barcode or external label is missing or damaged, or when the physical inventory utility (`vmphysinv`) is being used to aid in media management.



## 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 `bpmedia` 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

NetBackup stores media information and device configuration and status information in a central repository: the EMM database. When a robotic mount request is issued, the NetBackup Resource Broker (nrb) queries the EMM database. If the media ID is found in the EMM database, the media request is matched with a compatible drive in the robot and the mount request is forwarded to the appropriate robotic daemon (UNIX) or process (Windows), based on the location of the media (which robotic library and the storage slot number, if applicable).

A drive must meet the following criteria to be selected for the mount request.

- ◆ The drive is configured.
- ◆ The drive is in the robotic library that contains the media.



- ◆ The drive allows the requested media density.

nbemm, the EMM server, manages the drives and requests for locally-attached or shared drives in the EMM domain. nbemm 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. NetBackup selects the robotic-based drives over standalone drives, unless matching media is already loaded in the standalone drive.

The first drive in the drive configuration as shown by `tpconfig -d` will be used first, then the second drive, and so on.

*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.

## 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 371.

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 (non-robotic) 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 the EMM 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 unassigned volume, NetBackup selects a volume.
- ◆ 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, you can direct NetBackup to wait until a media is loaded in a compatible standalone drive instead of searching for other media and generating a pending mount request. This is helpful when a gravity feed stacker (a stacker that is not controlled by software) takes some time to load the next media in the drive.

To do this, specify the Media host property, **Media Request Delay**, for the server. This property specifies the number of seconds NetBackup will wait and try to use a media loaded in a compatible drive before looking for another drive and generating a pending mount request during spanned operations. NetBackup honors the **Media Request Delay** only when standalone drive extensions are enabled.

### Keeping Standalone Drives in the Ready State

To leave standalone drives in a ready condition after a backup or restore completes, use `nbemmcmd`.

See the *VERITAS NetBackup Commands for UNIX* for detailed information on the `nbemmcmd` command.

Using this command and its parameters, prevent Media Manager from ejecting the tape after an operation completes. The media is ejected if end of media (EOM) is reached, if an error is encountered, if the drive needs to be used with another media, or if the media needs to be used with another drive.

It is possible for more than one standalone drive to be ready and contain suitable media.

## 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



Symbol	Description
Image	Data from the backup.
EH	Empty Backup Header, used for position validation.

## Standard Tape Format

For all tape media except QIC/WORM, 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/WORM Tape Format

This format is used for quarter-inch cartridge and WORM media. With this format NetBackup does not write empty backup headers (EH). The format 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 378) 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 379.
- ◆ “Media Manager Security (Using SERVER Configuration Entries)” on page 381.
- ◆ “Possible NetBackup and Media Manager Conflicts” on page 381.
- ◆ “Media Manager Enhanced Authorization” on page 381.

## 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 *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II* or *VERITAS NetBackup System Administrator's Guide for Windows, Volume II* 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 `vmd` 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 379 and “`vm.conf` Entry is Present” on page 380) 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 387 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 381).

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)



Media Manager Security Matrix - No AUTHORIZATION\_REQUIRED Entry (continued)

Access to Media Manager functionality?	Server name is in vm.conf	No server names in vm.conf (or no vm.conf file)	Server name not in vm.conf (other server names are present)
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 vm.conf	No server names in vm.conf	Server name not in vm.conf (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 379 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 `vmid` or with the control functions for robotic services.

See the following related topics:

- ◆ “Supported Commands and Daemons” on page 382.



- ◆ “Allowing Enhanced Authorization” on page 382.
- ◆ “Enabling Robot Authorization” on page 383.

## 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 EMM database or Media Manager 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	
odld		vmchange	
tl4d		vmdelete	
tl8cd		vmopr cmd	
tl dcd		vmphyinv	
tlhcd	Applies only to NetBackup Enterprise Server.	vm pool	
tlmd	Applies only to NetBackup Enterprise Server.	vmquery	
tpautoconf		vmrule	

## Allowing Enhanced Authorization

If you want to allow nonroot users to administer Media Manager or control user access to administer Media Manager commands, use either of the following methods:

- ❖ See the *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II* for instructions on using the `nonroot_admin` script.



This script can be used to change permissions for these commands. In this case, nonroot authorized users may be able to run some of these commands. However, this use of the script is currently not supported. In particular for those commands that use the Media Manager databases, execution by nonroot users will fail since access to the databases is restricted.

- ◆ See the *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II* 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 383 and “Media Manager Log Files” on page 386) 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 *VERITAS NetBackup Commands for UNIX and Linux* for detailed information on most of the commands shown in the following tables.



The `jnbSA` command is located in the directory `/usr/opensv/netbackup/bin`. The other commands listed are located in `/usr/opensv/volmgr/bin`.

#### Administrative Utilities

---

Command	Description
<code>jnbSA</code>	Starts the Java media and device management, and device monitor administrative interfaces.
<code>vmadm</code>	Starts the character-based, menu-driven media management utility.
<code>tpconfig</code>	Starts the character-based, menu-driven utility for device configuration.
<code>robtest</code>	Starts the robotic test utilities. NOTE: This utility is not officially supported.

---

#### Starting Daemons

---

Command	Description	Note
<code>acsd</code>	The Automated Cartridge System robotic daemon. This daemon is started by <code>ltid</code> .	Applies only to NetBackup Enterprise Server.
<code>avrd</code>	The Automatic Volume Recognition daemon. This daemon is started by <code>ltid</code> .	
<code>ltid</code>	Starts the Media Manager device daemon. Starting <code>ltid</code> also starts the robotic, robotic control, and Media Manager volume and <code>avrd</code> daemons.	
<code>odld</code>	The Optical Disk Library robotic daemon. This daemon is started by <code>ltid</code> .	
<code>t14d</code>	The Tape Library 4MM robotic daemon. This daemon is started by <code>ltid</code> .	
<code>t18cd</code>	Starts the Tape Library 8MM robotic-control daemon. This daemon is started by <code>ltid</code> .	
<code>t18d</code>	The Tape Library 8MM robotic daemon. This daemon is started by <code>ltid</code> .	

---





## Starting Daemons (continued)

Command	Description	Note
<code>tlbcd</code>	Starts the Tape Library DLT robotic-control daemon. This daemon is started by <code>ltid</code> .	
<code>tlidd</code>	The Tape Library DLT robotic daemon. This daemon is started by <code>ltid</code> .	
<code>tlhcd</code>	Starts the Tape Library Half-inch robotic-control daemon. This daemon is started by <code>ltid</code> .	Applies only to NetBackup Enterprise Server.
<code>tlhd</code>	The Tape Library Half-inch robotic daemon. This daemon is started by <code>ltid</code> .	Applies only to NetBackup Enterprise Server.
<code>tlmd</code>	The Tape Library Multimedia daemon. This daemon is started by <code>ltid</code> .	Applies only to NetBackup Enterprise Server.
<code>vmd</code>	The Media Manager volume daemon. This daemon is started by <code>ltid</code> .	
<code>vmacd</code>	The NetBackup Status Collection daemon. <code>vmacd</code> is started by <code>nbemm</code> on the same host as the EMM server if and only if there are one or more NetBackup 5.x servers present in the configuration.	

## Stopping Daemons

Command	Description	Note
<code>kill <i>pid</i></code>	Stops the process for the daemon with the specified <i>pid</i> (process id). This is a system command with a path of <code>/usr/bin/kill</code> or <code>/bin/kill</code> .	
<code>stopltid</code>	Stops the device, robotic, and robotic-control daemons.	
<code>tlbcd -t</code>	Stops the Tape Library DLT robotic-control daemon.	
<code>tl8cd -t</code>	Stops the Tape Library 8MM robotic-control daemon.	



## Stopping Daemons (continued)

Command	Description	Note
<code>tlhcd -t</code>	Stops the Tape Library Half-inch robotic-control daemon.	Applies only to NetBackup Enterprise Server.

Monitoring Processes

---

Command	Description
<code>vmpps</code>	Lists the active processes. NOTE: This command is not officially supported.

## Media Manager Log Files

The following table contains descriptions of important Media Manager log files.

Log Files

---

Log File	Description	Note
System Log (syslog)	Contains general Media Manager logging, including errors. All log messages use the daemon facility.  For debug logging, use the <code>-v</code> option on the command starting the daemon or use <code>VERBOSE</code> in the <code>vm.conf</code> file.	
<code>daemon/log.ddmmyy</code>	Contains debug information for the volume daemon ( <code>vmd</code> ) and its associated processes ( <code>opr</code> and <code>rdevmi</code> ).  The path is <code>/usr/opensv/volmgr/debug/daemon</code> .	
<code>reqlib/log.ddmmyy</code>	Contains debug information on the processes that request <code>vmd</code> .  The path is <code>/usr/opensv/volmgr/debug/reqlib</code> .	

## Log Files (continued)

Log File	Description	Note
tpcommand/log.ddmmyy	Contains debug information for device configuration. Includes information for tpconfig, tpautoconf, and the NetBackup GUIs. The path is /usr/opensv/volmgr/debug/tpcommand.	
ltid/log.ddmmyy	Contains debug information for ltid, the Media Manager device daemon. The path is /usr/opensv/volmgr/debug/ltid.	
acsssi/event.log	Contains debug and error information for the acsssi component of ACS robotic control.	Applies only to NetBackup Enterprise Server.
robots/log.ddmmyy	Contains debug information for SCSI robotic daemons. Includes information for tldcd, t18cd, and t14d daemons. The path is /usr/opensv/volmgr/debug/robots.	

## The Media Manager Configuration File (vm.conf)

The /usr/opensv/volmgr/vm.conf file contains configuration entries for media and device management. This file may be created by NetBackup, but if it does not exist you may 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 406 for an example configuration file.

The entries that this file can contain are as follows.

- ◆ “ACS Media Mapping” on page 389
- ◆ “ACSSSEL Listening Socket” on page 389
- ◆ “ACSSSI CSI Host Port” on page 389
- ◆ “ACSSSI Host Name” on page 390



- ◆ “ACSSSI Inet Port” on page 390
- ◆ “ACSSSI Listening Socket” on page 391
- ◆ “ACSSSI RPC Communication Method” on page 392
- ◆ “Adjacent LSM Specification for ACS Robots” on page 392
- ◆ “API Robot Barcode Rule Enable” on page 393
- ◆ “Authorization Required” on page 394
- ◆ “Automatically Empty Robot MAP” on page 394
- ◆ “AVRD Pending Status Delay” on page 394
- ◆ “AVRD Scan Delay” on page 395
- ◆ “Cleaning Drives Timeout” on page 395
- ◆ “Client Port Range” on page 396
- ◆ “Connect to Firewall Options” on page 396
- ◆ “DAS Client Name” on page 397
- ◆ “Days To Keep Debug Logs” on page 397
- ◆ “Automatic Path Remapping” on page 398
- ◆ “Enable Robot Authorization” on page 398
- ◆ “Inventory Robot Filter” on page 398
- ◆ “Media Access Port Default for ACS Robots” on page 399
- ◆ “Media Access Port Timeout Control” on page 400
- ◆ “Media ID Generation” on page 400
- ◆ “Media ID Prefix” on page 401
- ◆ “Preferred Group” on page 401
- ◆ “Prevent Media Removal (for TL8 Robots)” on page 402
- ◆ “Random Port Numbers” on page 402
- ◆ “Cluster Name, Media Manager Name, Required Network Interface” on page 403
- ◆ “Server Entry” on page 403
- ◆ “SSO DA Re-register Interval” on page 404
- ◆ “SSO DA Retry Time” on page 404
- ◆ “SSO Host Name” on page 405
- ◆ “TLH Media Mapping” on page 405



- ◆ “TLM Media Mapping” on page 405
- ◆ “Verbose Message Logging” on page 405

## 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 483.

## ACSSEL Listening Socket

`ACS_SEL_SOCKET = socket_name`

*This configuration entry applies only to NetBackup Enterprise Server*

By default, `acsselect` listens on socket name 13740. If this entry is specified in `vm.conf`, you can change the default. This entry is read and interpreted on the host where `acsd` is running.

For more information, see the appendix, “STK Automated Cartridge System (ACS)” on page 483.

## ACSSSI CSI Host Port

`ACS_CSI_HOSTPORT = ACS_library_software_hostname socket_name`

*This configuration entry applies only to NetBackup Enterprise Server*

Valid value for `ACS_library_software_hostname` is the host name of the ACS library host. Do not use the IP address of the ACS library host for this parameter.

Valid values for `socket_name` are 1024 - 65535 and 0. The value specified must match the value set on the ACSLS server for the port used by the CSI for inbound packets.

0 (zero) indicates that the previous behavior of CSI and `acsssi` will be used (no specific ports).



This entry specifies the port where the `acsssi` process will send its ACSLS requests on the ACSLS server. The ACSLS CSI must be using this port to accept inbound ACSLS requests from `acsssi` processes.

This entry (in conjunction with `ACS_SSI_INET_PORT` and `ACS_TCP_RPCSERVICE` entries) is commonly used with firewall implementations. With these three entries added to `vm.conf`, TCP connections use the designated destination ports. Note that TCP source ports are not restricted. Also see “ACSSSI Inet Port” on page 390 and “ACSSSI RPC Communication Method” on page 392.

For example, a NetBackup media server has two ACSLS servers (`ACSL_1` and `ACSL_2`) behind firewalls. Both servers are listening for queries on port 30031 and the firewall allows traffic through this port. The entries would be as follows:

```
ACS_TCP_RPCSERVICE
ACS_CSI_HOSTPORT = ACSLS_1 30031
ACS_CSI_HOSTPORT = ACSLS_2 30031
ACS_SSI_INET_PORT = ACSLS_1 30032
ACS_SSI_INET_PORT = ACSLS_2 30033
```

This means that each `acsssi` process will send queries to the respective ACSLS server’s port 30031 and that the ACSLS server has been configured to listen for queries on this port.

For more information, see the appendix, “STK Automated Cartridge System (ACS)” on page 483.

## ACSSSI Host Name

```
ACS_SSI_HOSTNAME = host
```

*This configuration entry applies only to NetBackup Enterprise Server*

If this entry is specified in `vm.conf`, you can specify the host where RPC return packets from ACS library software are routed for ACS network communications. By default, the local host name is used. This entry is read and interpreted on the host where `acsd` and `acsssi` are running. Do not use the IP address of the host for this parameter.

See the appendix, “STK Automated Cartridge System (ACS)” on page 483 for more information.

## ACSSSI Inet Port

```
ACS_SSI_INET_PORT = ACS_library_software_hostname socket_name
```

*This configuration entry applies only to NetBackup Enterprise Server*



Valid value for *ACS\_library\_software\_hostname* is the host name of the ACS library host. Do not use the IP address of the ACS library host for this parameter.

The *socket\_name* entry specifies the port that *acsssi* will use for incoming ACSLS responses. Valid values are 1024 - 65535 and 0. This value must be unique for each *acsssi* process.

A value between 1024 - 65535 indicates the number to be used as the TCP port on which *acsssi* will accept ACSLS responses.

0 (zero) indicates that the previous behavior of allowing the port to be dynamically allocated should remain in effect.

This entry (in conjunction with *ACS\_CSI\_HOSTPORT* and *ACS\_TCP\_RPCSERVICE* entries) is commonly used with firewall implementations. With these three entries added to *vm.conf*, TCP connections use the designated destination ports. Note that TCP source ports are not restricted. Also see “ACSSSI CSI Host Port” on page 389 and “ACSSSI RPC Communication Method” on page 392.

For example, a NetBackup media server has two ACSLS servers (*ACSL\_1* and *ACSL\_2*) behind firewalls. Ports 30032 and 30033 have been opened in the firewall for *acsssi* to ACSLS server communication. The entries would be as follows:

```
ACS_TCP_RPCSERVICE
ACS_SSI_INET_PORT = ACSLS_1 30032
ACS_SSI_INET_PORT = ACSLS_2 30033
ACS_CSI_HOSTPORT = ACSLS_1 30031
ACS_CSI_HOSTPORT = ACSLS_2 30031
```

This means that the NetBackup media server will start two *acsssi* processes, one listening for *ACSL\_1* responses on port 30032, the other listening on port 30033 for responses from *ACSL\_2*.

For more information, see the appendix, “STK Automated Cartridge System (ACS)” on page 483.

## ACSSSI Listening Socket

```
ACS_SSI_SOCKET = ACS_library_software_hostname socket_name
```

*This configuration entry applies only to NetBackup Enterprise Server*

Valid value for *ACS\_library\_software\_hostname* is the host name of the ACS library host. Do not use the IP address of the ACS library host for this parameter.

By default, *acsssi* listens on unique, consecutive socket names starting with 13741. If this entry is specified in *vm.conf*, you can specify socket names on a ACS library software host basis. This entry is read and interpreted on the host where *acsd* and *acsssi* are running.



For more information, see the appendix, “STK Automated Cartridge System (ACS)” on page 483.

## ACSSSI RPC Communication Method

```
ACS_TCP_RPCSERVICE
ACS_UDP_RPCSERVICE
```

*This configuration entry applies only to NetBackup Enterprise Server*

These entries specify the method over which `acsssi` will communicate with ACSLS servers: `tcp` or `udp`.

Only one entry should be entered into `vm.conf`. If both entries are found, `acsssi` will default to `udp` communication. If neither entry is found, `udp` is used.

For `acsssi` firewall support, `ACS_TCP_RPCSERVICE` must be entered in `vm.conf` (see “ACSSSI CSI Host Port” on page 389 and “ACSSSI Inet Port” on page 390).

For more information, see the appendix, “STK Automated Cartridge System (ACS)” on page 483.

## 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 from the NetBackup Administration Console for Media Manager.

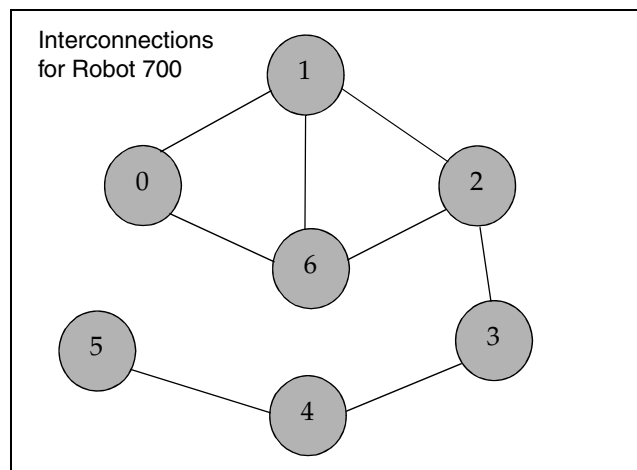
---



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 shows the entries required to specify the physical layout of LSM interconnections for robot number 700. This robot has 7 LSMs that are connected by pass-through mechanisms. The interconnections are shown first followed by the appropriate entries.



```

ADJ_LSM = 700 0,0 0,1
ADJ_LSM = 700 0,0 0,6
ADJ_LSM = 700 0,1 0,2
ADJ_LSM = 700 0,1 0,6
ADJ_LSM = 700 0,2 0,6
ADJ_LSM = 700 0,2 0,3
ADJ_LSM = 700 0,3 0,4
ADJ_LSM = 700 0,4 0,5
  
```

## 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 using different drive types such 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 `vmd`; 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 `vmd` is running.

If this entry is not specified, Media Manager and NetBackup utilities may connect to `vmd` 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 and a unit attention has been detected, the Media Access Port (MAP) of the robot will be emptied into the robotic library and the EMM 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 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.

On some server operating systems (Windows, Tru64, and HP-UX), NetBackup will 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.

## 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.

---

## 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 `vm` on other hosts. This entry is read and interpreted on the hosts where `vm` 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 *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I* or *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* 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 or higher 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 `t1md` is running.

See the appendix, "ADIC Distributed AML Server/Scalar Distributed Library Controller" on page 519 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. This entry does not impact debug logs created by Unified Logging. See the *NetBackup Troubleshooting Guide for Unix, Windows, and Linux* for more information about Unified Logging.



## Automatic Path Remapping

`AUTO_PATH_CORRECTION = YES|NO`

If this entry is specified in `vm.conf`, it specifies whether automatic device path remapping is enabled or disabled.

If the value specified is `NO`, the device configuration will remain unchanged when the NetBackup Device Manager service or `ltid` is started. This may result in the device configuration becoming out of sync with the host's view of devices following a reboot.

If the value specified is `YES`, an attempt is made to discover attached devices and automatically update the device configuration for any device paths that are incorrect in the device configuration. On Windows systems, this entry is read and interpreted on the host where the NetBackup Device Manager service is running. On UNIX and Linux systems, this entry is read and interpreted on the host where `ltid` is running.

Device path remapping is enabled by default on Windows and Linux servers. It is disabled by default on all other servers.

## 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, or TLH 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 was previously required if you were doing a robot inventory for an ACS robot and the ACS library software host was an STK Library Station. There are new versions of STK Library Station available that allow robot inventory commands to function without requiring filters.

---

*robot\_type* can be ACS, or TLH.

*robot\_number* is the number of the robot as was configured in Media Manager.

*mode* is BY\_ACS\_POOL for ACS, or BY\_CATEGORY for TLH.

The following are some examples:

```
INVENTORY_FILTER = ACS 0 BY_ACS_POOL 4 5
INVENTORY_FILTER = TLH 0 BY_CATEGORY FFFA CDB0
```

See the appendices, “STK Automated Cartridge System (ACS)” on page 483, or “IBM Automated Tape Library (ATL)” on page 505 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 392).

*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 Access Port Timeout Control

`MAP_CONTINUE_TIMEOUT = seconds`

This entry is read and interpreted on the host where the SCSI-controlled robotic daemon or process is running.

If this entry is specified in `vm.conf`, the SCSI robotic daemons will wait the number of seconds specified before timing out. A timeout can occur while waiting for a reply from the user to continue after removing volumes from the media access port. A timeout results in the operation being aborted.

This entry applies only when using the `vmchange` command and specifying the `-w` option. The default timeout value for `seconds` is 300 (5 minutes). `seconds` cannot be zero and values greater than 1200 (20 minutes) may cause the robotic daemon to cancel the operation.

---

**Caution** Non-mount activities such as a robotic inventory can not occur during this timeout period.

---

## 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 354.

## 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 190.

## 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 in the *netgroup* using the *innetgr()* function. If a *PREFERRED\_GROUP* entry is not specified or the user is not a member of the *netgroup*, the local group name is obtained.

The following is an example:



```
PREFERRED_GROUP = nbadmins
```

## Prevent Media Removal (for TL8 Robots)

```
PREVENT_MEDIA_REMOVAL
```

This entry is read and interpreted on the host where the TL8 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 `vmc` 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 *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I* or *VERITAS NetBackup System Administrator's Guide for Windows, Volume I* for more information on NetBackup network configuration.

## 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 `vmc` 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 EMM/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 EMM/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 EMM/DA. The default is the local host name.

## 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 505 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 519 for more information.

## 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
```

## Using `tpconfig`

## B

This appendix explains how to configure drives and robots using the device management configuration utility, `tpconfig`. This menu-driven utility updates the EMM database which retains the device configuration used by Media Manager.

There are also other Media Manager interfaces available to configure drives and robots (see “Media Manager Administrator and User Interfaces” on page 7). The terminology, general concepts, and results are the same, regardless of which interface you use.

### Robot Number

You assign a robot number when you add a robot to the configuration. `tpconfig` prompts you to enter a number or accept the next available robot number which it displays. This number identifies the robot in displays and listings, and it follows the robotic type in parentheses, such as TL8(2). It is also used when entering the robot's media in the EMM database, as described in “Managing Media” on page 103.

*The following point applies only to NetBackup Enterprise Server.*

If you are configuring robots on multiple systems, robot numbers must be unique. If you are connecting drives from a robot (for example, drives in a Tape Library 8MM (TL8)) to multiple systems, you must specify the same robot number for the robot on both systems.

### Robotic Control Path

For most robots, you or the operating system creates this path in the `/dev` directory when you add a robot to the configuration. When `tpconfig` prompts you, enter the path to the robotic control as found in the `/dev` directory. If the entries do not exist, see the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

*The following point applies only to NetBackup Enterprise Server.*

For API robots, see the appendices in this guide for information on configuring robotic control. The control path to a robot may be on another host. If so, enter the host name of the host instead of a path. When you define a robot that is actually controlled by another host, the robot number must be the same on both hosts.



---

## Host Name

*This is a NetBackup Enterprise Server topic.*

You must specify a host name in the following cases. When you add

- ◆ An ACS robot, enter the name of the host where the ACS Library Software resides, instead of a robotic control path.

See the ACS appendix, “STK Automated Cartridge System (ACS)” on page 483.

- ◆ A TLM robot, enter the DAS/SDLC server name instead of a robotic control path.

See the TLM appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 519.

- ◆ An TL8, TLD, or TLH robot that has robotic control on another host, you are prompted for the host name of that host.

## No Rewind On Close Device Name

You specify a no rewind on close device name when you add a drive. Usually the device name is preceded or followed by the letter n. If the device name entries do not exist, you must create them as explained in the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

In `tpconfig` displays and listings, these device names are shown under the heading DrivePath.

## Character Device Name

Character device name applies only to optical disk devices. A drive used as a character device uses a complete 512-byte block each time it writes (note that some systems may use 1024 byte blocks). If less than 512 bytes are used, the remaining bytes are padded out. A character device is also referred to as a raw device. NetBackup and Storage Migrator use character mode.

You specify a device name when you add an optical disk to the configuration. When prompted, enter the path name to the device as found in the `/dev` directory. If the entries do not exist, you must create them as explained in the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux*.

In `tpconfig` displays and listings, the character device name appears under the heading DrivePath.



## Volume Header Device Name

---

**Note** Volume headers do not apply to all systems.

---

The volume header device name is used internally, but must be specified when adding an optical drive to a configuration. When prompted, enter the path name to the device as found in the `/dev` directory. To display the volume header device name, choose the Update or Delete option from the Drive Configuration menu.

On Solaris systems, the `MAKEDEV` command may have to be run first to create these entries. For more information, see the *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* and the `MAKEDEV(8)` command.

## Drive Status

Drive status indicates whether Media Manager considers a drive available. You specify the initial drive status when you add a drive to the configuration. You can change the status, using the Update option of the Drive Configuration menu in `tpconfig` or `ifltid` has been started, by using a Device Monitor interface or `vmopr cmd`.

## Starting the tpconfig Utility

You can start `tpconfig` from the `vmadm` Media Management menu or using the following command from the command line. You must have root user privileges.

```
/usr/opensv/volmgr/bin/tpconfig
```

The following menu appears:

```
Device Management Configuration Utility
```

- ```
1) Drive Configuration
2) Robot Configuration
3) NDMP Host Credentials Configuration
4) Print Configuration
5) Help
6) Quit
```

```
Enter option:
```

---

**Note** If the Media Manager device daemon is running, you should stop it with the `stopltid` command (see “Media Manager Device Daemon (ltid)” on page 265).

---



The following table describes the main menu choices:

| Option | Menu Choice                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | Drive Configuration                 | Opens a menu for adding, deleting, updating definitions of drives, listing definitions of drives and robots, or configuring drive paths.                                                                                                                                                                                                                                                                                                                                                             |
| 2      | Robot Configuration                 | Opens a menu for adding, deleting, updating definitions of robots, or listing definitions of drives and robots                                                                                                                                                                                                                                                                                                                                                                                       |
| 3      | NDMP Host Credentials Configuration | Opens a menu for adding, deleting, updating or listing NDMP host credentials.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 4      | Print Configuration                 | <p>The List Configuration commands on subsequent menus allow you to display the current configuration on the screen or write it to a file.</p> <p>Specifying just the <code>-d</code> option on the <code>tpconfig</code> command also writes the current configuration to stdout (the screen) without invoking the menus.</p> <p>Other command options are available. Run <code>tpconfig -help</code> or see <code>tpconfig</code> in the <i>VERITAS NetBackup Commands for UNIX and Linux</i>.</p> |
| 5      | Help                                | Online help is available on the main menu and most submenus.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 6      | Quit                                | Terminates the utility and returns you to the UNIX prompt.                                                                                                                                                                                                                                                                                                                                                                                                                                           |

You can return to the main menu from anywhere in the utility by entering Ctrl C or using the Escape key.

## Adding Robots

When you configure robots and drives, the most efficient process is to first add the robot using the Robot Configuration menu and then add the drives using the Drive Configuration menu.

If you want to reconfigure drives configured as standalone to indicate that they are in a robot, use the Update option of the Drive Configuration menu. See “Updating Drive Configurations” on page 414.



▼ **To add a robot**

1. Select the Robot Configuration menu. If any robots exist, they are displayed above this menu.
2. Select the Add option.  
From the list of possible robot types, select the one you want to add.
3. Enter a robot number you know is unused or accept the default robot number.
4. Indicate where the robotic control for the library is by entering the device file path or library name. The Help option on the Robot Configuration menu has examples of typical path names.
5. *This step applies only to NetBackup Enterprise Server.*
  - a. If robotic control is on another host, enter that host name.  
For an ACS robot you must enter the name of the ACS library software host. See the appendix, “STK Automated Cartridge System (ACS)” on page 483.  
For a TLM robot, you must enter the name of the DAS/SDLC server. See the appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 519.
  - b. If robotic control is on this host, enter the device file path or library name. The Help option on the Robot Configuration menu has examples of typical path names.  
For an ACS robot you enter the name of the ACS library software host. See the appendix, “STK Automated Cartridge System (ACS)” on page 483.  
For a TLH robot, enter the LMCP Device File, if this is an AIX system. Otherwise, enter the Automated Tape Library Name. See the appendix, “IBM Automated Tape Library (ATL)” on page 505.  
For a TLM robot, you enter the name of the DAS/SDLC server. See the appendix, “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 519.
6. If no conflicts are detected with the new configuration, you see a message that the robot has been added.



## Adding Drives

### ▼ To add a drive

1. Select the Drive Configuration menu.
2. Select the Add option.
3. From the list of possible drive types displayed, select the one you want to add.
4. Enter the no rewind on close device path as shown in the `/dev` directory.  

If the device is an optical disk, enter the character device and volume header device file paths, from the `/dev` directory (volume headers are not applicable to all systems).

The Help option on the Drive Configuration menu has examples of typical path names.
5. Enter the drive status (Up or Down).
6. If a robot exists that the drive could be added to, indicate whether the drive should be added to the robot or be a standalone drive.  

If there are no robots to which the drive can be added, `tpconfig` automatically adds the drive as a standalone drive.

If you choose to add a drive to a robot and more than one possible robot exists, enter the robot number that will control the drive.

Depending on the type of robot, you may also be prompted to add the robot drive number (see “Robot Drive Number” on page 69).
7. *This step applies only to NetBackup Enterprise Server.*  

For a drive in an ACS robot, you are prompted for four drive identifiers. For more information on ACS robots, see the appendix “STK Automated Cartridge System (ACS)” on page 483.

For a drive in a TLH robot, you are prompted for an IBM device number. For more information see the appendix “IBM Automated Tape Library (ATL)” on page 505.

For a drive in a TLM robot, you are prompted for a DAS/SDLC drive name. For more information see the appendix “ADIC Distributed AML Server/Scalar Distributed Library Controller” on page 519.
8. Type a drive name or use the Enter key to use the default drive name that is shown.  

Specify a name that will be used by Media Manager to identify the drive.



*The following point applies only to NetBackup Enterprise Server.*

If you are using the shared drives option, all hosts that are sharing the same physical drive must use the same name for the drive. Descriptive drive names are recommended.

9. When finished, you see a message that the drive has been added, followed by a listing of the drive.

## Updating Robot and Drive Configurations

### Updating Robot Configurations

#### ▼ To change the robot number or the robotic control path

1. On the main menu, choose Robot Configuration.

---

**Note** If only one robot is configured, step 2 is skipped.

---

2. On the Robot Configuration menu, choose Update. The following prompt is displayed

Enter robot number to update:

Enter the number of the robotic library you want to change.

3. The following prompt is displayed:

Enter new robot number or <RETURN> to use existing (n):

Enter a new robot number to replace the existing robot number, or press Enter to retain the current robot number.

4. You are prompted to enter robotic control information. The actual prompts depend on the type of robotic library you are updating.

Enter the appropriate robotic control path or host name associated with the robot.

When you are done, a message confirming that the robot has been updated is displayed.



## Updating Drive Configurations

You can change information for a drive (for example, you can add it to a robot).

### ▼ To change information for a drive

1. On the main menu, choose Drive Configuration.
2. On the Drive Configuration menu choose Update.
3. Enter the name of the drive you want to update.
4. The current drive information is displayed, followed by prompts to change each field. Enter a new value or use the Enter key to keep the existing value.  
  
One of the prompts asks if you want to configure the drive in a robot and, if so, adds the drive immediately or gives you the opportunity to choose from any existing robot of the appropriate type.
5. When you have responded to all prompts, a revised Drive Information display appears, along with the following prompt:  
  
`Are you sure you want to UPDATE drive name xxxxx? (y/n) n:`
6. A message confirming that the drive has been updated (or not updated) is displayed.

## Deleting Drives and Robots

### Deleting Drives

#### ▼ To delete a drive

1. On the main menu, choose Drive Configuration.
2. In the Drive Configuration menu, choose Delete.
3. Enter the name of the drive you want to delete:
4. Drive information and a prompt similar to the following are displayed:  
  
`Are you sure you want to DELETE drive name xxxxx? (y/n) n:`



5. Enter y to delete the drive, or n (Enter key) to cancel the action.
  - a. If you respond with y, a message confirming the drive has been deleted is displayed.
  - b. If you respond with n, pressing any key returns you to the Drive Configuration menu and the delete action is canceled.

## Deleting Robots

### ▼ To delete a robot

1. On the main menu, choose Robot Configuration.
2. On the Robot Configuration menu, choose Delete.

---

**Note** If only one robot is configured, step 3 is skipped.

---

3. The following prompt is displayed:  

```
Enter robot number to delete:
```
4. A prompt similar to the following is displayed:  

```
Deleting robotic definition:
TLD(0) robotic path = /dev/sg/clt0d0s0,
Any drives defined on this robot will be changed to standalone
drives
Do you want to proceed? (y/n) n:
```
5. Enter y to delete the robot, or n (or Enter key) to cancel the action.
  - a. If you respond with y, a message confirming that the robot has been deleted is displayed.
  - b. If you respond with n, pressing any key returns you to the Robot Configuration menu and the delete action is canceled.



## Configuring Drive Paths

From the Drive Configuration menu, select Drive Path Configuration. The following prompt is displayed:

```
Enter name of drive to configure path(s) for:
```

Enter a drive name and the Drive Path Configuration menu is displayed.

### ▼ To add a drive path

1. Select Add from the Drive Path Configuration menu. A prompt similar to the following is displayed:

```
Enter the new drive path:
```

Enter a valid drive path.

2. A prompt similar to the following is displayed:

```
Enter drive status on this path - (u)p, (d)own or dis(a)bled:
```

3. Specify the drive status on the path. The drive can be Up, Down, or Disabled for the path.

### ▼ To delete a drive path

- ❖ Select Delete from the Drive Path Configuration menu. When prompted, enter the drive path to delete.

### ▼ To update a drive path

1. Select Update from the Drive Path Configuration menu. A prompt similar to the following is displayed:

```
Enter the current drive path:
```

Enter the drive path to update.

2. Specify a new drive path or press Return to update the status of the drive path.

3. A prompt similar to the following is displayed:

```
Enter drive status on this path - (u)p, (d)own or dis(a)bled:
```

Enter the path status.



## Configuring NDMP Host Credentials

### ▼ To add NDMP host credentials

1. On the main menu, choose NDMP Host Credentials Configuration.
2. On the NDMP Host Credentials Configuration menu, select Add.
3. Enter an NDMP host name.
4. Use the default credentials or enter a new user ID and password.
5. Specify the scope of the credentials. The credentials may be valid on a specific media server or on all media servers attached to the host.

### ▼ To delete NDMP host credentials

1. On the main menu, choose NDMP Host Credentials Configuration.
2. On the NDMP Host Credentials Configuration menu, select Delete.
3. Enter an NDMP host name.
4. Specify the scope of the credentials. The credentials to delete may be valid on a specific media server or on all media servers attached to the host.

### ▼ To update NDMP host credentials

1. On the main menu, choose NDMP Host Credentials Configuration.
2. On the NDMP Host Credentials Configuration menu, select Update.
3. Enter an NDMP host name.
4. Enter the user ID and password to update.
5. Specify the scope of the credentials. The credentials to update may be valid on a specific media server or on all media servers attached to the host.



▼ **To configure default credentials**

1. On the main menu, choose NDMP Host Credentials Configuration.
2. On the NDMP Host Credentials Configuration menu, select Configure Default Authentication Credentials.
3. From the Configure Default Authentication Credentials menu, you can add, delete, or update default credentials by selecting the appropriate option and supplying valid NDMP credentials.

## Displaying and Printing Your Device Configuration

You can display the current configuration from every menu in `tpconfig` by using the Print Configuration option on the main menu, or the List Configuration option on the subsequent menus.

You can print the configuration using the Print Configuration option on the main menu. When prompted, specify a file where the configuration will be written, or press Enter to display the configuration on the screen.

In addition, you can specify the `-d` option on the `tpconfig` command to write the current configuration to standard output (stdout) without invoking the menus.

## Using the Media Management Utility (vmadm)

C

This appendix explains how to use the media management utility (vmadm) to add, delete, or change media in a Media Manager volume configuration. This utility has a character-based interface that can be used at most terminals.

There are also other Media Manager interfaces available to configure media (see “Media Manager Administrator and User Interfaces” on page 7). The terminology, general concepts, and results in the database are the same, regardless of which interface you use.

### Starting vmadm

▼ To start vmadm

- ❖ To start vmadm, enter `/usr/opensv/volmgr/bin/vmadm` (requires root privileges).

### Starting and Stopping vmd

You can control the Media Manager volume daemon, vmd in the following ways:

▼ To start vmd from the UNIX prompt

- ❖ Enter `/usr/opensv/volmgr/bin/vmd`.

▼ To start vmd from vmadm

1. On the main menu, choose s for Special Actions.
2. Choose i for Initiate Media Manager Volume Daemon. This starts vmd and returns you to the Special Actions menu.



▼ **To stop vmd from vmadm**

1. On the main menu, choose s for Special Actions.
2. Choose t for Terminate Media Manager Volume Daemon. This stops vmd and returns you to the Special Actions menu.

## The vmadm Main Menu

The main menu is similar to the following:

```
Database Host:  shark
Media Management
-----
a) Add Volumes
d) Delete Volumes
m) Move Volumes
p) Print Information about Volumes

c) Configure Volume Pools
s) Special Actions

u) Device Configuration Utility

h) Help
q) Quit
ENTER CHOICE:
```

The Database Host name displayed at the top of the main menu is the host where the EMM database is located and the Media Manager volume daemon (vmd) is running.

The following table summarizes each main menu command. The remaining topics in this chapter explain how to perform common operations.

| Character | Menu Choice                     | Summary                                                                              |
|-----------|---------------------------------|--------------------------------------------------------------------------------------|
| a         | Add Volumes                     | Adds one or more volumes.                                                            |
| d         | Delete Volumes                  | Deletes one or more volumes.                                                         |
| m         | Move Volumes                    | Moves one or more volumes.                                                           |
| p         | Print Information about Volumes | Prints or displays information about selected volumes based on criteria you provide. |



| Character | Menu Choice                  | Summary                                                                                                                                                  |
|-----------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| c         | Configure Volume Pools       | Adds a new volume pool, deletes an existing one, changes information about a volume pool, or lists information about the currently defined volume pools. |
| s         | Special Actions              | Opens a menu with special actions.                                                                                                                       |
| u         | Device Configuration Utility | Starts the <code>tpconfig</code> device configuration utility. See the appendix “Using <code>tpconfig</code> ” on page 407.                              |
| h         | Help                         | Provides on line help.                                                                                                                                   |
| q         | Quit                         | Terminates the utility and returns you to the UNIX prompt. You can abort many operations by pressing the ESC key.                                        |

## Configuring Volume Pools

A volume pool identifies a logical set of volumes that are associated by usage rather than physical location. For example, you can create a volume pool for each storage application you are using. Then, as you add volumes to use with an application, you can associate them with a volume pool. You can also move volumes to a different pool later. Volumes associated with a particular volume pool are grouped together and protected from access by unauthorized users, groups, or applications.

Before adding volumes to a pool, you must add the pool and configure its attributes as explained in the following topics.

You do not have to configure a pool for NetBackup, or DataStore, or for catalog backups. Media Manager automatically reserves a pool named NetBackup that you specify when adding NetBackup volumes, a pool named DataStore when adding DataStore volumes, and a pool named CatalogBackup for use with hot catalog backups.



When you enter c from the main menu, the following menu appears:

```
          Display Mode:  BRIEF
Output Destination:  SCREEN

Configure Volume Pools
-----
a)  Add Pool
c)  Change Pool
d)  Delete Pool
l)  List Pools
s)  List Scratch Pools

m)  Mode (brief or full)
o)  Output Destination (screen or file)
h)  Help
q)  Quit Menu

ENTER CHOICE:
```

The following table summarizes the operations you can perform from this menu:



| Character | Menu Choice | Summary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a         | Add Pool    | <p>Defines a new volume pool. After choosing this option, you are prompted to define the following:</p> <ul style="list-style-type: none"><li>• Volume pool name - Name for the new volume pool. Enter a name of 20 ASCII characters or less. Names are case-sensitive, and no spaces or special characters are allowed.</li><li>• Description - Enter the description of the new volume pool (30 ASCII characters or less).</li><li>• Pool host name - Name of the host that can request and use volumes in this volume pool. Entering a specific host name allows only that host to access the volume pool. Using the default, ANYHOST, allows any host to access the volume pool.<br/><br/>If you have a single NetBackup server, use ANYHOST or the name of the server (not a client).<br/><i>The following point applies only to NetBackup Enterprise Server.</i><br/><br/>If you have multiple NetBackup servers (master and media servers), always set this value to ANYHOST (the default).</li><li>• Pool user name - Login name of the user that is allowed to request and use volumes in the volume pool.<br/><br/>Entering a specific name allows only the processes running as that user to access the volume pool. If a different user requests the pool, then Media Manager verifies the group name (see Pool group name). Using the default, ANY, allows any user to access the pool. For NetBackup or Storage Migrator, enter root for the pool user name.</li><li>• Pool group name - Name of the user group that can request and use volumes in this volume pool.<br/><br/>Entering a specific name allows any processes running as that user group to access the volume pool. Using the default, NONE, allows only the user specified by User Name to request or access the volume pool. All other users in any groups are denied access.</li><li>• Scratch pool - select Yes or No.</li></ul> |



| Character | Menu Choice                         | Summary                                                                                                                                                                                                      |
|-----------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| c         | Change Pool                         | Changes the description, pool host name, pool user name, pool group name, or changes a pool to become the scratch pool. You are prompted for each of these items and Scratch pool - Yes or No.               |
| d         | Delete Pool                         | Deletes the volume pool and its allocated name, description, and access permissions.                                                                                                                         |
| l         | List Pools                          | Lists the currently defined volume pools and their associated descriptions and permissions.                                                                                                                  |
| s         | List Scratch Pools                  | Lists the currently defined scratch pools (if any are defined).                                                                                                                                              |
| m         | Mode (brief or full)                | Toggles the display mode to BRIEF or FULL.                                                                                                                                                                   |
| o         | Output destination (screen or file) | Toggles the output destination between SCREEN and FILE (SCREEN is the default). If you choose to write to a file, you can define your own file name or you can use the default file, /tmp/vmadm_pool_output. |
| h         | Help                                | Provides on line help.                                                                                                                                                                                       |
| q         | Quit Menu                           | Terminates the menu.                                                                                                                                                                                         |

## Adding Volumes for Standalone Drives

### Adding a Single Standalone Volume

#### ▼ To add a volume

1. On the main menu, choose a for Add Volumes.

The following prompt appears. Enter s to add a single volume.

```
Add Single Volume, Range of Volumes, or Auto-Populate? (s/r/a):
```





2. You are prompted for the media type with a menu similar to the following that displays the possible types. Enter the number for the type of media you want to add.

```

Adding Volume
-----
Media Type
-----
1)  1/4" cartridge tape
2)  1/2" cartridge tape
3)  1/2" cartridge tape 2
4)  1/2" cartridge tape 3
5)  4MM cartridge tape
6)  8MM cartridge tape
7)  8MM cartridge tape 2
8)  8MM cartridge tape 3
9)  DLT cartridge tape
10) DLT cartridge tape 2
11) DLT cartridge tape 3
12) DTF cartridge tape
13) Optical disk rewritable
14) Optical disk WORM
15) 1/2" cleaning tape
16) 1/2" cleaning tape 2
17) 1/2" cleaning tape 3
18) 4MM cleaning tape
19) 8MM cleaning tape
20) 8MM cleaning tape 2
21) 8MM cleaning tape 3
22) DLT cleaning tape
23) DLT cleaning tape 2
24) DLT cleaning tape 3
25) DTF cleaning tape
Enter Choice [1-25]:

```

3. If you are adding a cleaning tape, you are prompted for the number of cleanings you want available. For any other media type, the next step occurs immediately.
4. You are prompted to enter the media ID. If you selected an optical disk media type, you are prompted to enter a media ID for both side A of the platter and side B of the platter. Media ID's can be from 1 to 6 characters. See "Allowable Media Manager Characters" on page 308.
5. You are prompted for a description. Enter 1 to 25 characters of text to describe the media being added.



6. If the media is not a cleaning media type you are prompted to enter a number for the volume pool.

```
Volume Pool
-----
1)  None
2)  NetBackup
3)  DataStore
4)  CatalogBackup
5)  oldpool
6)  newpool
7)  POOL1
8)  POOL2
Enter Choice:
```

Enter a number as follows:

- ◆ If you enter 1 (None) the volume is assigned to a generic volume pool and is available to any user or application.
  - ◆ Enter 2 if you want the volume to be available only to NetBackup.
  - ◆ Enter another choice to have the volume assigned to one of the volume pools listed.
7. For all media types, you are prompted to enter the physical location of the volume using a menu of possible locations, similar to the following menu for an 8mm cartridge tape. Enter 1 for a volume for a standalone drive.

```
Physical Location
-----
1)  Not in robotic device
2)  TL8 - Tape Library 8MM
3)  TLD - Tape Library DLT
4)  TLM - Tape Library Multimedia
Enter Choice [1-4]:
```

8. You are prompted to enter the volume group, by a menu similar to the following. You may do any of the following actions:
- ◆ Choose from any existing standalone volume groups that allow this volume's media type.
  - ◆ Elect not to associate the volume with any volume group (if the option is offered).
  - ◆ Enter a new name of your own choice.
  - ◆ Have a name generated by `vmadm`, if the name of volume group is not important in this case.

```
Volume Group
-----
1)  tl8grp1
2)  No Volume Group
3)  Specify New Volume Group Name
4)  Auto-Generate New Volume Group Name
Enter choice:
```

9. The action taken next depends on the media type you selected.
- ◆ If you selected a tape media type, the volume is added at this point and you are returned to the main menu.
  - ◆ If you selected an optical disk, you are given the option to format the platters using `tpformat`. (Formatting may cause an operator mount request to occur on the host.) Choosing `n` adds the volume immediately and you are returned to the main menu. If you choose `y` and the formatting does not complete, the volumes are still added.

---

**Note** All platforms and operating systems do not support 1024 byte-per-sector platters. Most support only 512 byte-per-sector sizes. Before purchasing optical disk platters, check your vendor documentation to determine the sector sizes supported by your platform and operating system. VERITAS urges you to use platters that have been formatted.

---



## Adding a Range of Standalone Volumes

### ▼ To add a range of volumes

1. On the main menu, choose a for Add Volumes.
2. The following prompt appears. Enter r to add a range of volumes.  
Add Single Volume, Range of Volumes, or Auto-Populate? (s/r/a):
3. You are prompted for the media type with a menu similar to the following that displays the possible types. Enter the number for the type of media you want to add.

```
Adding Range of Volumes
-----
Media Type
-----
1)  1/4" cartridge tape
2)  1/2" cartridge tape
3)  1/2" cartridge tape 2
4)  1/2" cartridge tape 3
5)  4MM cartridge tape
6)  8MM cartridge tape
7)  8MM cartridge tape 2
8)  8MM cartridge tape 3
9)  DLT cartridge tape
10) DLT cartridge tape 2
11) DLT cartridge tape 3
12) DTF cartridge tape
13) Optical disk rewritable
14) Optical disk WORM
15) 1/2" cleaning tape
16) 1/2" cleaning tape 2
17) 1/2" cleaning tape 3
18) 4MM cleaning tape
19) 8MM cleaning tape
20) 8MM cleaning tape 2
21) 8MM cleaning tape 3
22) DLT cleaning tape
23) DLT cleaning tape 2
24) DLT cleaning tape 3
25) DTF cleaning tape
Enter Choice [1-25]:
```



4. If you selected to add a range of cleaning tapes, you are prompted to enter a single number which indicates the number of cleanings you want available on each volume in the range. For any other media type, the next step occurs immediately.
5. You are prompted for a description. Enter 1 to 25 characters of text to describe the media being added. This description applies to all of the volumes in the range.
6. If the media is not a cleaning media type, you are prompted to enter a number for the volume pool, as follows:
  - ◆ Enter 1 for a range of standalone volumes. If you enter 1, the volumes are associated with a generic volume pool and are available to any user or application.
  - ◆ Enter 2 if you want the volumes to be available to NetBackup only.
  - ◆ Enter another choice to have the volumes assigned to one of the volume pools listed.

```
Volume Pool
-----
1)  None
2)  NetBackup
3)  DataStore
4)  CatalogBackup
5)  oldpool
6)  oldpool4
7)  POOL1
8)  POOL2
Enter Choice:
```

7. You are prompted to enter the physical location of the volumes using a menu of possible locations, similar to the following menu for an 8mm cartridge tape:

```
Physical Location
-----
1)  Not in robotic device
2)  TL8 - Tape Library 8MM
3)  TLD - Tape Library DLT
3)  TLM - Tape Library Multimedia
Enter Choice [1-4]:
```



8. You are prompted to enter the volume group, by a menu similar to the following. You can do any of the following actions:
- ◆ Choose from any existing standalone volume groups that allow this volume's media type.
  - ◆ Elect not to associate the volume with any volume group (if the option is offered).
  - ◆ Enter a new name of your own choice.
  - ◆ Have a name generated by `vmadm`, if the name of volume group is not important in this case.

```
Volume Group
-----
1)  tl8grp1
2)  No Volume Group
3)  Specify New Volume Group Name
4)  Auto-Generate New Volume Group Name
Enter choice:
```

9. You are prompted to enter the media ID naming mode with a menu displaying the possible modes. If you selected an optical disk media type, the display is as follows.

If you selected any device other than an optical disk media type, only options a through d or e are displayed, depending on the robot type.

```
Media ID Naming Mode
-----
a)  0 characters and 6 digits
b)  1 character  and 5 digits
c)  2 characters and 4 digits
d)  3 characters and 3 digits
e)  4 characters and 2 digits
f)  0 characters, 5 digits, and 1 character platter-side
g)  1 character,  4 digits, and 1 character platter-side
h)  2 characters, 3 digits, and 1 character platter-side
i)  3 characters, 2 digits, and 1 character platter-side
j)  4 characters, 1 digit,  and 1 character platter-side
Enter Choice:
```

Enter the desired naming mode. When the volumes are added, the digit field is incremented by one for each volume. (Only numbers are incremented.)

**10.** You are prompted for the media ID of the first volume:

Enter Media ID for first volume -- using naming mode e:

If you had selected naming mode e and entered the 4-character, 2-digit ID, tape01, the media ID of the first volume added would be TAPE01, the second TAPE02, and so on.

**11.** You are prompted for the number of volumes to add.

**a.** If you selected an optical disk media type, the prompt is as follows:

Enter Number of Platters (2 Volumes/Platters) in Range:

Each side of a platter is considered one volume. Entering the number 4, for example, causes eight volumes (four platters) to be added.

You are then given the option to format the platters being added using `tpformat`. Choosing n (no) adds the volumes immediately and you are returned to the main menu.

**b.** If you selected any media type other than optical disk, the prompt is as follows:

Enter Number of Volumes in Range:

**12.** The volumes are added to the database and you are returned to the main menu.

If any volume cannot be added (for example, if the range you specified overlaps with existing volumes), the operation aborts but volumes added before the failure remain in the database.

## Adding Volumes to a Robot

### Auto-Populating a Robot

You can use auto-populate for robots that support barcodes and for robots that do not support barcodes with some operational limitations (see “Robot Attributes” on page 311). The easiest way to add new media to a robot is to physically add the media and then use Media Manager’s auto-populate feature to update the EMM database to agree with the contents of the robot. The database update includes automatic creation of media IDs.

If the robot *supports* barcodes and the volumes have readable barcode labels, auto-populate generates media IDs for new volumes based on the last six characters of the barcodes as the default or the specific characters that you specify if you are using Media ID generation rules.



When you use barcode rules, new media that is added through a barcode rule is also assigned a media type, pool name, maximum number of mounts (or cleaning count), and description (see “Configuring Barcode Rules” on page 477).

If the robot *does not* support barcodes or the media does not have readable barcodes, the new media IDs are based on a media ID prefix that you specify.

## Using Auto-Populate

The auto-populate operation is the same as an inventory and update operation (see “Inventory and Update Robot Volume Configuration” on page 465).

### ▼ To use auto-populate

The following procedure refers you to the update procedure at the proper time.

1. Insert the new media into the robot.
2. Check the barcode capabilities of the robot and its media.  
Before starting an auto-populate operation, perform “Inventory and Compare Robot Volume Configuration” on page 463 and check whether the following are true:
  - ◆ The robot supports barcodes.
  - ◆ The new media that was inserted has readable barcodes.
3. 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 verify for reference, in case you assign a media ID prefix later in this procedure. You do not need a prefix if the robot supports barcodes and the media has a readable barcode.

You also may want to consider using the physical inventory utility (see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354).

4. Create barcode rules (optional).  
Refer to “Configuring Barcode Rules” on page 477 and create any additional barcode rules that you want to use for auto-populating the database, for the media you have inserted into the robot.
5. For robot types that are not API robots, create media ID generation rules (optional).  
See “Media ID Generation Tab (Advanced Options)” on page 207 for more information.



6. For API robots, create media type mappings for the robot as explained in step 2 under “Changing Update Options” on page 469

You can change the default media type mappings as explained in “Adding Mapping Entries to vm.conf” on page 213.

7. Ensure that the appropriate control daemons are active on the robot control host.
8. On the main menu, choose a for Add Volumes.
9. Respond to the prompt with a, to use auto-populate.

This brings up a robot selection prompt for selecting the robot where you added the media.

The remaining steps are the same as for a robot inventory and update operation. Go to step 8 under “Inventory and Update Robot Volume Configuration” on page 465.

## Adding a Single Volume to a Robot (Without Auto-Populate)

The following procedure explains how to add a single volume to a robot using the s option, rather than using Auto-Populate.

---

**Note** The first seven steps of this procedure are the same as adding a standalone volume (see “Adding a Single Standalone Volume” on page 424) and are only summarized here. Refer to that procedure for details.

---

### ▼ To add a volume

1. On the main menu, choose a for Add Volumes.
2. Respond to the prompt with s, to add a single volume.
3. Enter the number for the type of media you want to add.  
If you selected a cleaning tape, enter the number of cleanings you want available.
4. Enter a single media ID for tape or two media IDs for an optical disk. A Media Manager media ID can contain from 1 to 6 characters.

---

**Note** Media IDs for API robots must always match the barcodes. This means that you must get a list of the barcode labels prior to adding the volumes to Media Manager. You can obtain this information from the interface that is provided by the robot vendor or operating system, or you can use one of the robotic inventory options on the Special Actions menu.

---



5. Enter a media description (1 to 25 characters).
6. Select a volume pool.
7. Specify that you want the volume added to a robot. You are prompted to enter the physical location of the volume using a menu of possible locations, similar to the following menu for an 8mm cartridge tape:

```
Physical Location
-----
1)  Not in robotic device
2)  TL8 - Tape Library 8MM
3)  TLD - Tape Library DLT
4)  TLM - Tape Library Multimedia
Enter Choice [1-4]:
```

Enter the number of the type of device to which you want to add a volume. If a device of the specified type does not currently exist, step 9 occurs immediately.

8. The devices of the selected type that currently have volumes in the database are displayed, along with the option to specify a new one, similar to the following. Enter the number of the robot you want to add to, or n to specify a new robot.

```
Applicable Robot List
-----
22)  TL8 - Tape Library 8MM  (bobcat)
n)   New Robot Number
Enter Choice:
```

9. If you enter n or the robot you chose does not exist, you are prompted for a new, unique robot number (which must match the number that will be used when you configure the robot or was used when you configured the robot), and the new robot control host (where the robotics are controlled). Otherwise, the next step occurs.

*The following point applies only to NetBackup Enterprise Server.*

No robot control host name is requested for an ACS or TLM robot.

10. You are prompted for specific information about the volume and where it should go. This information varies depending on the type of robot to which the volume is being added.
  - ◆ If the robot is an API robot, you do not enter slot information. Media Manager does not require slot location for those robot types because this information is tracked by the robot vendor software.
  - ◆ If the robot is not an API robot, you are prompted to enter the slot number.

11. You are prompted to enter the volume group by a menu similar to the following. You may choose from any existing volume groups on the device.

```
Volume Group
-----
1)  t18grp1
2)  Specify New Volume Group Name
3)  Auto-Generate New Volume Group Name
Enter choice:
```

12. For some robots, you are asked whether the volume should be injected using the media access port. For an ODL robot, you are asked whether the platters should be formatted.

---

**Note** The inject prompt occurs for robot types that support media access ports. This prompt may appear for some robots that do not have these ports, since the Media Manager robot type for the robot only indicates that media access ports are possible.

---

13. A reminder to insert the volume in the media access port or into the specified slot of the robot is displayed, and you are then returned to the main menu.

If you do not insert the volume now, it is still added to the database and logically associated with the robot.

If the robot is not an API robot and it has a barcode reader, the barcode is read and added to the database when you add the volume, provided you also physically insert the volume in the proper slot.

If you insert the volume later, then you must use Update/Validate Barcodes for Volumes on the Special Actions menu at that time (see “Updating Barcodes for Selected Volumes in a Robot” on page 460).

## Adding a Range of Volumes to a Robot (Without Auto-Populate)

The following procedure explains how to add a range of volumes to a robot by using the `r` option, rather than Auto-Populate.

---

**Note** The first six steps of this procedure are the same as adding a standalone volume (see “Adding a Range of Standalone Volumes” on page 428) and are only summarized here. Refer to that procedure for details.

---



▼ **To add a range of volumes**

1. On the main menu, choose a for Add Volumes.
2. Respond to the prompt with r, to add a range of volumes.
3. Enter the number for the type of media you want to add.
4. If you selected a range of cleaning tapes, enter a single number that indicates the number of cleanings you want available on each volume in the range.
5. Enter a description (1 to 25 characters) that applies to all media in the range.
6. Select a volume pool.
7. Specify that you want to add the volumes to a robot. You are prompted for the physical location of the volumes using a menu of possible locations, similar to the following menu for an 8 mm cartridge tape:

```
Physical Location
-----
1)  Not in robotic device
2)  TL8 - Tape Library 8MM
3)  TLD - Tape Library DLT
4)  TLM - Tape Library Multimedia
Enter Choice [1-4]:
```

Enter the number of the type of robot to which you want to add the volumes. (If a device of the specified type does not currently exist, step 8 is skipped and step 9 occurs.)

8. The devices of the selected type that currently exist in the database are displayed, along with the option to specify a new robot, similar to the following. Enter the number of the robot you want to add to, or n to specify a new robot.

```
Applicable Robot List
-----
22) TL8 - Tape Library 8MM  (bobcat)
n)  New Robot Number
Enter Choice:
```

9. If you enter n or the robot you chose does not exist, you are prompted for a new, unique robot number and a new control host. Otherwise, the next step occurs.

*The following point applies only to NetBackup Enterprise Server.*

No robot control host name is requested for an ACS or TLM robot.



- 10.** You are prompted to enter the volume group, by a menu similar to the following. You may choose from any existing volume groups on the device.

```
Volume Group
-----
1)  t18grp1
2)  Specify New Volume Group Name
3)  Auto-Generate New Volume Group Name
Enter choice:
```

- 11.** You are prompted for specific information about the volume and where it should go. This information varies depending on the type of robot to which the volume is being added.

If the robot is an API robot, you do not enter slot information. Media Manager does not require slot location for those robot types, because this information is tracked by the robot vendor software.

If the robot is not an API robot, you are prompted to enter the slot number for the volume.

- 12.** At this point, the procedure is similar to adding a standalone volume. You are prompted to enter the media ID naming mode with a menu displaying the possible modes.

---

**Note** Media IDs for API robots must always match the barcodes. This means that you must get a list of the barcode labels prior to adding the volumes to Media Manager. You can obtain this information from the interface that is provided by the robot vendor or operating system, or you can use one of the robotic inventory options on the Special Actions menu.

---



If you selected an optical disk media type, the following display appears. If you selected any device other than an optical disk media type, only options a through d or e are displayed, depending on the robot type.

```
Media ID Naming Mode
-----
a)  0 characters and 6 digits
b)  1 character  and 5 digits
c)  2 characters and 4 digits
d)  3 characters and 3 digits
e)  4 characters and 2 digits
f)  0 characters, 5 digits, and 1 character platter-side
g)  1 character,  4 digits, and 1 character platter-side
h)  2 characters, 3 digits, and 1 character platter-side
i)  3 characters, 2 digits, and 1 character platter-side
j)  4 characters, 1 digit,  and 1 character platter-side
Enter Choice:
```

Enter the desired naming mode. When the volumes are added, the digit field is incremented by one for each volume. Only numbers are incremented.

- 13.** For all devices other than an API robot, you are prompted for the media ID of the first volume. The prompt is appropriate for the media type and is similar to one of the following prompts (xxx is the slot number you entered in step 11):

```
Enter Media ID for slot xxx, side A -- using naming mode e:
Enter Media ID for slot xxx -- using naming mode a:
Enter 3 Character Prefix for ALL Media IDs:
```

If you had selected naming mode e and entered the ID, tape01, the media ID of the first volume added would be TAPE01, the second TAPE02, and so on.

- 14.** You are prompted for the number of volumes to add.

- a.** If you selected an optical disk media type, the prompt is as follows, where x and y represent the range of platters available.

```
Enter Number of Platters (2 Volumes/Platter) in Range [x-y]:
```

For example, entering 4 causes eight volumes (four platters) to be added.

You are then given the option to format the platters being added using `tpformat`. Choosing n (no) adds the volumes immediately and you are returned to the main menu.



- b. If you selected a media type other than optical disk, the prompt is as follows, where x and y represent the range of volumes available. A range is not presented if the robot is an API robot.

Enter Number of Volumes in Range [x-y]:

15. The volumes are added to the database and you are returned to the main menu.

If any volume cannot be added (for example, if the range you specified overlaps with existing volumes), the operation aborts, but volumes added before the failure remain in the database.

If you do not insert the volume now, it is still added to the database and logically associated with the robot.

If the robot is not an API robot and it has a barcode reader, the barcode is read and added to the database when you add the volume, providing you also physically insert the volume in the proper slot. If you insert the volume later, then you must use Update/Validate Barcodes for Volumes on the Special Actions menu at that time (see “Updating Barcodes for Selected Volumes in a Robot” on page 460).

## Displaying the Volume Configuration

### ▼ To display a volume configuration

1. On the `vmadm` menu, choose `p` for Print Information about Volumes. The current print criteria are displayed along with a menu which allows you to change the criteria, similar to the following example:

```

Display Filter:  ALL
Display Mode:   BRIEF
Output Destination:  SCREEN

Display Options
-----
s) Search
m) Mode (brief or full)
o) Output Destination (screen or file)
f) Filter
h) Help
q) Quit Menu
ENTER CHOICE:
```

2. To accept the current settings, select `s` for Search. With the settings shown above in the example, you would receive brief information about all volumes on your screen.



**3.** To change the print criteria, select one of the following options:

- m       Toggles the display mode.  
FULL mode displays the most extensive information about each selected volume.  
BRIEF mode displays a subset, one line of information about each selected volume. In this mode, volumes are listed in alphabetical order by media ID. The default mode is BRIEF.
- o       Toggles the output destination between the screen and a file of your choice. When you switch from the screen setting to a file, you are prompted for the file name. You must enter an absolute path or the enter key for the default file `/tmp/vmadm_output`.
- f       Changes the display filter that determines which volumes are displayed. The following options are shown:
  - 1) ALL
  - 2) MEDIA ID
  - 3) MEDIA TYPE
  - 4) VOLUME GROUP
  - 5) ROBOT NUMBER
  - 6) ROBOT TYPE
  - 7) VOLUME POOL
  - 8) VAULT CONTAINER IDFor entries 2 through 8, you are prompted to enter the appropriate value. Menus of the possibilities are provided for entries 3 through 7. For entry 8, the dash character clears the Vault container ID. The default is the last value chosen and is always shown in parentheses following the prompt. Initially, information about all volumes is shown.

After you change a print option, you must select `s` for the information to be printed or displayed. If you choose to copy the information to a file, you receive a message after you select `s` that output is written to the file. `vmadm` uses the `more` utility to display information on the screen.





The amount of information displayed depends on the mode that you specify. FULL mode displays all available information about the selected volumes in a format similar to the following example for a single volume:

```

media ID:                MIN028
media type:              8MM cartridge tape (4)
barcode:                00000018
media description:      configured by GJK
volume pool:            POOL2 (7)
robot type:             TL8 - Tape Library 8MM (6)
robot number:           0
robot slot:             28
robot control host:     hare
volume group:           TL8-0
vault name:             V1
vault sent date:        Wed Dec 02 09:34:01 1993
vault return date:      Tue Feb 17 09:34:01 1994
vault slot:             546
vault session id:       37
vault container id:     offsite32
created:               Mon Nov 29 08:39:09 1993
assigned:              Tue Nov 30 20:51:28 1993
last mounted:          Sun Dec  5 20:51:49 1993
first mount:           Tue Nov 30 20:54:00 1993
expiration date:       ---
number of mounts:       6
max mounts allowed:     ---
status:                0x0

```

For a standalone volume, fields that do not apply (for example, robot type, robot number, and so on) are not included in the FULL mode display.

For a cleaning tape, number of mounts is replaced by cleanings left.

The status field is not displayed unless the media is assigned.

BRIEF mode displays a subset of the most pertinent information, showing one line per volume, by default in alphabetical order by media ID, similar to the following example:

| media<br>ID | media<br>type | robot<br>type | robot<br># | robot<br>slot | side/<br>face | optical<br>partner | # mounts/<br>cleanings | last<br>mount time |
|-------------|---------------|---------------|------------|---------------|---------------|--------------------|------------------------|--------------------|
| 000001      | DLT           | TLD           | 1          | 1             | -             | -                  | 17                     | 06/03/1996 00:01   |
| 000002      | DLT           | TLD           | 1          | 12            | -             | -                  | 14                     | 06/03/1996 00:02   |
| 000022      | DLT           | TLD           | 0          | 7             | -             | -                  | 1                      | 04/18/1996 09:25   |



Even when the same kind of information is returned, such as media type and robot type, the FULL display expands the description and is more complete. With an optical disk, for example, BRIEF mode shows a media type of REWR\_O while FULL mode shows Rewritable optical disk. When using brief mode, some media attributes may not fit within the limited field width. For example, only 6 characters of the media type attribute are displayed.

## Moving Volumes

When you move volumes in or out of a robot, or from one robot to another, you must physically and logically move the volume. The physical part of the move is when you remove or insert the volume. The logical move changes the EMM database to show the volume at the new location.

You can perform the following types of logical moves:

- ◆ Move single volumes
- ◆ Move multiple volumes
- ◆ Move volume groups

Common instances where you use the move options are:

- ◆ Replacing full volumes in a robot. When a robotic volume is full and there are no more empty slots in the robot, you move the full volume to standalone, and then configure a volume for the empty slot or move a volume into that slot. You could use a similar process to replace a defective volume.
- ◆ Moving volumes from a robot to an offsite location or from an offsite location into a robot. When you move tapes to an offsite location you move them to standalone.
- ◆ Moving volumes from one robot to another (for example, if a robot is down).

## Moving Volumes (With Inventory and Update)

Inventory a Robot and Update Volume Configuration on the Special Actions menu provides the easiest way to logically move media when the following are true:

- ◆ The move involves a robot that supports barcodes, see “Robot Attributes” on page 311.
- ◆ The media has readable barcodes.

See “Inventory and Update Robot Volume Configuration” on page 465 for instructions on using this option.

If the robot does not support barcodes or the barcodes are unreadable, use one of the following:

- ◆ The move procedures explained in the following topics.
- ◆ The physical inventory utility (see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354).

## Moving a Single Volume (Without Inventory and Update)

Moving a volume in `vmadm` changes only its logical residence in the EMM database. It must also be moved physically, unless it is injected or ejected using the media access port.

When you move a volume to a non-API robot that has a barcode reader, Media Manager performs a Validate and Update Barcode operation on that volume.

### ▼ To move a volume

1. On the main menu, choose `m` for Move Volumes.
2. The following prompt is displayed. Enter `s` to move a single volume.  
Move Single Volume, Multiple Volumes, or Volume Group? (s/m/v):
3. You are prompted for the media ID of the volume you want to move.

```
Changing Volume Residence
-----
Enter Media ID:
```



4. The current residence of the volume is displayed, along with the possible locations to which it could be moved, similar to the following example:

```
Current Residence of 000003:
robot type:          TL8 - Tape Library 8MM   (6)
robot number:        10
robot control host:  dill
volume group:        Scal000
robot slot:          4
barcode:             000003
```

New Residence:

```
Physical Location
-----
1)  Not in robotic device
2)  TL8 - Tape Library 8MM
3)  TLD - Tape Library DLT
4)  TLM - Tape Library Multimedia
Enter Choice [1-4]: (2)
```

5. Enter the new residence for the volume.
- a. If you move a volume out of an ODL, TSH, TLD, or TL8 robot to a standalone location, you are asked whether the volume should be ejected using the media access port. This is the final step in the procedure.

---

**Note** This prompt occurs for robot types that support media access ports (and if `vmadm` supports the eject operation for the robot type). This prompt may be shown for some robots that do not have this support, since the robot type for the robot only indicates that media access ports are possible.

---

- b. If you choose to move a volume into a robot, you are prompted with a menu of possible robots, similar to the following.

Enter the number of the appropriate robot. If you choose `n`, you are prompted to enter a new robot number and robot control host.

```
Applicable Robot List
-----
10) TL8 - Tape Library 8MM (dill)
20) TL8 - Tape Library 8MM (dill)
n)  New Robot Number
Enter choice:
```

- c. You are prompted for specific information about where the volume should be moved. This information varies depending on the device to which the volumes are being moved.
  - ◆ If the robot is an API robot, see step 6.
  - ◆ If the robot is not an API robot, you are prompted for the tape slot where the volume should be moved.
6. You are prompted to enter the volume group. You may do any of the following actions:
  - ◆ Choose from any volume groups in the list.
  - ◆ Elect not to associate the volume with any volume group (if the option is offered).
  - ◆ Enter a new name of your own choice.
  - ◆ Have a name generated by `vmadm`, if the name of volume group is not important in this case.

```

Volume Group
-----
1)  tl8grp1
2)  No Volume Group
3)  Specify New Volume Group Name
4)  Auto-Generate New Volume Group Name
Enter choice:

```
7. If you move a volume from or to robots that support media access ports (and `vmadm` supports that robot with `eject` or `inject`), you are asked whether the volume should be ejected and then injected using the media access port.

## Moving Multiple Volumes

Moving multiple volumes is similar to moving single volumes, except that once you choose where you want the volumes to be moved, you are prompted to continue entering media IDs of volumes to move. You also do not have the option to eject and inject volumes using the media access port.

Moving volumes in `vmadm` changes only their logical residence in the EMM database. They must also be moved physically. When you move volumes to a non-API robot that has a barcode reader, Media Manager performs a Validate/Update Barcode operation on those volumes.



▼ **To move multiple volumes**

1. On the main menu, choose m for Move Volumes.
2. The following prompt is displayed. Enter m to move multiple volumes:  
Move Single Volume, Multiple Volumes, or Volume Group? (s/m/v):

3. You are prompted for the media ID of the first volume you want to move:

```
Moving Volumes
-----
Enter First Media ID:
```

4. If you are moving a volume on an optical disk, you are reminded that moving the volume on one side of the platter also moves the volume on the other side.

The current residence of the volume is displayed, along with the possible locations to which it could be moved, similar to the following menu. Enter the new residence for the volumes.

```
Current Residence for all volumes in list:
robot type:          TL8 - Tape Library 8MM  (6)
robot number:        10
robot control host:  dill
volume group:        Sca1000
robot slot:          3
barcode:             000002
```

New Residence for all volumes in list:

```
Physical Location
-----
1)  Not in robotic device
2)  TL8 - Tape Library 8MM
3)  TLD - Tape Library DLT
4)  TLM - Tape Library Multimedia
Enter Choice [1-4]: (2)
```



5. If you move the volumes into a robot, you are prompted with a menu of possible libraries, similar to the following. Enter the number of the appropriate robot. If you choose n, you are prompted to enter a new robot number and a new robot control host.

```
Applicable Robot List
-----
10) TL8 - Tape Library 8MM (dill)
20) TL8 - Tape Library 8MM (dill)
n) New Robot Number
Enter choice:
```

6. You are prompted to enter the volume group. You may do any of the following actions:

- ◆ Choose from any volume groups in the list.
- ◆ Elect not to associate the volume with any volume group (if the option is offered).
- ◆ Enter a new name of your own choice.
- ◆ Have a name generated by `vmadm`, if the name of volume group is not important in this case.

```
Volume Group
-----
1) tl8grp1
2) No Volume Group
3) Specify New Volume Group Name
4) Auto-Generate New Volume Group Name
Enter choice:
```

7. Depending on the device, you are prompted for a media ID or to specify location information for each volume.

---

**Note** You do not enter slot information for media added to an API robot. Media Manager does not require slot location for these robot types, since this information is tracked by the operating system or the robot vendor software.

---

8. At this point, the volumes are moved, messages confirming the moves are displayed, and you are returned to the main menu.



## Moving a Volume Group

A volume group can be moved to a new robot or made standalone. All volumes must have their new slot numbers identified, as the move operation leaves slot numbers unmodified.

Moving volumes in `vmadm` changes only their logical residence in the EMM database. They must also be moved physically.

See “Volume Pools and Volume Groups” on page 344, for a definition of a volume group.

---

**Note** If a volume group is moved back into a robot, every volume must be returned to its original slot.

---

### ▼ To move a volume group

1. On the main menu, choose `m` for Move Volumes.
2. The following prompt is displayed. Enter `v` to move a volume group.  
`Move Single Volume, Multiple Volumes, or Volume Group? (s/m/v):`

3. A menu of possible groups is displayed, similar to the following menu. Enter the number of the volume group you want to move.

```
Volume Group
-----
1)  00_025_TL8
2)  10i-1
3)  10i-2
4)  axc
Enter choice:
```

4. The current residence of the volume group is displayed, along with a prompt to choose the new location, similar to the following:

```
Current Residence for Volume Group 00_025_TL8:
-----
robot type:          TL8 - Tape Library 8MM  (3)
robot number:        25
robot control host:  bobcat

New Residence:

Physical Location
-----
1)  Not in robotic device
Enter Choice [1-1]: (1)
```





You can move a volume group only between a robotic location and standalone. To move a group from one robot to another, you must move the group to standalone, as an intermediate step, and then to the new robot.

5. If you selected a standalone volume group to move, the physical locations listed would not offer option (1), but would show the robot type to which the volumes could be moved, as in the following sample menu:

```
New Residence:
Physical Location
-----
1)  TL8 - Tape Library 8MM
2)  TLD - Tape Library DLT
3)  TLM - Tape Library Multimedia
Enter Choice [1-3]:
```

Enter the new residence for the volume group. The volumes are logically moved and you are returned to the main menu.

## Deleting a Single Volume

The volume is deleted from the EMM database, not physically from the device.

---

**Note** You cannot delete volumes that are assigned until they are unassigned. Only NetBackup and Storage Migrator use the assigned state. See “Deassigning Volumes” on page 161 for more information.

---

### ▼ To delete a volume

1. On the main menu, choose d for Delete Volumes.
2. The following prompt appears. Enter s to delete a single volume.  

```
Delete Single Volume, Multiple Volumes, or Volume Group? (s/m/v):
```
3. You are then prompted for the media ID of the volume you want to delete:  

```
Deleting Volume
-----
Enter Media ID:
```



4. If you are deleting an optical disk volume, you get the following additional warning and prompt (xxxxxA and xxxxxB represent the media IDs of sides A and B of the volume's platter). Entering n cancels the operation. Entering y continues the operation.

```
Deleting volume xxxxxA will also delete xxxxxB
are you sure you want to delete both volumes? (y/n):
```

5. The deletion is confirmed with a message, and you are returned to the main menu.

## Deleting Multiple Volumes

The volumes are deleted from the EMM database, not physically from the device.

---

**Note** You cannot delete volumes that are assigned until they are unassigned. Only NetBackup and Storage Migrator use the assigned state. See "Deassigning Volumes" on page 161 for more information.

---

### ▼ To delete multiple volumes

1. On the main menu, choose d for Delete Volumes.

2. The following prompt appears. Enter m to delete multiple volumes.

```
Delete Single Volume, Multiple Volumes, or Volume Group? (s/m/v):
```

3. You are prompted for the media ID of the volume you want to delete:

```
Deleting Volumes
-----
Enter Media ID:
```

4. If you are deleting an optical disk volume, you get the following additional warning (xxxxxA and xxxxxB represent the media IDs of sides A and B of the volume's platter).

```
Deleting volume xxxxxA will also delete xxxxxB
```

5. Pressing the Escape key cancels the operation. Continuing causes the volume to be deleted, when all the desired volumes have been entered. You continue to be prompted for media IDs until you press only the Enter key.

The volumes are deleted, messages confirm each deletion, and you are returned to the main menu.



## Deleting a Volume Group

The volume is deleted from the EMM database, not physically from the device.

---

**Note** You cannot delete volumes that are assigned until they are unassigned. Only NetBackup and Storage Migrator use the assigned state. See “Deassigning Volumes” on page 161 for more information.

---

### ▼ To delete a volume group

1. On the main menu, choose **d** for Delete Volumes.
2. The following prompt appears. Enter **v** to delete a volume group.  
Delete Single Volume, Multiple Volumes, or Volume Group? (s/m/v):
3. A menu of the possible volume groups is displayed, similar to the following. Enter the number of the volume group you want to delete.

```
Volume Group
-----
1)  00_025_TL8
2)  10i-1
3)  10i-2
4)  cc
Enter choice:
```

4. The volumes in the specified group are deleted and you are returned to the main menu.

## Changing a Volume's Description

### ▼ To change a description for a volume

1. On the main menu, choose **s** for Special Actions.
2. Choose **d** for Change Media Description for Volume.
3. The following prompt appears. Enter the media ID of the volume whose description you want to change.

```
Changing Media Description for Volume
-----
Enter Media ID:
```



4. The current media description and a prompt for the new description is displayed. Enter the new description and press Enter. You are returned to the Special Actions menu.

```
Current Media Description for 000000: test
Enter Media Description (25 char max):
```

## Changing a Volume's Volume Pool

Volumes are in a specific volume pool or are associated with a generic volume pool. The volume pool row in the Print Information about Volumes FULL display mode, shows the name of the volume pool to which the volumes belong (if any).

Once associated with a pool, volumes are assigned or unassigned. Only the NetBackup and Storage Migrator applications use the assigned state. A NetBackup or Storage Migrator volume becomes assigned when it is requested by a user or an application. The time of the assignment appears in the assigned row in the Print Information about Volumes FULL display mode.

A volume must be in an unassigned state before you can change its volume pool. Attempting to change its volume pool while the volume is assigned results in an error.

Changing the volume pool for an optical disk volume also changes the volume pool for its partner volume.

### ▼ To change a volume pool for a volume

1. Unassign the volume if it is assigned to NetBackup (See “Deassigning Volumes” on page 161 for more information).
2. On the main menu, choose s for Special Actions.
3. Choose p for Change Volume Pool for Volumes. The list of defined volume pools appears. You can do any of the following actions:
  - ◆ Enter 1, if you want the volume associated with the generic volume pool; the volume will be available to any user or application.
  - ◆ Enter 2 if you want the volume to be available only to NetBackup.

- ◆ Enter another choice to have the volume associated with one of the volume pools listed.

```
Changing Volume Pool for Volumes
-----
Volume Pool
-----
1)  None
2)  NetBackup
3)  DataStore
4)  CatalogBackup
5)  oldplatters
6)  newplatters
7)  POOL1
8)  DataStore
Enter Choice:
```

4. You are prompted for the media ID of the volume to change. You will continue to be prompted for media IDs until you press the Enter key without typing a media ID.

## Changing the Expiration Date for Volumes

The administrator can change the expiration date for any volume in the EMM database. The expiration date refers to the age of the media (not the data on the media) and is the time at which the media is considered too old to be reliable.

When its expiration date has passed a volume can still be read, but it will not be mounted for a write access. Requesting write access to a volume whose expiration date has passed results in an error; requesting read access results in a warning being logged to the system console log.

You can set or change an expiration date for a single volume or for multiple volumes.

### ▼ To change the expiration date for a volume

1. On the main menu, choose s for Special Actions.
2. Choose e for Change Expiration Date for Volumes.



3. At the prompt, enter 0 for no expiration date or enter a date in one of the following formats:
  - ◆ mm/dd/yy hh/mm/ss
  - ◆ mm/dd/yyyy hh/mm/ss
  - ◆ mm/dd/yy
  - ◆ mm/dd/yyyy
  - ◆ mm/dd
4. You are then prompted to enter the media ID of the volume to associate with this expiration date. You will continue to be prompted for media IDs until you press the Enter key without typing a media ID.

## Changing the Volume Group for Volumes

### ▼ To change a volume group for a volume

1. On the main menu, choose s for Special Actions.
2. Choose g for Change Volume Group for Volumes. The following prompt appears:

```
Changing Volume Group for Volumes
```

```
-----
```

```
Enter Media ID:
```

Enter the media ID of the first volume you want to change and press Enter. You will continue to be prompted for media IDs until you press the Enter key without typing a media ID.

As you enter the media IDs, Media Manager validates them to ensure they have common media types and residences.

3. When you exit from this prompt, a list similar to the following appears. The list will include existing volume groups that are valid for the media you specified in step 2, (00\_000\_TL8 is the volume group in this example), and also have options for specifying a new volume group name or having `vmadm` generate a new name.

```
Volume Group
-----
1) 00_000_TL8
2) Specify New Volume Group Name
3) Auto-Generate New Volume Group Name
Enter Choice:
```

If you choose to specify a new volume group name, a prompt appears allowing you to enter the name.

## Change Vault Name for Volumes

You can set, clear, or change the vault name that contains the volume. This field is used by NetBackup Vault to determine what offsite location the volume is located in while off site.

You can change the vault name for a single volume or for multiple volumes.

### ▼ To change the vault name

1. On the main menu, choose `s` for Special Actions.
2. Choose `a` for Change Vault Parameters for Volumes.
3. Choose `n` for Change Vault Name for Volumes. The following prompt appears. Enter the new vault name. Entering a hyphen means that the name will be cleared.

```
Changing Vault Name for Volumes
-----
(enter '-' to clear vault name)
Enter Vault Name(25 chars max):
```

4. You are prompted for the media IDs for which you want this vault name applied. You will continue to be prompted for media IDs until you press the Enter key without typing a media ID. If you enter the ESC key, your changes will not be applied.



## Change Date Volumes are Sent to Vault

You can set, clear, or change the date a volume is sent to the vault. This field is used by NetBackup Vault to record when a volume was sent to an offsite vault.

You can change the date for a single volume or for multiple volumes.

### ▼ To change the date

1. On the main menu, choose **s** for Special Actions.
2. Choose **a** for Change Vault Parameters for Volumes.
3. Choose **s** for Change Date Volumes are sent to Vault. The following prompt appears. Enter the new date the volume is sent off site. Entering 0 means that the date will be cleared.

```
Changing Date Volume(s) Sent to Vault
-----
(vault sent date of 0 means clear entry)
Enter date volume(s) sent to vault:
```

4. You are prompted for the media IDs for which you want this date applied.  
You will continue to be prompted for media IDs until you press the Enter key without typing a media ID. If you enter the ESC key, your changes will not be applied.

## Change Date Volumes Return from Vault

You can set, clear, or change the date a volume returns from the vault. This field is used by NetBackup Vault to record when a volume is requested to be returned from the vault.

You can change the date for a single volume or for multiple volumes.

### ▼ To change the date

1. On the main menu, choose **s** for Special Actions.
2. Choose **a** for Change Vault Parameters for Volumes.





3. Choose **r** for Change Date Volumes return from Vault. The following prompt appears. Enter the new date. Entering 0 means that the date will be cleared.

```
Changing Date Volume(s) return from Vault
-----
(vault return date of 0 means clear entry)
Enter date volume(s) return from vault):
```

4. You are prompted for the media IDs for which you want this date applied.  
You will continue to be prompted for media IDs until you press the Enter key without typing a media ID. If you enter the ESC key, your changes will not be applied.

## Change Vault Slot for Volumes

You can set, clear, or change the slot that the volume is contained in at the vault. This field is used by NetBackup Vault to determine what slot the volume is located in while in the vault.

You can change the slot for a single volume or for multiple volumes.

### ▼ To change the slot

1. On the main menu, choose **s** for Special Actions.
2. Choose **a** for Change Vault Parameters for Volumes.
3. Choose **s** for Change Vault Slot for Volumes. The following prompt appears. Enter the new vault slot. Entering 0 means that the slot will be cleared.

```
Setting Vault Slot for Volumes
-----
Enter Vault Slot: (0)
```

4. You are prompted for the media IDs for which you want this slot applied.  
You will continue to be prompted for media IDs until you press the Enter key without typing a media ID. If you enter the ESC key, your changes will not be applied.



## Change Vault Session ID for Volumes

You can set, clear, or change the vault session ID that a volume was processed in. This field is used by NetBackup Vault to determine what session was used for a volume when it was vaulted.

You can change the vault session ID for a single volume or for multiple volumes.

### ▼ To change the session ID

1. On the main menu, choose **s** for Special Actions.
2. Choose **a** for Change Vault Parameters for Volumes.
3. Choose **i** for Change Vault Session ID for Volumes. The following prompt appears. Enter the new session ID. Entering 0 means that the session ID will be cleared.

```
Setting Vault Session ID for Volumes
-----
Enter Vault Session ID: (0)
```

4. You are prompted for the media IDs for which you want this session ID applied.  
You will continue to be prompted for media IDs until you press the Enter key without typing a media ID. If you enter the ESC key, your changes will not be applied.

## Setting the Maximum Mounts for Volumes

You can set or change the maximum number of times a volume can be mounted. Once this number is reached, any further requests to mount the volume for a write operation result in an error. Specifying a maximum allowed mount count of 0 means there is no limit on the number of times a volume can be mounted.

To help determine the maximum mount count to use, consult your vendor documentation for information on the expected life of the media.

You can set the maximum allowed mounts for a single volume or for multiple volumes.

---

**Note** You cannot set the maximum number of mounts for a cleaning cartridge.

---

### ▼ To set the maximum mounts

1. On the main menu, choose **s** for Special Actions.
2. Choose **s** for Set Maximum Allowed Mounts for Volumes.



3. A prompt is displayed for specifying a maximum mount count. Entering a zero means there is no limit to the number of times the volume can be mounted. If you enter a value larger than 99999, it may be displayed by Media Manager as 0. For example, the output of the `vmrule` command will display 0 for values larger than 99999. However, Media Manager will correctly interpret the actual value.
4. You are prompted for the media IDs for which you want this maximum allowed mounts applied.

You will continue to be prompted for media IDs until you press the Enter key without typing a media ID.

## Changing the Cleanings Allowed for a Cleaning Tape

When you added cleaning tapes, you specified a cleaning count. For more information about cleaning tapes, see `tpclean(1M)` in the *VERITAS NetBackup Commands for UNIX and Linux*.

### ▼ To adjust the cleaning count

1. On the main menu, choose `s` for Special Actions.
2. Choose `m` for Modify Number of Cleanings on Cleaning Cartridge.
3. The following prompt appears. Enter the media ID of the cleaning tape for which you want to change the cleaning count.

```
Changing Cleaning Count for Volume
-----
Enter Media ID:
```

4. The current number of cleanings and a prompt to enter a new number for the cleaning count is displayed, similar to the following. Enter a new number. The cleaning count is changed to the new number and you are returned to the Special Actions menu.

```
Current Number of Cleanings for TEST:26
Enter New Number of Cleanings:
```



## Updating Barcodes for Selected Volumes in a Robot

Use Update/Validate Barcode for Volumes on the Special Actions menu to check the barcodes of selected volumes in robots (that can read barcodes) and update the EMM database if necessary. “Robot Attributes” on page 311 lists the robots that support barcodes.

Use this menu option only to fill in barcodes that are missing from the database. For example, if you logically add a new volume but do not physically insert it into the robot, the database will not include the barcode. In this case, you can use the Update/Validate Barcode option to fill in the missing barcode.

Do not use this option to correct a database entry that shows an incorrect media ID in a slot. Here, you must update the database by using a move option (see “Moving Volumes” on page 442) or the inventory and update option (see “Inventory and Update Robot Volume Configuration” on page 465).

---

**Note** You cannot use the Update/Validate Barcodes option for API robots since Media Manager does not manage location information for media in these robot types.

---

### ▼ To update barcodes

1. Ensure that the appropriate robotic daemons are active on the robot control host. To start the daemons, see “Robotic Daemons” on page 268.
2. On the main menu, choose **s** for Special Actions.
3. Choose **u** for Update/Validate Barcode for Volumes. The following prompt appears:  

```
Validating/Updating Barcodes for Volumes
-----
Enter Media ID:
```
4. Enter the media ID of the first volume you want to update and press the Enter key. You will continue to be prompted for media IDs until you press the Enter key without entering a media ID.

When you press the Enter key to exit from the Enter Media ID prompt, the barcodes are updated and you are returned to the Special Actions menu.



## Inventory and Report Robot Volume Configuration

Use Inventory a Robot and Report Contents from the Special Actions menu, to inventory a selected robot and obtain a report that shows which media ID is in each slot. If the robot can read barcodes (see “Robot Attributes” on page 311) then barcode information is included in the report.

---

**Note** If a volume happens to be in a drive, the report shows it in the slot it came from.

---

This option does not check or change the database, but is useful for listing the contents of a robot.

1. Ensure that the appropriate robotic daemons are active on the robot control host. To start the daemons, see “Robotic Daemons” on page 268.
2. On the main menu, choose s for Special Actions.
3. Choose c for Inventory a Robot and Report Contents.

If the EMM database has entries for robotic volumes, `vmadm` lists the robot number, robot type, and robot control host for those robot types. For example:

```
Robot from Volume Configuration
-----
1)  TLD 2 -- breaker
2)  TL4 3 -- breaker
3)  TL8 0 -- whale
4)  none of the above
Enter choice:
```

- a. If the desired robot is not in the list, choose (none of the above) and go to step 4.
- b. If the desired robot is in the list, enter the number corresponding to the robot (for example, enter 3 for TL8 0 on whale) and go to step 5.
- c. *The following step applies only to NetBackup Enterprise Server.*

If the desired robot is an ACS type, the menu shows a robot control host of NONE. If you choose an ACS robot, you are prompted for the Robot Control Host. At this prompt, enter the host on which the ACS daemon (`acsd`) is running. This can be the ACS library software host or it can be another host.



- d. *The following step applies only to NetBackup Enterprise Server.*

If the desired robot is a TLM type, the menu shows a robot control host of NONE. If you choose a TLM robot, you are prompted for the Robot Control Host. At this prompt, enter the host on which the TLM daemon (`tlmd`) is running. This can be the TLM library software host or it can be another host.

If the EMM database has no entries for robotic volumes, you are prompted to specify a robot control host on which to search the device configuration for robots. Respond to this prompt as explained in step 4.

```
Enter Robot Control Host:    (whale)
```

4. If the device configuration has no robots, or you have chosen an ACS or TLM robot or (none of the above) in step 3; you are prompted to select a robot control host on which to search for robots.

```
Enter Robot Control Host:    (whale)
```

- a. Enter a host name and then the Enter key, or press Enter without typing a name to select the default host shown in the parentheses. Media Manager searches for robots in the device configuration on the selected host.

---

**Note** If Media Manager does not find any robots in the device configuration, `vmadm` displays a “robot not obtained” message.

---

- b. If Media Manager finds robots in the device configuration, it lists their robot number, robot type, and robot host. If a list appears but the desired robot is not shown, choose (none of the above). In this case, `vmadm` shows a “robot not obtained” message and you must configure the robot before you can perform the inventory and report.

To report the contents of a robot in the list, enter the number corresponding to the robot (for example, 1 for TLD 0 on shark) and go to step 5.

```
Robot from Device Configuration
-----
1)  TLD 0 -- shark
2)  TLD 1 -- shark
3)  none of the above
Enter choice:
```

5. When you have selected a robot, `vmadm` displays a report that shows the contents of the robot.

For robots with a barcode reader, Media Manager obtains the barcode information and includes it in the report. If the robot does not support barcodes or the media does not have a readable barcode, `<none>` appears in place of the barcode.



## Inventory and Compare Robot Volume Configuration

Use the Inventory a Robot and Compare with Volume Configuration on the Special Actions menu to physically inventory a robot, compare the results with the contents of the EMM database, and obtain a list of recommended changes.

The report shows discrepancies between the contents of the robot and the contents of the EMM database. If the robot can read barcodes, then barcode information is included in the report.

This option does not change the database, but is useful for verifying whether the EMM database is correct after tapes have been physically moved in the robot. If the report shows that the media in a slot does not match what is in the database, you can physically move the media or change the database using a move option (see “Moving Volumes” on page 442) or the inventory and update option (see “Inventory and Update Robot Volume Configuration” on page 465).

### ▼ To inventory and compare a robot

1. Ensure that the appropriate control daemon is active on the host that controls the robot you are going to inventory. To start the daemons, see “Robotic Daemons” on page 268.
2. On the main menu, choose **s** for Special Actions.
3. Choose **v** for Inventory a Robot and Compare with Volume Configuration.

If the EMM database has entries for robotic volumes, `vmadm` lists the robot number, robot type, and robot host for those robots. For example:

```
Robot from Volume Configuration
-----
1)  TLD 2 -- breaker
2)  TL4 3 -- breaker
3)  TL8 0 -- whale
4)  none of the above
Enter choice:
```

- a. If the desired robot is not in the list, choose (none of the above) and go to step 4.

- b. *The following step applies only to NetBackup Enterprise Server.*

If the desired robot is an ACS type, the menu shows a robot control host of NONE. If you choose an ACS robot, you are prompted for the Robot Control Host. At this prompt, enter the host on which the ACS daemon (`acsd`) is running. This can be the ACS library software host or it can be another host.



- c. *The following step applies only to NetBackup Enterprise Server.*

If the desired robot is a TLM type, the menu shows a robot control host of NONE. If you choose a TLM robot, you are prompted for the Robot Control Host. At this prompt, enter the host on which the TLM daemon (`tlmd`) is running. This can be the TLM library software host or it can be another host.

- d. If the desired robot is in the list, enter the number corresponding to the robot (for example, enter 3 for TL8 0 on whale) and go to step 5.
- e. If the EMM database has no entries for robotic volumes, you are prompted to specify a robot control host on which to search the device configuration for robots. Respond to this prompt as explained in step 4.

```
Enter Robot Control Host:  (whale)
```

4. If the EMM database has no robotic volumes or you have chosen (none of the above) in step 3, you are prompted to select a robot control host on which to search the device configuration for robots.

```
Enter Robot Control Host:  (whale)
```

- a. Enter a host name and then the Enter key, or press Enter without typing a name to select the default host shown in the parentheses. Media Manager searches for robots in the device configuration on the selected host.

---

**Note** If Media Manager does not find any robots in the device configuration, `vmadm` shows a “robot not obtained” message.

---

- b. If Media Manager finds robots in the device configuration, it lists their robot number, robot type, and robot host. If a list appears but the desired robot is not shown, choose (none of the above). In this case, `vmadm` displays a “robot not obtained” message and you must configure the robot and insert media before you can perform the inventory and update.

To inventory and compare the EMM database entries for a robot in the list, enter the number corresponding to the robot (for example, 1 for TLD 0 on shark) and go to the next step.

```
Robot from Device Configuration
-----
1)  TLD 0 -- shark
2)  TLD 1 -- shark
3)  none of the above
Enter choice:
```



5. When you have selected a robot, `vmadm` displays a report comparing the contents of the robot with the contents of the EMM database.

See “Comparing Robot Contents with the Volume Configuration” on page 182 for example reports.

For API robots, Media Manager determines whether the media ID and media type that is stored in the EMM database matches the database for the robot-vendor software.

For robots that are not API robots that have a barcode reader, Media Manager determines whether the barcodes in the robot match those in the EMM database. When the report shows `<none>`, it means that the media does not have a barcode.

For robots that cannot read barcodes, `vmadm` verifies only whether the EMM database correctly shows whether a slot contains media.

## Inventory and Update Robot Volume Configuration

Use Inventory a Robot and Update Volume Configuration on the Special Actions menu to inventory a robot and compare the results with the contents of the EMM database.

You can then optionally update the EMM database to agree with what is in the robot. When you insert new media, the database update includes automatic creation of media IDs (based on barcodes or a prefix that you specify). If you use barcode rules, new media that is added through a barcode rule can also be assigned a media type, volume pool, maximum number of mounts (or number of cleanings), and description (see “Configuring Barcode Rules” on page 477).

See “Updating the Volume Configuration for a Robot” on page 184 for instructions on when to use and when not to use the Inventory and Update option.

## To Inventory and Update Robot Volume Configuration

### ▼ To inventory and update a robot

1. Check the barcode capabilities of the robot and its media (optional).

Before doing an inventory and update, perform “Inventory and Compare Robot Volume Configuration” on page 463 and check whether the following are true:

- ◆ The robot supports barcodes.
- ◆ The new media that was inserted 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 verify for reference, in case you assign a media ID prefix later in this procedure. You do not need a prefix if the robot supports barcodes and the media has a readable barcode.

You also may want to consider using the physical inventory utility (see “Using the Physical Inventory Utility for Non-Barcoded Media” on page 354).

3. For API robots, create media type mappings for the robot as explained in step 2 under “Changing Update Options” on page 469.

You can change the default media type mappings as explained in “Adding Mapping Entries to `vm.conf`” on page 213.

4. For robot types that are not API robots, create media ID generation rules (optional).

See “Media ID Generation Tab (Advanced Options)” on page 207 for more information.

5. Create barcode rules (optional).

Refer to “Configuring Barcode Rules” on page 477 and create any barcode rules that you want to use for updating the database for media that has been inserted into the robot.

6. Ensure that the appropriate control daemons are active on the robot control host. To start the daemons, see “Robotic Daemons” on page 268.

7. On the main menu, choose `s` for Special Actions.

8. Choose `r` for Inventory a Robot and Update Volume Configuration.

If the EMM database has entries for robotic volumes, `vmadm` lists the robot number, robot type, and robot host for those robots.

```
Robot from Volume Configuration
```

```
-----
```

```
1)  TLD 2 -- breaker
2)  TL4 3 -- breaker
3)  TL8 0 -- whale
4)  none of the above
```

```
Enter choice:
```

- a. If the robot you want to inventory and update is in the list, enter the number corresponding to the robot (for example, enter 3 for TL8 0 on whale) and go to step 10.
- b. If the desired robot is not in the list, choose (none of the above) and go to step 9.

- c. *The following step applies only to NetBackup Enterprise Server.*

If the desired robot is an ACS type, the menu shows a robot control host of NONE. If you choose an ACS robot, you are prompted for the Robot Control Host. At this prompt, enter the host on which the ACS daemon (`acsd`) is running. This can be the ACS library software host or it can be another host.

- d. *The following step applies only to NetBackup Enterprise Server.*

If the desired robot is a TLM type, the menu shows a robot control host of NONE. If you choose a TLM robot, you are prompted for the Robot Control Host. At this prompt, enter the host on which the TLM daemon (`tlmd`) is running. This can be the TLM library software host or it can be another host.

- e. If the EMM database has no entries for robotic volumes, you are prompted to specify a robot control host on which to search the device configuration for robots. Respond to this prompt as explained in step 9.

```
Enter Robot Control Host:    (whale)
```

---

**Note** This will be the case if you configure a new robot and are adding media to it using the inventory and update option.

---

9. If the EMM database has no robotic volumes or you have chosen (none of the above) in step 8, you are prompted to select a robot control host on which to search the device configuration for robots:

```
Enter Robot Control Host:    (whale)
```

- a. Enter a host name and then the Enter key, or press Enter without typing a name to select the default host shown in the parentheses. Media Manager searches for robots in the device configuration on the selected host.

---

**Note** If Media Manager does not find any robots in the device configuration, `vmadm` shows a “robot not obtained” message.

---



- b.** If Media Manager finds robots in the device configuration, it lists their robot number, robot type, and robot host. If a list appears but the desired robot is not shown, choose (none of the above). In this case, `vmadm` shows a “robot not obtained” message and you must configure the robot and insert media before you can perform the inventory and update.

To inventory and update the EMM database entries for a robot in the list, enter the number corresponding to the robot (for example, 0 for TLD 1 on shark) and go to step 10.

```
Robot from Device Configuration
-----
1)  TLD 0  -- shark
2)  TLD 1  -- shark
3)  none of the above
Enter choice:
```

- 10.** When you have selected a robot, the Inventory and Update Robot menu appears. For example:

```
Inventory and Update Robot:  TLD (10) - whale
```

```
Update Mode:  INTERACTIVE
```

```
Inventory and Update
-----
```

```
u)  Inventory Robot and Update Volume Configuration

m)  Change Update Mode
o)  Change Update Options

h)  Help
q)  Quit Menu
```

```
ENTER CHOICE:
```



Inventory a robot and update its EMM database entries as follows:

- a. Use the `m` option to toggle the update mode.
    - ◆ `INTERACTIVE` causes `vmadm` to display a list of recommended changes after the inventory, and prompts you to confirm whether to proceed with updating the database.
    - ◆ `NOT INTERACTIVE` causes `vmadm` to make the recommended database changes without prompting for a confirmation.

You may want to use the `NOT INTERACTIVE` mode after you become familiar with performing robot inventories.
  - b. To view the current inventory and update settings or change them, choose `o` and refer to “Changing Update Options” on page 469.
  - c. When the update options are as you want them, choose the `u` option to start the inventory and update operation.
- See “Updating the Volume Configuration for a Robot” on page 184 for example reports.

## Changing Update Options

When you choose `o` from the Inventory and Update Robot menu, the Update Options menu appears. The example that follows shows the defaults for a new installation.

These are also the defaults each time you enter the options menu, with the possible exception of the Media ID Prefix. The Media ID prefix default will be the last entry in the `vm.conf` file, if one exists (see step 6).



For most configurations, the default update options work well. You should only change the defaults if your configuration has special hardware or usage requirements.

Update Robot: TL8 (10) - whale

OPTION FOR REMOVED MEDIA

-----  
Volume Group: DEFAULT  
OPTIONS FOR ADDED OR MOVED MEDIA

-----  
Volume Group: DEFAULT  
Use Barcode Rules: YES  
Media Type: DEFAULT  
Media ID Prefix: DEFAULT  
Volume Pool: DEFAULT

Update Options

-----  
b) Use Barcode Rules      r) Volume Group for REMOVED media  
m) Media Type            a) Volume Group for ADDED or MOVED media  
i) Media ID Prefix        p) Volume Pool

h) Help  
q) Quit Menu

ENTER CHOICE:

### ▼ To change update options

1. Choose whether to use barcode rules when adding new media, by using the b option to toggle Use Barcode Rules between YES and NO.

---

**Note** Media Manager attempts to use barcode rules only for volumes that are not already in the EMM database.

---

- ◆ YES causes Media Manager to search existing barcode rules and apply them to new media that has been inserted into a robot.
- ◆ NO causes Media Manager to ignore the barcode rules.

See “Configuring Barcode Rules” on page 477 for more information on barcode rules and how to define them.



**2.** If you are updating an API robot, check the Media Type Mappings.

To change the mapping choose `c` from the Update Options menu and make your changes on the menu. The `c` option appears only for these robot types.

The default mapping originates from the `vm.conf` file on the host where you are running `vmadm`. If this file does not exist or contain a mapping for the media, Media Manager uses the defaults for these robot types (see the tables in “Default and Allowable Media Types for API Robots” on page 214).

**3.** Choose `m` to open a menu that shows the media types that are valid for this robot. The menu will be similar to the following example:

```
Media Type
-----
1)  DEFAULT
2)  1/2" cartridge tape
3)  1/2" cartridge tape 2
4)  DLT cartridge tape
5)  DLT cartridge tape 2
6)  1/2" cleaning tape
7)  1/2" cleaning tape 2
8)  DLT cleaning tape
9)  DLT cleaning tape 2

Enter Choice [1-9]:  (1)
```

**a.** If you are *not* using barcode rules:

- ◆ To use the default media type, select `DEFAULT`.

If the robot is an API robot, Media Manager uses the Media Type Mappings that are displayed.

If a robot is not an API robot, Media Manager uses the default media type for the robot (see the table “Default Media Types for Robots (Not API robots)” on page 198) as follows:

If all of the drives in the robotic library (configured on this robot host) are 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.

If all of the drives in the robotic library (configured on this robot host) are not the same type, then Media Manager uses the default media type for the robotic library.



- ◆ To use a media type other than the default, choose one from the menu.

Selecting from the menu is required if the robotic library supports multiple media types and you do not want the default media type.

*The following point applies only to NetBackup Enterprise Server.*

Selecting from the menu is required, if the drives are not configured on the robot control host and the drives are not the default media type for the robot.

**b.** If you *are* using barcode rules:

- ◆ Choose DEFAULT to let the barcode rule determine the media type that is assigned.

For example, assume you want to add both DLT and half-inch cartridges to a TLD robot with a single update operation. To accomplish this, first create separate rules for DLT and half-inch cartridges and select the specific media type in the barcode rules. Then, select DEFAULT from the Update Options menu. Media Manager will now use the media type in the barcode rules when it does the inventory and update.

---

**Note** If you also choose DEFAULT for the barcode rule, Media Manager assigns the default media type for the robot (see the table “Default Media Types for Robots (Not API robots)” on page 198).

---

- ◆ To use a media type other than the default, choose a specific type from the menu.

For example, to use the same rule to add DLT or half-inch cartridges to a TLD robot, choose specific media from the Update Options menu and DEFAULT for 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 update media type always overrides the rule. If you specify any value other than DEFAULT on the Update Options menu, the media type for the rule must be the same type or DEFAULT in order to obtain a match (except for cleaning media as explained later).



The following sample list shows what happens for various combinations of update and barcode rule media types.

| Update Options<br>Media Type | Barcode Rule<br>Media Type | Rule<br>Used | Media Type in<br>EMM database |
|------------------------------|----------------------------|--------------|-------------------------------|
| -----                        | -----                      | -----        | -----                         |
| DLT                          | DEFAULT                    | Yes          | DLT                           |
| 1/2" CART                    | DEFAULT                    | Yes          | 1/2" CART                     |
| DLT                          | DLT                        | Yes          | DLT                           |
| DLT                          | DLT CLEAN                  | Yes          | DLT CLEAN                     |
| DLT CLEAN                    | DLT                        | No           | DLT CLEAN                     |
| DLT CLEAN                    | DLT CLEAN                  | Yes          | DLT CLEAN                     |
| DLT CLEAN                    | DEFAULT                    | Yes          | DLT CLEAN                     |
| DLT                          | (4MM ...)                  | No           | DLT                           |
| DEFAULT                      | DEFAULT                    | Yes          | DLT                           |
| DEFAULT                      | DLT                        | Yes          | DLT                           |
| DEFAULT                      | DLT CLEAN                  | Yes          | DLT CLEAN                     |
| DEFAULT                      | 1/2" CART                  | Yes          | 1/2" CART                     |
| DEFAULT                      | (4MM ...)                  | No           | Robot-type dependent          |

- ◆ The fourth barcode rule in the list shows Media Manager's ability to automatically add cleaning cartridges with regular media, when you execute an update for a robot.

If the media you insert includes a cleaning tape, then Media Manager automatically adds the tape correctly, if the following are true:

- ◆ The update media type is for the regular media (DLT in this example).
- ◆ The barcode on the tape matches a barcode tag and the barcode rule media type is the cleaning media (DLT CLEAN in this example).

Also see "Example 5: Adding Cleaning Tapes to a Robot" on page 225.

- ◆ The sixth and seventh rules in the list illustrate how to add only cleaning media.

In the sixth rule, you specify the cleaning media type on both the Update Options menu and in the barcode rule. In the seventh rule, you specify the cleaning media on the Update Options menu and choose default in the barcode rule.

4. Choose a to open a menu for selecting the volume group that Media Manager will assign to media that you have inserted into the robot (or moved to a new location within the robot). The menu always has choices for the following:
  - ◆ Specifying a new volume group name.
  - ◆ Auto generating a new volume group (default). You can also auto generate a new volume group name by entering DEFAULT for the new volume group name.

Other choices that are available depend on the selected media type.



- ◆ If Media Type is DEFAULT, the menu shows existing volume groups that are valid for the robot's default Media Type.
- ◆ If Media Type is other than DEFAULT, the menu shows the existing volume groups that are valid for the media type.

```
Volume Group
-----
1) 00_000_TL8
2) Specify New Volume Group Name
3) Auto-Generate New Volume Group Name
Enter choice:
```

5. Choose **r** to open a menu for selecting the volume group that Media Manager will assign to media that you have removed from the robot. The menu always has choices for the following:

- ◆ Specifying no volume group name.
- ◆ Specifying a new volume group name.
- ◆ Auto generating a new volume group (default). You can also auto generate a new volume group name, by entering DEFAULT for the new volume group name.

Other choices that are available depend on the selected media type, as follows:

- ◆ If Media Type is DEFAULT, the menu shows existing volume groups that are valid for the robot's default Media Type.
- ◆ If Media Type is other than DEFAULT, the menu shows the existing volume groups that are valid for the media type.

```
Volume Group
-----
1) 00_000_NON
2) No Volume Group
3) Specify New Volume Group Name
4) Auto-Generate New Volume Group Name
Enter choice:
```

6. Specify a value for Media ID prefix if either of the following conditions are true (see step 1 under "Inventory and Update Robot Volume Configuration" on page 465):

- ◆ The robot does not support barcodes
- ◆ The media that was inserted does not have readable barcodes.

If *neither* of the previous conditions are true, a prefix is not required since Media Manager assigns the last six characters of the barcode or the specific characters that you specify if you are using Media ID generation rules as the media ID for media added to the robot. This applies whether or not a barcode rule is used.

To select a value for Media ID prefix, choose *i* from the Update Options menu to display a selection list that is similar to the following:

```
Media ID Prefix
-----
1)  NV
2)  NETB
3)  ADD
4)  Default Media ID Prefix
5)  Use No Media ID Prefix
6)  Specify New Media ID Prefix
Enter choice:
```

Choose one of the following from the list:

- ◆ If there are existing media ID prefixes, you can choose one of them from the list. The existing prefixes come from `MEDIA_ID_PREFIX` entries that you added to the `vm.conf` file on the host where you are running `vmadm`. For example, entries for the previous list would be:

```
MEDIA_ID_PREFIX = NV
MEDIA_ID_PREFIX = NETB
MEDIA_ID_PREFIX = ADD
```

- ◆ Default Media ID Prefix

In this case, Media Manager first checks the `vm.conf` file for `MEDIA_ID_PREFIX` entries, as follows:

- ◆ If `vm.conf` has `MEDIA_ID_PREFIX` entries, then Media Manager assigns the last one as the default prefix.
- ◆ If `vm.conf` does not have any prefix entries, Media Manager assigns the letter A as the default prefix.

- ◆ Use No Media ID Prefix

This operation will succeed only if the robot supports barcodes and the media has readable barcodes. Otherwise, Media Manager is unable to assign new media IDs and the operation fails (with an accompanying error message).

This choice may be useful if you are using media with barcodes and want updates to fail when unreadable or missing barcodes are encountered.

- ◆ Specify New Media ID Prefix

You can specify a new media ID prefix having from one to five alpha-numeric characters. Media Manager assigns the remaining numeric characters. For example, if the prefix is `NETB`, the media IDs are `NETB00`, `NETB01`, and so on.



For optical disk media, the final character reflects the platter side, unless you choose NO for Use Platter Side in Optical ID (see step 7).

---

**Note** A new media ID prefix is used only for the current operation. It is not added to `vm.conf` and does not appear in the Media ID prefix list the next time you use the Update Options menu.

---

7. If the robot is an ODL robot, choose the `s` option to toggle Use Platter Side in Media ID to YES or NO, depending on whether you want designate the platter-side in media IDs for optical disk media.

---

**Note** Use Platter Side in Media ID appears on the Update Options menu only if you are doing the inventory and update on an ODL robot and are using a Media ID Prefix.

---

The two sides of an optical disk platter are referred to as media ID partners.

- ◆ If you set Use Platter Side in Media ID to YES, one side will have a media ID of `xxxxxA` and the other side `xxxxxB`, where `xxxxx` is the media ID prefix and is an auto-generated number.
  - ◆ If you set Use Platter Side in Media ID to NO, the platter side is not included in the media ID.
8. Choose `p` to change the volume pool from the default. A menu similar to the following appears.

If you *are* using barcode rules:

- ◆ Choose Default Volume Pool to let the barcode rule determine the volume pool that is assigned.
- ◆ To use a volume pool other than the default, choose one from the menu.

The Update Options volume pool always overrides the rule.

If you are *not* using barcode rules:

- ◆ Choose Default Volume Pool to use the NetBackup volume pool for data volumes and no volume pool for cleaning tapes (the same as choosing None).
- ◆ To use a volume pool other than the default, choose one from the menu.

```
Volume Pool
-----
1)  None
2)  NetBackup
3)  DataStore
4)  CatalogBackup
5)  a_pool
6)  Default Volume Pool
Enter choice:
```

9. When you are satisfied with the settings, choose q to return to the Inventory and Update Robot menu.

## Configuring Barcode Rules

A barcode rule specifies criteria for creating EMM database entries for new robotic volumes that you are adding through an auto-populate or inventory and update operation (see “Auto-Populating a Robot” on page 431 and “Inventory and Update Robot Volume Configuration” on page 465). You select whether to use barcode rules when you set up the auto-populate, or inventory and update.

The following are some sample barcode rules.

| Barcode<br>Tag | Media<br>Type | Volume<br>Pool | Max Mounts/<br>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                       | 8mm cleaning    |
| TS8            | 8MM           | t_pool         | 0                        | 8mm backup      |
| TS             | 8MM           | None           | 0                        | 8mm no pool     |
| <NONE>         | DEFAULT       | None           | 0                        | no barcode      |
| <DEFAULT>      | DEFAULT       | NetBackup      | 0                        | other barcodes  |



## Barcode Rule Sorting

Rules are sorted, first according to the number of characters in the barcode tag (see the previous example barcode rule list) and then in the order you add them. The two exceptions are the <NONE> and <DEFAULT> rules which are always at the end of the list.

When an inventory and update, or auto-populate operation uses barcode rules and a new barcode is detected in a slot, Media Manager searches the rules starting at the top of the list and checks for a barcode tag that matches the new barcode.

If a barcode tag matches, the media type for the rule is checked to ensure that it is compatible with what you specified for the inventory and update. If the media type also matches, Media Manager uses the rule's media type, volume pool, max mounts (or number of cleanings), and description to create an EMM database entry for the media ID.

---

**Note** Media Manager attempts to use barcode rules only for volumes that are not already in the EMM database.

---

## Barcode Rule Examples

For example, assume that during an inventory and update for a TS8 robot, you select the following update options for a new 8 mm tape (see "Inventory and Update Robot Volume Configuration" on page 465):

```
Media Type: 8MM
Volume Group: 00_000_TL8
Use Barcode Rules: YES
Volume Pool: DEFAULT
```

If a new tape in this robot has a barcode of TS800001 and there are no media generation rules defined, Media Manager uses the rule with the barcode tag named TS8 and includes the following values in the EMM database entry for the tape:

```
Media ID: 800001 (last six characters of barcode)
Volume Group: 00_000_TL8
Volume Pool: t_pool
Max Mounts: 0 (infinite)
```

If a new tape has a barcode of TS000001 and there are no media generation rules defined, the rule named TS is used and EMM database entry for the tape will contain:

```
Media ID: 000001 (last six characters of barcode)
Volume Group: 00_000_TL8
Volume Pool: None
Max Mounts: 0 (infinite)
```



## Barcode Rule Menu

To configure barcode rules, choose Configure Barcode Rules from the Special Actions menu. The following menu appears:

```

          Display Mode:  BRIEF
    Output Destination:  SCREEN

Configure Barcode Rules
-----
a)  Add Rule
c)  Change Rule
d)  Delete Rule
l)  List Rules

m)  Mode (brief or full)
o)  Output Destination (screen or file)
h)  Help
q)  Quit Menu

ENTER CHOICE:
```

## Adding a Barcode Rule

To add a new barcode rule, choose a from the Configure Barcode Rules menu and enter the following information at the prompts:

### Barcode Tag

Enter a barcode tag for the rule. The tag can have from 1 to 16 characters and no spaces.

The only rules where you can use special characters in the barcode tags are as follow:

◆ <NONE >

Matches when rules are used and the media has an unreadable barcode, or the robot does not support barcodes.

◆ <DEFAULT>

For media 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 Update Options menu are compatible. The Update Options menu is where you set up the criteria for an inventory and update operation (see “Inventory and Update Robot Volume Configuration” on page 465).



**Description**

Enter a 1 to 25 character description of the rule that will be assigned to new volumes when the rule is used.

**Media Type**

A rule is disregarded if the media type in the rule is not compatible with the media type for the update. See “Inventory and Update Robot Volume Configuration” on page 465.

Select the media type for this rule, as follows:

- ◆ Select DEFAULT to have the rule match *any* media type that you select on the Update Options menu. If you also select DEFAULT for the update, Media Manager uses the default media type for the robot. See “Media Settings Tab (Advanced Options)” on page 190.
- ◆ Select a specific media type to have the rule match *only* when you select that specific media type or DEFAULT on the Update Options menu. If you choose DEFAULT for the update, Media Manager assigns the rule’s media type.

The following example shows the results with various combinations of update selections and barcode rule media types for a TLD robot. This type of robot is the most complex case because it can have DLT, half-inch cartridge, and other types of media.

| Update Options<br>Media Type | Barcode Rule<br>Media Type | Rule<br>Used | Media Type in<br>EMM database |
|------------------------------|----------------------------|--------------|-------------------------------|
| -----                        | -----                      | -----        | -----                         |
| dlt                          | default                    | Yes          | dlt                           |
| 1/2" cart                    | default                    | Yes          | 1/2" cart                     |
| dlt                          | dlt                        | Yes          | dlt                           |
| dlt                          | dlt clean                  | Yes          | dlt clean                     |
| dlt clean                    | dlt                        | No           | dlt clean                     |
| dlt clean                    | dlt clean                  | Yes          | dlt clean                     |
| dlt                          | (4mm ...)                  | No           | dlt                           |
| default                      | default                    | Yes          | dlt                           |
| default                      | dlt                        | Yes          | dlt                           |
| default                      | dlt clean                  | Yes          | dlt clean                     |
| default                      | 1/2" cart                  | Yes          | 1/2" cart                     |
| default                      | (4mm ...)                  | No           | Robot-type dependent          |





### Maximum Allowed Mounts or Number of Cleanings

When a barcode rule is used, Media Manager adds the number you specify to the EMM database for the media ID.

For media other than cleaning tapes, enter the maximum number of mounts to allow for this media ID (also see “Setting the Maximum Mounts for Volumes” on page 458).

For cleaning tapes, enter the number of cleanings to allow (also see “Changing the Cleanings Allowed for a Cleaning Tape” on page 459).

### Volume Pool

Specify a volume pool for the volume. This is the pool that the volume will be added to when a barcode matches the rule.

Whenever the barcode rule is used and the Update Options menu shows

- ◆ DEFAULT for the volume pool, then the volume is assigned to the pool specified in the barcode rule.
- ◆ A specific volume pool, then that selection overrides the pool specified in the barcode rule.

## Changing a Barcode Rule

To change a barcode rule, choose c from the Configure Barcode Rules menu and select the desired rule from the resulting list. You are then prompted to change the description, Media Type, Maximum Allowed Mounts (or Number of Cleanings), and Volume Pool.

For Media Type, Maximum Allowed Mounts, and Number of Cleanings, the current value appears in parentheses (pressing the Enter key without typing a new value leaves the value unchanged).

---

**Note** You cannot use Change Barcode Rule to change the barcode tag. To change a barcode tag, delete the rule and then add a rule with the new tag.

---

## Deleting a Barcode Rule

To delete a barcode rule, choose d from the Configure Barcode Rules menu and select the desired rule from the list.



## Listing Barcode Rules

To list existing barcode rules, set the Display Mode and Output Destination options and then choose l (List Rules) from the Configure Barcode Rules menu.

## Formatting Optical Disks

Before an optical disk platter can be used with Media Manager, a media ID (this should match the external media ID) and a volume label must be written to it. There are two ways to write this information:

- ◆ Format the platter when you add the optical disk volume using `vmadm`.
- ◆ Use the `tpformat` command.

When you use `vmadm`, the media ID becomes the recorded media ID. The following steps use `vmadm`. See `tpformat` in the *VERITAS NetBackup Commands for UNIX and Linux* for a description of how to use `tpformat`.

---

**Note** All platforms and operating systems do not support 1024 byte-per-sector platters. Most support only 512 byte-per-sector sizes. Before purchasing optical disk platters, check your vendor documentation to determine the sector sizes supported by your platform and operating system. Also see the VERITAS support web site for information on what is supported. VERITAS urges you to use platters that are already formatted.

---

### ▼ To format an optical disk

1. Perform the same steps for adding a volume, described in the preceding sections on adding single volumes or ranges of volumes.
2. The last step is a prompt similar to the following. (xxxxxA and xxxxB represent sides A and B of the volume's platter). Enter y to proceed or n to cancel the operation.

Do you want to tpformat xxxxxA and xxxxB? (y/n)

The `tpformat` request is sent to the host on which `vmadm` is running. This action may cause a mount request that requires manual assignment by the operator. If labels already exist on the tape, you are asked if they should be overwritten.

Even if the formatting cannot be completed for some reason, the volume or volumes are still added.

## STK Automated Cartridge System (ACS)

## D

---

**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 484.

- ◆ Automated Cartridge System Library Software (ACSL)
- ◆ STK Library Station
- ◆ Storaget 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.

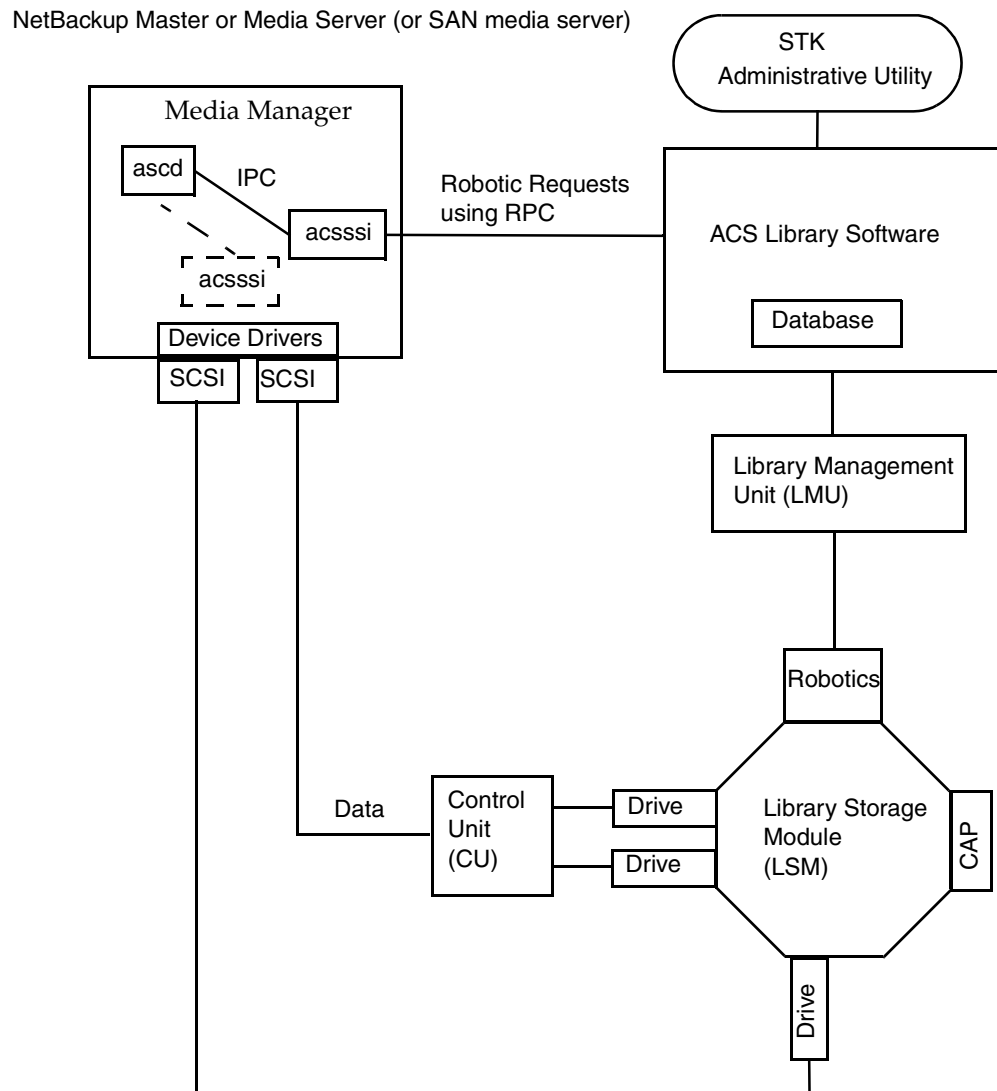
The topics in this appendix include the following:

- ◆ 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                                                                                                                                                                                                                   | Acts as a client to the ACS library software host.<br>The ACS robotic daemon ( <code>acsd</code> ) formulates requests for mounts, unmounts, and inventories. An API then routes these requests to the ACS Storage Server Interface ( <code>acsssi</code> ) using IPC communications. The requests are converted into RPC-based communications and sent to the ACS library software. |
| ACS library software (any of the following) <ul style="list-style-type: none"> <li>Automated Cartridge System Library Software (ACSL)</li> <li>STK Library Station</li> <li>Storagenet 6000 Storage Domain Manager (SN6000)</li> </ul> | 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.<br>On compatible host platforms, you may be able to configure ACS library software and Media Manager software on the same host.                                                                        |
| 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)                                                                                                                                                                                                                      | 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.<br>Most drives do not require a separate Control Unit. In these cases, the Media Manager server connects directly to the drives.         |
| CAP                                                                                                                                                                                                                                    | Cartridge Access Port.                                                                                                                                                                                                                                                                                                                                                               |

## Media Requests

A request for media in an ACS robot begins in the same manner as other media requests. The Media Manager device daemon, `ltid`, receives the request from `bptm`. Next, `ltid` sends a mount request to the ACS daemon, `acsd`.



`acsd` formulates the request and uses Internal Process Communications (IPC) to send it to the ACS Storage Server Interface (`acsssi`). The request is then converted into RPC-based communications and sent to the ACS library software.

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 `acsssi` (on the Media Manager server) receives a successful response from the ACS library software, it returns the status to `acsd`.

The `acsd` child process associated with the mount request scans 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 Drives

Using the Device Configuration wizard is the recommended method of configuring robots and drives in a Media Manager configuration.

See “The Device Configuration Wizard” on page 48 for information on using the wizard to configure devices.

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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* 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.

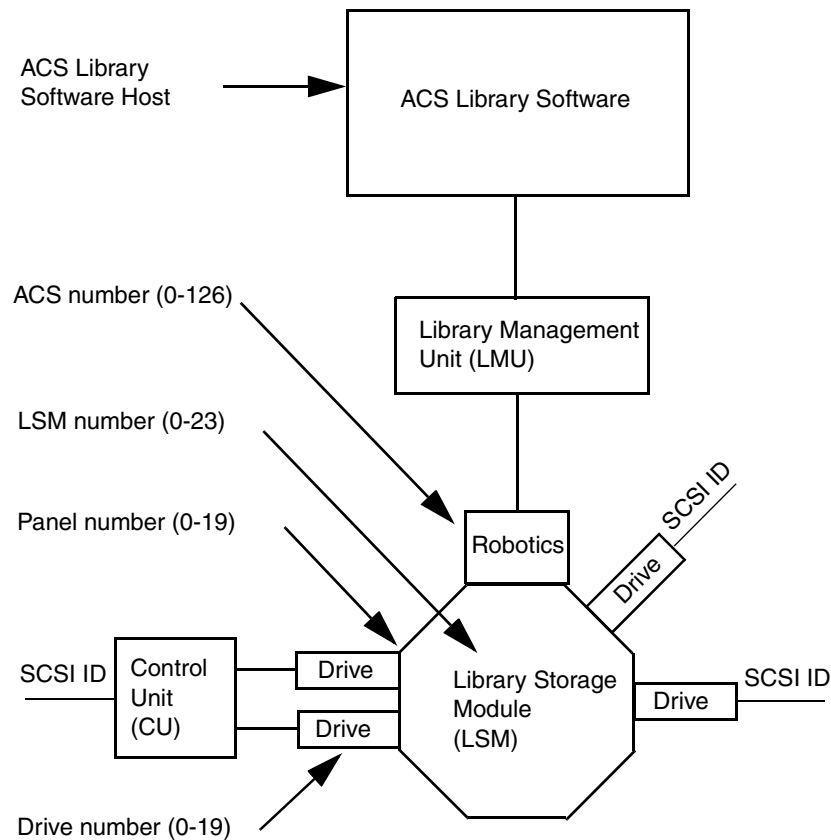
| ACS Drive Coordinate | Description                                                                              |
|----------------------|------------------------------------------------------------------------------------------|
| ACS number           | The index, in ACS library software terms, that 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:



### ACS Robot and Drive Configuration Information



## Configuring Shared ACS Drives

If the ACS server does not support serialization (ACSL versions prior to 6.1), use the following procedure to configure drives in an 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.



### ▼ To use the Device Configuration wizard in non-serialized configurations

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 336 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 by the NetBackup scheduler.

## 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 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, `acstest`.
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 184.
  - ◆ Add new volumes as explained in “Adding New Volumes” on page 123.

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 484), you must logically move the media to standalone using Media Manager. To accomplish this, do one of the following:

- ❖ Update the volume configuration, as explained in “Updating the Volume Configuration for a Robot” on page 184.
- ❖ Move volumes as explained in “Moving Volumes” on page 151.

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 “Using the Eject Volumes From Robot Command” on page 147).
- ❖ Use the `vmchange` command (see the *VERITAS NetBackup Commands for UNIX and Linux*).

## Robot Inventory Operations

---

**Note** An `INVENTORY_FILTER` entry may be 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. Old versions of Library Station do not support queries of all volumes in an ACS robot.

---

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, media types, ACS location, and LSM location from its database. The following table is an example of the ACS information that Media Manager receives:

| ACS Volume ID | ACS Media Type | ACS | LSM |
|---------------|----------------|-----|-----|
| 100011        | DLTIV          | 0   | 0   |
| 200201        | DD3A           | 0   | 0   |
| 412840        | STK1R          | 0   | 1   |
| 412999        | STK1U          | 0   | 1   |
| 521212        | JLABEL         | 0   | 0   |
| 521433        | STK2P          | 0   | 1   |
| 521455        | STK2W          | 0   | 1   |
| 770000        | LTO_100G       | 0   | 0   |
| 775500        | SDLT           | 0   | 0   |
| 900100        | EECART         | 0   | 0   |
| 900200        | UNKNOWN        | 0   | 0   |

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 180 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 211. Media Manager adds the ACS and LSM locations for new volumes to the EMM database. This location information is used for media and drive selection.



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 187.

## Advanced ACS Robot Topics

*The following sections cover these advanced NetBackup Enterprise Server topics:*

- ◆ ACS Daemon (acsd)
- ◆ ACS Storage Server Interface (acsssi)
- ◆ ACS SSI Event Logger (acssel)
- ◆ ACS Robotic Test Utility (acstest)
- ◆ Making ACS Robotic Configuration Changes
- ◆ Multiple ACS Robots with One ACS Library Software Host
- ◆ Multiple ACS Robots and ACS Library Software Hosts
- ◆ Robotic Inventory Filtering
- ◆ ASCLS Firewall Configuration

### ACS Daemon (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 ltid. You can also start acsd manually, if ltid is already running.

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.

When acsd is started, it starts acsssi and acssel. When starting acsssi, acsd passes the ACS library software host name to acsssi. One copy of acsssi is started for each ACS library software host that appears in the Media Manager device configuration for the media server (or SAN media server). If you have multiple media servers sharing drives in an ACS robot, acsssi must be active on each media server.

See “ACS Storage Server Interface (acsssi)” on page 495 and “ACS SSI Event Logger (acssel)” on page 497 for information about these processes.

## ACS Storage Server Interface (acsssi)

`acsssi` is the storage server interface (SSI) for a particular ACS library software host. All RPC communications from `acsd` or the ACS robotic test utility intended for ACS library software are handled by `acsssi`.

One copy of `acsssi` must be running for each unique ACS library software host that is configured on a Media Manager server(s). `acsd` tries to start copies of `acsssi` for each host, but these `acsssi` processes fail during initialization if an `acsssi` process for a particular ACS library software host is already running.

In normal operations, `acsssi` should be started to run in the background. Log messages for `acsssi` are sent to `acssel`. `acssel` should be started before `acsssi`. See “ACS SSI Event Logger (`acssel`)” on page 497 for more information.

The socket name (IP port) used by `acsssi` can be specified in any of the following ways:

- ◆ On the command line, when starting `acsssi`.
- ◆ Using an environment variable (`ACS_SSI_SOCKET`).
- ◆ Through the default value.

---

**Note** If you configure `acsssi` to use a non-default socket name, the ACS daemon and ACS test utility also must be configured to use the same socket name. If this is not done, successful IPC communications cannot be established.

---

The ACS library software host name is passed to `acsssi` using the `CSI_HOSTNAME` environment variable.

`acsssi` is based on the SSI provided by STK and supports features, such as use of environment variables to affect most aspects of operational behavior. See “Optional Environment Variables” on page 496, for a list of environment variables that are supported.

### Using the `ACS_SSI_SOCKET` Environment Variable

By default, `acsssi` listens on unique, consecutive socket names starting at 13741. To specify socket names on a ACS library software host basis, you can add a configuration entry in `vm.conf`.

Use the following format:

```
ACS_SSI_SOCKET = ACS_library_software_hostname socket_name
```

The following is an example entry (do not use the IP address of the ACS library host for this parameter):

```
ACS_SSI_SOCKET = einstein 13750
```



## Starting acsssi Manually

---

**Note** This is not the recommended method to start acsssi. Normally, acsd starts acsssi.

---

### ▼ To start acsssi

1. Start the event logger, acssel.
2. Start acsssi. The format is `acsssi socket_name`.

The CSI\_HOSTNAME environment variable is required. The following is a Bourne shell example:

```
CSI_HOSTNAME=einstein
export CSI_HOSTNAME
/usr/opensv/volmgr/bin/acsssi 13741 &
```

## Optional Environment Variables

If you want individual acsssi processes to operate differently, you can set environment variables before the acsssi processes are started manually or from a custom-designed script.

The following are the optional environment variables:

- ◆ SSI\_HOSTNAME  
Specifies the name of the host where ACS library software RPC return packets are routed for ACS network communications. By default, the local host name is used.
- ◆ CSI\_RETRY\_TIMEOUT  
Set this to a small positive integer. The default is 2 seconds.
- ◆ CSI\_RETRY\_TRIES  
Set this to a small positive integer. The default is 5 retries.
- ◆ CSI\_CONNECT\_AGETIME  
Set this in the range of 600 to 31536000 seconds. The default is 172800 seconds.



## ACS SSI Event Logger (acsssel)

`acsssel` is modeled after the `mini_el` event logger provided by StorageTek, so its functional model differs slightly from other robotic test tools provided with Media Manager.

If ACS robots have been configured, the event logger is automatically started by `acsd`. Event messages are logged to the file,  
`/usr/opensv/volmgr/debug/acsssi/event.log`.

---

**Note** `acsssel` should be running for optimum ACS SSI performance, since `acsssi` tries to connect on the event logger's socket for its message logging. If `acsssi` cannot connect to `acsssel`, request processing from ACS library software is delayed. This leads to retries and error recovery situations. VERITAS recommends that `acsssel` be kept running for best results.

---

`acsssel` can be started automatically or manually, but only stopped using the `kill` command (such as is done in the NetBackup `bp.kill_all` utility).

The full path to the event logger is `/usr/opensv/volmgr/bin/acsssel`. The usage format is as follows:

```
acsssel [-d] -s socket_name
```

where

- ◆ `-d` displays debug messages (by default, there are no debug messages).
- ◆ `socket_name` is the socket name (or IP port) to listen on for messages.

### Using `acsssel` with a Different Socket Name

If there is no `ACS_SEL_SOCKET` entry in `vm.conf`, `acsssel` listens on socket name 13740 by default. This default can be changed using one of the following methods:

#### ▼ To change the default by modifying the Media Manager configuration file

1. Edit `vm.conf` and add an `ACS_SEL_SOCKET` entry.

For example:

```
ACS_SEL_SOCKET = 13799
```

2. Use `/usr/opensv/netbackup/bin/goodies/bp.kill_all` to stop the `acsd`, `acsssi`, and `acsssel` processes. (This script stops all NetBackup and Media Manager processes.)
3. Restart the NetBackup/Media Manager daemons.



```
/usr/opencv/netbackup/bin/goodies/netbackup start
```

▼ **To change the default by using environment variables**

This method assumes there is one ACS robot configured and the SSI default socket name has not been changed with an `ACS_SEL_SOCKET` entry in `vm.conf`.

1. Use `/usr/opencv/netbackup/bin/goodies/bp.kill_all` to stop the `acsd`, `acsssi`, and `acsse` processes. (This script stops all NetBackup and Media Manager processes.)
2. Set the desired socket name in an environment variable and export it.

```
ACS_SEL_SOCKET = 13799
export ACS_SEL_SOCKET
```

---

**Note** `acsse` also has a command line option to specify the socket name. However, since the `acsssi` needs to know the event logger socket name, setting an environment variable is preferred.

---

3. Start the event logger in the background.  

```
/usr/opencv/volmgr/bin/acsse &
```
4. Set the ACS library software host name for `acsssi` in an environment variable.  

```
CSI_HOSTNAME = einstein
export CSI_HOSTNAME
```
5. Start `acsssi`.  

```
/usr/opencv/volmgr/bin/acsssi 13741 &
```
6. Optionally, start `acctest` using `robtest` or by using the following command line:  

```
/usr/opencv/volmgr/bin/acctest -r einstein -s 13741
```

---

**Note** If you request SCSI unloads, you must also specify drive paths on the `acctest` command line (see “ACS Robotic Test Utility (`acctest`)” on page 499). This is done automatically by `robtest` if ACS drives have been configured.

---

7. Start `ltid`, which starts `acsd`. You can use the `-v` option for verbose message output.  

```
/usr/opencv/volmgr/bin/ltid
```

During initialization, `acsd` obtains the SSI Event Logger socket name from `vm.conf` and sets `ACS_SEL_SOCKET` in the environment before starting `acssel`. If `acsssi` is started manually, it has to use (listen on) the same SSI socket that `acsd` is using to send data.

## 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 `acsssi` being started successfully. You can use the system command, `netstat -a`, to verify there is a process listening on the SSI socket. `acstest` attempts to communicate with ACS library software using `acsssi` and connects on an existing socket.

`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. You can pass the socket name on the command line. Otherwise, the default socket name (13741) is used.

```
acstest -r ACS_library_software_hostname [-s socket_name]
[-d drive_path ACS, LSM, panel, drive] ... [-C sub_cmd]
```

The following example assumes that `acsssi` has been started using socket name 13741:

```
/usr/opencv/volmgr/bin/acstest -r einstein -s 13741
```

## Making ACS Robotic Configuration Changes

After making any ACS robotic configuration changes, you should follow the correct steps so that `acsssi` can successfully communicate with `acsd`, `acstest`, and ACS library software.

Any `acsssi` processes must be cancelled after your changes are made and before the Media Manager device daemon, `ltid`, is restarted. Also in order for the `acstest` utility to function, `acsssi` for the selected robot must be running.

### ▼ To make configuration changes

1. Make your configuration changes.
2. Use `bp.kill_all` to stop all running processes.

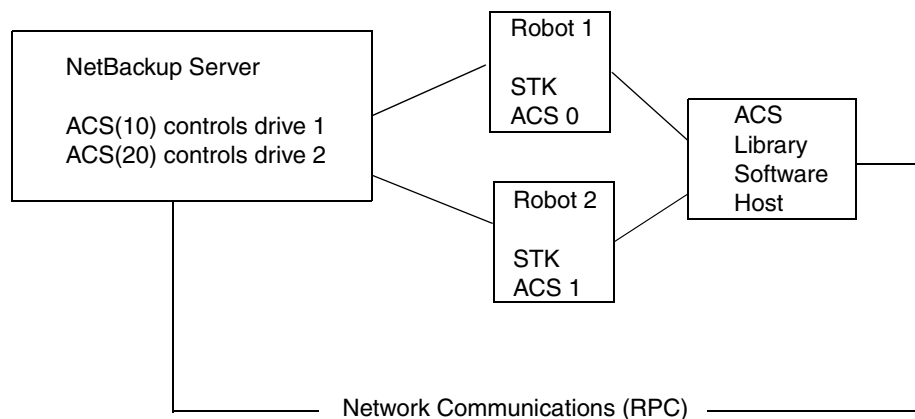


3. Restart all processes.

```
/usr/opencv/netbackup/bin/goodies/netbackup start
```

## Multiple ACS Robots with One ACS Library Software Host

NetBackup supports configurations where a NetBackup server is connected to drives in multiple ACS robots, and these robots are controlled from a single ACS library software host. See the following example:



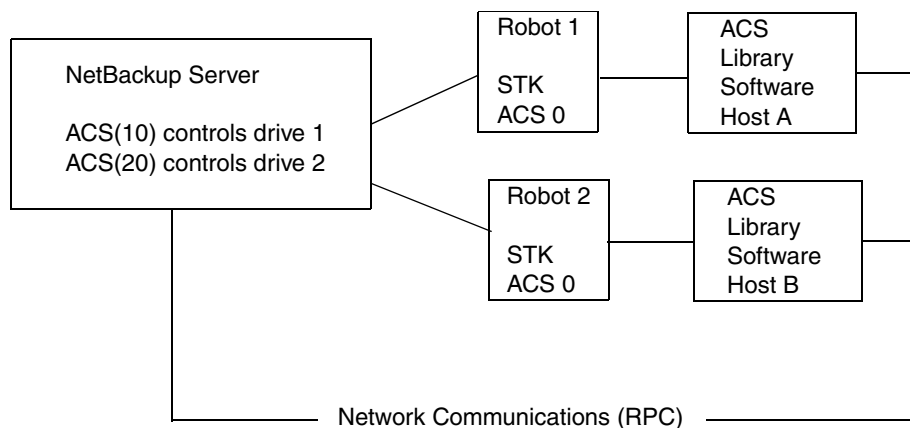
Inventory requests for a robot will include those volumes configured on the ACS library software host which are resident to the ACS robot (ACS 0 or ACS 1) that is designated in the drive address.

In the example, assume that drive 1 has an STK address (ACS, LSM, panel, drive) of 0,0,1,1 in the Media Manager device configuration and is under control of robot number 10 (ACS(10)). If any other drives configured under robot number 10 have a different ACS drive address (for example, 1,0,1,0) it is considered an invalid configuration.

Configurations consisting of multiple LSMs in a single ACS robot are supported if a passthru port exists.

## Multiple ACS Robots and ACS Library Software Hosts

NetBackup supports configurations where a NetBackup server is connected to drives in multiple ACS robots and these robots are controlled from separate ACS library software hosts. See the following example:



Inventory requests for a robot will include those volumes configured on the ACS library software host (in this example, Host A for Robot 1 and Host B for Robot 2) which are resident to the robot (ACS 0 for each) that is designated in the STK drive address.

In this example, assume drive 1 has an STK address (ACS, LSM, panel, drive) of 0,0,1,1 in the Media Manager device configuration and is under control of robot number 10 (ACS(10)). If any other drives configured under robot number 10 have a different ACS drive address (for example, 1,0,1,0) it is considered an invalid configuration.

Configurations consisting of multiple LSMs in a single ACS robot are supported if a passthru port exists.

## 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 may be required if you are doing a robot inventory for an ACS robot and the ACS library software host is an STK Library Station. Old versions of Library Station do not support of all volumes in an ACS robot.

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 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
```

## ASCLS Firewall Configuration

To configure an ACS robot in an ASCLS firewall environment, designate ports that TCP connections will use in the following configuration entries.

- ◆ ACS\_CSI\_HOSTPORT
- ◆ ACS\_SSI\_INET\_PORT
- ◆ ACS\_TCP\_RPCSERVICE

Corresponding settings on the ACSLS server must match the settings in the `vm.conf` file. For example, in a typical ACSLS firewall configuration, you would change the following settings as shown:

◆ **Changes to alter use of TCP protocol...**

Set to **TRUE** - Firewall-secure ACSLS runs across TCP.

◆ **Changes to alter use of UDP protocol...**

Set to **FALSE** - Firewall-secure ACSLS runs across TCP.

◆ **Changes to alter use of the portmapper...**

Set to **NEVER** - Ensures that the ACSLS server will not make any queries of the portmapper on the client platform.

◆ **Enable CSI to be used behind a firewall...**

Set to **TRUE** - Allows specification of a single port to be used by the ACSLS server.

◆ **Port number used by the CSI...**

Port chosen by user, but default value is most commonly used and is 30031. This port number must match the port number specified in NetBackup's `vm.conf` file.

For complete information about setting up a firewall-secure ACSLS server, refer to your vendor documentation.

For information about specifying these configuration entries, see "The Media Manager Configuration File (`vm.conf`)" on page 387.







## IBM Automated Tape Library (ATL)

---

**E**

---

**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.

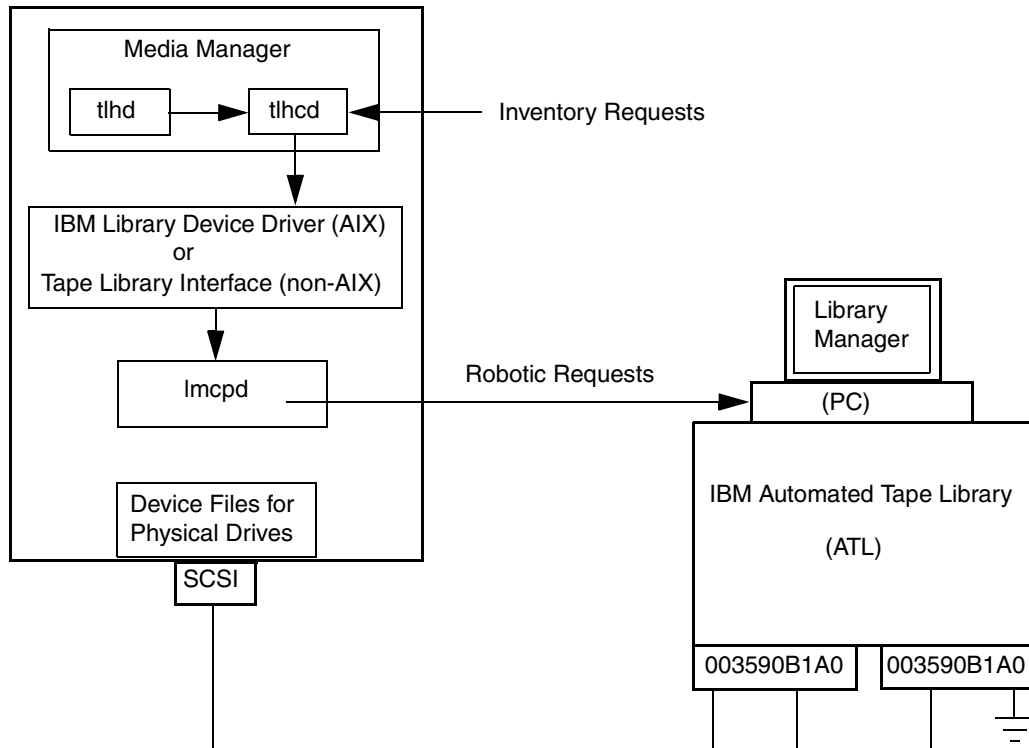


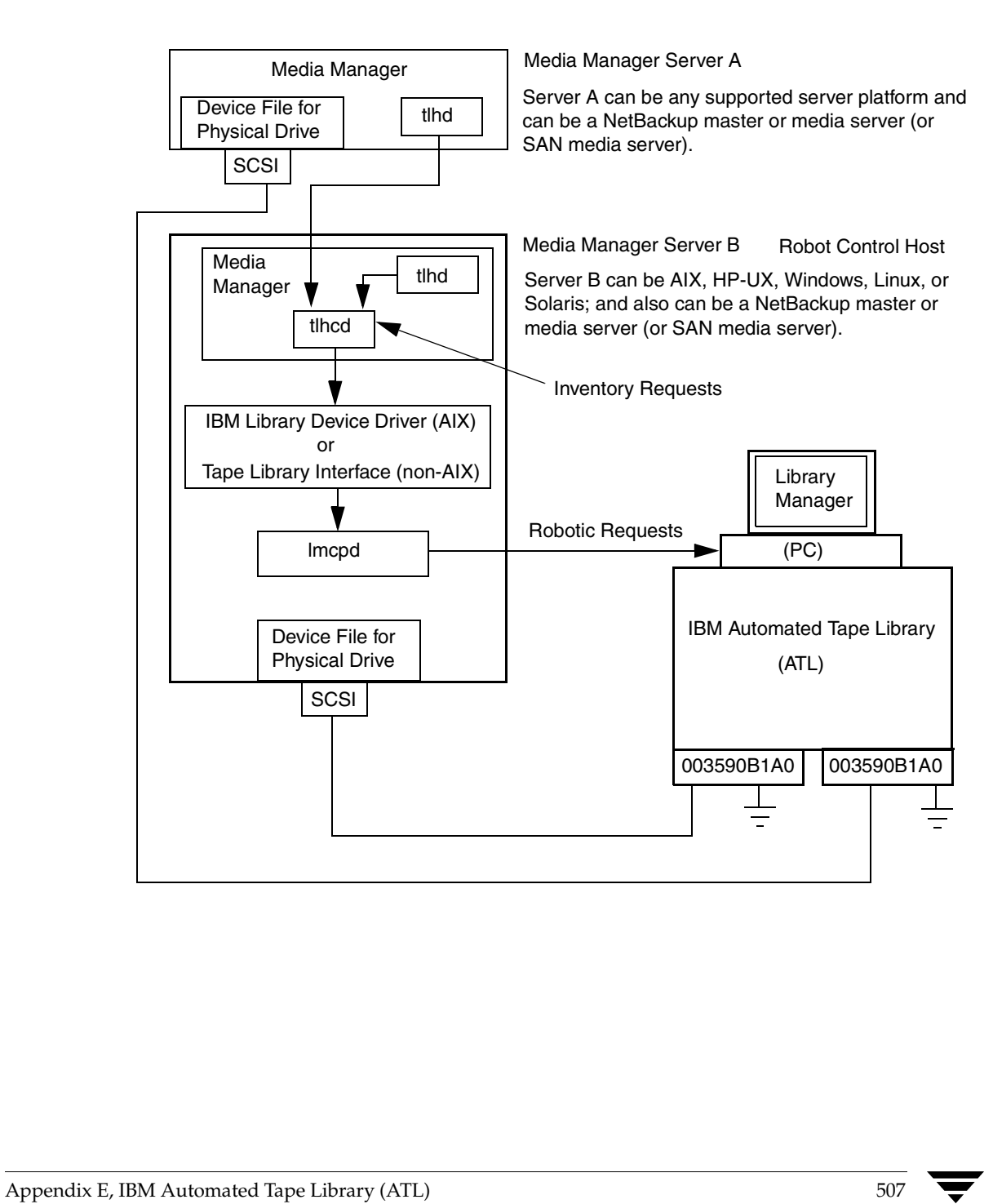
### Robotic Control Host Communicates Directly to Robot

#### Media Manager Server

This server can be an AIX, HP-UX, Windows, Linux, or Solaris server.

This server also can be a NetBackup master or media server (or SAN media server).





| Component                                                    | Description                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Media Manager Server                                         | This host has Media Manager software and acts as a client to the ATL through the Library Manager Control Point daemon ( <code>lmcpd</code> ). Media Manager's device daemon, <code>ltid</code> , forwards mount and dismount requests to the Tape Library Half-inch daemon ( <code>tlhd</code> ).                                               |
| Tape Library Half-inch daemon ( <code>tlhd</code> )          | This daemon resides on a Media Manager server and passes mount and dismount requests to the Tape Library Half-inch control daemon ( <code>tlhcd</code> ) on the robotic control host.                                                                                                                                                           |
| Tape Library Half-inch control daemon ( <code>tlhcd</code> ) | This daemon 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 <code>lmcpd</code> by using the IBM Library Device Driver interface (on AIX) or IBM Tape Library system calls (on non-AIX). |
| Library Manager Control Point daemon ( <code>lmcpd</code> )  | 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 daemon (`ltid`) receives the request from `bptm`. `ltid` sends a mount request to the TLH daemon (`tlhd`). This daemon passes the request to the TLH control daemon (`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. If the Media Manager server is an AIX system, the control daemon communicates with the Library Manager Control Point daemon (`lmcpd`)



by using the Library Device Driver interface. If the Media Manager server is a non-AIX system, such as Solaris, the control daemon communicates with `lmcpd` through Tape Library system calls from an application library interface.

`lmcpd` 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://support.veritas.com>).
- ◆ You are using a recommended version for the Automated Tape Library. Visit the VERITAS support web site to locate the recommended levels.

## Robotic Control on an AIX System

The following topics explain the steps needed for configuring robotic control when the media server (or SAN media server) is an AIX system.

### Determine the Path to the LMCP Device File

Use the Library Manager Control Point (LMCP) device file as the robotic device file in Media Manager. This file is set up when the Automated Tape Library is first configured.

Use the `lsdev` command (or `smit`) to determine the LMCP device file.

The following example uses the `lsdev` command:

```
/etc/lsdev -C | grep "Library Management"
```

The following is the output from this command:

```
lmcp0          Available          LAN/TTY Library Management Control Point
```



## Verify Library Communications

After you determine the path to the LMCP device file, verify library communications through the IBM-provided `mtlib` interface. Resolve all errors before attempting to configure IBM 3494 support in Media Manager.

To verify communications with a specific library, specify the Library Manager Control Point device file with the `mtlib` command. For example, if the LMCP device path is `/dev/lmcp0`, the following command verifies communication with the library:

```
/usr/bin/mtlib -l /dev/lmcp0 -qL
```

The following is the output from this command:

```
Library Data:
state..... Automated Operational State
                        Dual Write Disabled
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.
avail 3490 cleaner cycles..0
avail 3590 cleaner cycles..92
```

## Configure the Robotic Device File

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. In this example, the first two drives shown are standalone drives. The drive with drive index 31 is under TLH robotic control and the drive with drive index 78 is under TL4 control.

```
# /usr/openv/volmgr/bin/tpconfig -d
```

| Id    | DriveName    | Type  | Residence          | Status |
|-------|--------------|-------|--------------------|--------|
| ***** |              |       |                    |        |
| 5     | Drive0       | hcart | TLH(8) 003590B1A00 |        |
|       | /dev/rmt4.1  |       |                    | DOWN   |
| 13    | Drive2       | hcart | TLH(8) 003590B1A00 |        |
|       | /dev/rmt8.1  |       |                    | DOWN   |
| 31    | Drive1       | hcart | TLH(8) 003590B1A00 |        |
|       | /dev/rmt12.1 |       |                    | DOWN   |
| 78    | Drive1       | 4mm   | TL4(77) DRIVE=1    |        |
|       | /dev/rmt11.1 |       |                    | UP     |

Currently defined robotics are:

```
TL4(77)    robotic path = /dev/ovpass0
TLH(8)     LMCP device path = /dev/lmcp0
```

```
EMM Server = maui
```

In this example, note the following lines:

```
TLH(8)     LMCP device path = /dev/lmcp0
EMM Server = maui
```

Where `/dev/lmcp0` is the path to the robotic device file and `maui` is the EMM server for this robot.

## Robotic Control on a Non-AIX System

The following topics explain the steps for configuring robotic control when the media server is not an AIX UNIX system.

### Determine the Library Name

Use the library name instead of the robotic device file when configuring in Media Manager. This name is set up when the Automated Tape Library is first configured (see your IBM system documentation). The library name is configured in the `/etc/ibmatl.conf` file and you 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:

```
/usr/bin/mtlib -l 3494AH -qL
```

The following is the output from this command:

Library Data:

```
state.....Automated Operational State
                        Dual Write Disabled

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.
avail 3490 cleaner cycles..0
avail 3590 cleaner cycles..92

```

## Configure the Robotic Device File

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.

```
/usr/openv/volmgr/bin/tpconfig -d
```

| Id    | DriveName<br>Drive Path  | Type  | Residence          | Status |
|-------|--------------------------|-------|--------------------|--------|
| ***** |                          |       |                    |        |
| 6     | Drive2<br>/dev/rmt/17cbn | hcart | TLH(0) 003590B1A00 | UP     |
| 55    | Drive1<br>/dev/rmt/15cbn | dlt   | TLD(5) DRIVE=1     | UP     |

Currently defined robotics are:

```

TLH(0)      library name = 3494AH
TLD(5)      robotic path = /dev/sg/c2t0l0

```

```
EMM Server = grozer
```

In this example, note the following lines:

```

TLH(0)      library name = 3494AH
EMM Server = grozer

```

Where 3494AH is the library name and grozer is the EMM server for this robot.

## Configuring Drives for TLH Robots

The TLH robot has half-inch cartridge tape drives, usually with a SCSI interface, and you use the same methods to create or identify device files for these drives as for other drives. Refer to the system documentation for your platform and operating system for details on physically adding drives to your robots. The *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX and Windows* has information on configuring device files.

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:

```
/usr/opensv/volmgr/bin/tlhtest -r /dev/lmcp0
```

The following is the output from `tlhtest` (the user entered the `drstat` command on the third line). You would use 156700 and 156600 when adding these drives in Media Manager.

```
Opening /dev/lmcp0
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
```

If the robotic control is configured on a non-AIX UNIX server using the IBM Automated Tape Library support, use the library name as configured in `/etc/ibmatl.conf` in place of the LMCP device path on the call to `tlhtest`.

## 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 184.
  - ◆ Add new volumes as explained under “Adding New Volumes” on page 123.

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 **Media** 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 “Using the Eject Volumes From Robot Command” on page 147).
  - ◆ The `vmchange` command (see the *VERITAS NetBackup Commands for UNIX and Linux*).
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 EMM 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 184.
- ◆ Move volumes as explained in “Moving Volumes” on page 151.

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 daemon.
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           |



| TLH Volume ID | TLH Media Type |
|---------------|----------------|
| 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 180 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 211.

The Update Volume Configuration report for an TLH robot is similar to the figure shown for an API robot in “Procedure To Update the Volume Configuration” on page 187.



## 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

---

**F**

---

**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 519.

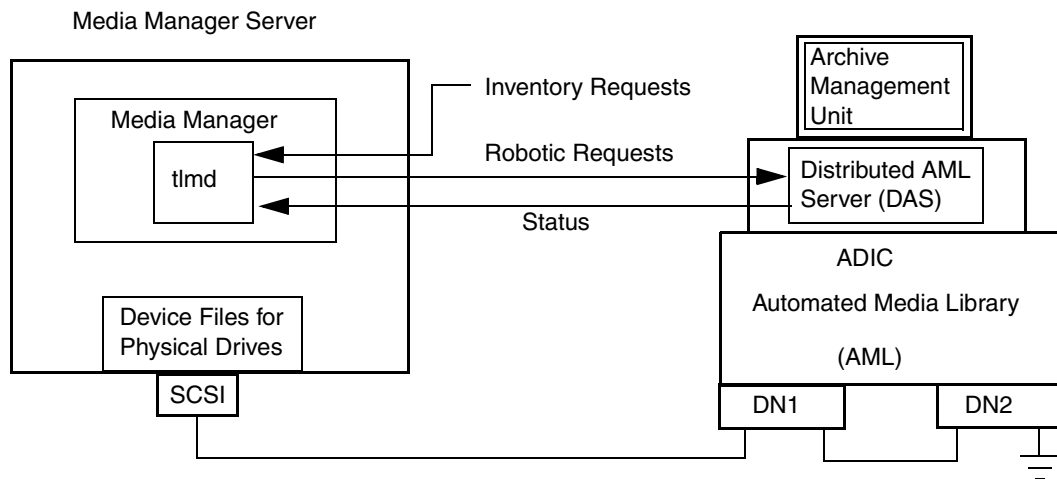
Portions of this appendix use the term *DAS/SDLC* to refer to either of these ADIC software products. Other portions use the terms *DAS* or *SDLC* when referring to a particular ADIC software product.

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.<br>Media Manager's device daemon, <code>tlmd</code> , forwards mount and dismount requests to the TLM daemon ( <code>tlmd</code> ).                                                |
| TLM daemon ( <code>tlmd</code> )                                                | This daemon passes mount and dismount requests to the DAS/SDLC server and handles return status. <code>tlmd</code> 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)<br>Scalar Distributed Library<br>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).<br>The Media Manager robotic daemon (or TLM daemon) 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 daemon, `ltid`, receives the request from `bptm`. Next, `ltid` sends a mount request to the TLM daemon, `tlmd`. This daemon 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

The VERITAS support web site (<http://www.support.veritas.com>) contains compatibility information for the ADIC client software. Ensure that your ADIC client software is compatible with your version of NetBackup. Do the following to install ADIC software on UNIX servers:

### ▼ To install and configure ADIC software

- ❖ Install the ADIC library (`libaci.so`) in the operating system folder `/usr/lib`. The ADIC library is named `libaci.sl` on servers running HP-UX.

## 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. Use this name in a `DAS_CLIENT` entry in the `/usr/opensv/volmgr/vm.conf` file on the Media Manager server. These entries are of the form:

```
DAS_CLIENT = DASclientname
```

Where *DASclientname* is the name that you want Media Manager to use as its DAS/SDLC client name. In this example, this entry would be

```
DAS_CLIENT = dolphin2
```

3. Stop and start the `ltid` daemon to enable the TLM daemon 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 522), 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 522), 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 can have several different types of drives, usually with a SCSI interface, and you use the same methods to create device files for these drives as for other drives. If the drives are SCSI and connect to the robot through a 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 *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX, Windows, and Linux* also has information on configuring device files.

Using the Device Configuration wizard is the recommended method of configuring robots and drives in a Media Manager configuration. See “The Device Configuration Wizard” on page 48 for information on using the wizard to configure devices.

### To add drives manually

For older drives or for DAS/SDLC servers that do not support serialization, you may need to add drives to your configuration manually. 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`:

```
/usr/opensv/volmgr/bin/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

Use the Device Configuration wizard to configure shared drives in your Media Manager configuration. During the setup phase, the wizard will discover the tape drives available; and for the robot types where serialization is available, the positions of the drives within the library.

However, if the DAS/SDLC server does not support serialization, then use the following procedure to configure drives in an 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.

### ▼ To use the Device Configuration wizard in non-serialized configurations

1. Run the Device Configuration wizard on one of the hosts where drives in a 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 336 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

Since all Media Manager servers use the same EMM database, 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 184.
  - ◆ Add new volumes as explained under “Adding New Volumes” on page 123.



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 NetBackup EMM database. 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 “Using the Eject Volumes From Robot Command” on page 147).
  - ◆ The `vmchange` command (see the *VERITAS NetBackup Commands for UNIX and Linux*).
2. If you are using the `vmchange` command or the NetBackup Administration Console (see step 1), you can skip this step.

Update the EMM 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 184.
- ◆ Move volumes as explained in “Moving Volumes” on page 151.

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     | DECULT         |
| 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 180 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 211.



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 187.





# Index

---

## **Symbols**

/etc/ibmatl.conf file 511

## **A**

accessibility features xxx

ACS (see Automated Cartridge System)

ACS or TLM robot types 301

ACS, TL8, TLD, TLH, or TLM robot types 285

ACS, TLH, or TLM robot types 285

ACS\_ vm.conf entry 389

ACS\_CSI\_HOSTPORT, vm.conf entry 390

ACS\_SEL\_SOCKET, vm.conf entry 389

ACS\_SSI\_HOSTNAME, vm.conf entry 390

ACS\_SSI\_INET\_PORT, vm.conf entry 391

ACS\_SSI\_SOCKET, vm.conf entry 391

ACS\_TCP\_RPCSERVICE, vm.conf entry 392

ACS\_UDP\_RPCSERVICE, vm.conf entry 392

acsd daemon 268, 494

acssel 497

acsssi 495

acstest 491, 498, 499

Activate host 21, 50

Active for Disk 31

Active for Tape 31

Active for Tape and Disk 31

Active Node 31

adding

drives 61, 412

NDMP host credentials 417

robot 51, 410

shared drives 60

volume pool 136, 421

volumes

actions menu 126

nonrobotic 424

robotic 431, 433, 435

update volume configuration 126

ADIC Automated Media Library (AML) 519

ADIC software, installing 521

ADJ\_LSM, vm.conf entry 392

administrative interfaces

character based 10

Java 7

administrator quick reference 383

advanced configuration topics 363

advanced options, robot inventory 176, 188

Allow Backups to Span Media 373

Allow Media Overwrite 369

allowable Media Manager characters 308

allowing nonroot users 382

alternate media types

ACS robots 486

defined 311

example 311

AML (see Distributed AML Server)

AMU (see Archive Management Unit)

API robots 155, 188, 211, 351, 407, 433, 434, 437, 445, 465, 471, 483, 505, 519

API\_BARCODE\_RULES, vm.conf entry 393

Arbitrated Loop Physical Address (ALPA) 295

Archive Management Unit (AMU) 520

assigned

host, drive status 238

volumes 161

assigning tape requests 256

ATL (see Automated Tape Library)

authentication/authorization 44, 378

AUTHORIZATION\_REQUIRED, vm.conf entry 394

auto cleaning 340

AUTO\_PATH\_CORRECTION, vm.conf entry 398

AUTO\_UPDATE\_ROBOT, vm.conf entry 394



---

- Automated Cartridge System
  - adding volumes 491
  - barcode operations 492
  - configuration example 95
  - daemon, acsd 268
  - drive information 70
  - Library Server (ACSLs) 483, 485
  - media requests 485
  - removing tapes 491
  - special characters 491
  - STK Library Station 483, 485
  - Storagenet 6000 (SN6000) 483, 485, 489
- Automated Tape Library (ATL) 508
- Automatic Volume Recognition (AVR)
  - setting 234
- Automatic Volume Recognition (avrd),
  - daemon 266
- auto-populate robot 431
- AVRD\_PEND\_DELAY, vm.conf entry 330, 395
- AVRD\_SCAN\_DELAY, vm.conf entry 395

## B

- Backup Exec, managing volumes 104, 175
- barcode rules
  - add 202, 479
  - change 203, 481
  - delete 481
  - list 482
  - overview 352
  - tag 204
- barcodes
  - overview 350
  - update in robot 149, 460
- bp.conf file 331, 366
- bpclntcmd utility 284
- bpexppdate command 162

## C

- changing
  - cleaning frequency 67, 252
  - cleanings allowed 167, 343
  - drive configuration 77
  - host
    - for Device Monitor 248
  - media description 166, 451
  - robot configuration 77
  - volume attributes 163
  - volume expiration date 165, 453
  - volume group 454

- volume group name 168
  - volume maximum mounts 165, 458
  - volume pool attributes 139, 421
  - volume pool for a volume 166, 167, 452
- character device 74, 412
- CLEAN\_REQUEST\_TIMEOUT, vm.conf
  - entry 395
- cleaning
  - count 117
  - drives 251, 515
  - frequency-based 251, 340, 341
  - library-based 340
  - operator-initiated 252, 340
  - reactive 340
- cleaning tape
  - change cleanings allowed 167, 343, 459
  - number of cleanings left 117
  - set count 132
- CLIENT\_PORT\_WINDOW, vm.conf
  - entry 396
- cluster environments 332, 403
- Cluster Name 31
- CLUSTER\_NAME, vm.conf entry 403
- comment
  - drive, adding 253
  - in drive status list 239
- configuring
  - devices 281
  - drives and robots 17, 37, 407
  - examples, drives and robots 84
  - media 47, 123, 419
  - STK SN6000 drives 490
  - TLM drives 521
- CONNECT\_OPTIONS, vm.conf entry 396
- control mode, drive 237, 241
- control path, robotic 56, 407
- control unit, ACS 485
- crawlreleasebyname, vmopr cmd option 328
- create media ID generation rules 188
- customize
  - Device Monitor window 246
  - Devices window 35
  - Media window 121

## D

- daemons
  - acsd 268
  - avrd 266
  - check with vmops 271



- ltid 265
- nbemm 267
- odld 268
- overview 263
- robotic 270
- stopping 271
- tl4d 269
- tl8cd 269
- tl8d 269
- tlcd 268
- tldd 268
- tlhcd 269
- tlhd 269
- tlmd 270
- tshd 270
- vmd 267
- vmcd 267
- DAS (see Distributed AML Server)
- DAS drive name 25
- DAS\_CLIENT, vm.conf entry 397, 522
- DASADMIN command 523, 526
- Data Lifecycle Manager 110, 115
- data loss 325
- DataSet volume pool 344, 421
- DAYS\_TO\_KEEP\_LOGS, vm.conf entry 397
- Deactivate host 21, 50
- Deactivated 31
- deassign volumes 161
- decommission a media server 365
- deleting
  - drive 79, 414
  - robot 415
  - volume group 156, 451
  - volume pool 141, 424
  - volumes 155, 449, 450
- density for media types 245
- denying requests 260
- description, for new volume 131
- device
  - character 74
  - configuration wizard 11, 12, 48, 60, 61, 71, 77, 287, 296, 488
  - discovery 36, 48, 321
  - drivers 281, 282
  - file permission 277
  - files 282
  - no rewind 67
  - volume header 74
- device allocation host 285, 301, 302
- Device Configuration wizard 336, 527
- device file, robotic 56, 411
- device host
  - for move volume 154
  - for new volume 129
  - viewing remotely 42
- device management
  - daemons 263
  - starting ltid 265
  - stopping ltid 266
- device mapping file 39
- Device Monitor
  - add drive comment 253
  - assigning requests 256
  - changing host 248
  - display pending requests 254
  - display the window 232
  - overview 231
  - resubmit request 259
- Devices management window
  - displaying 18
  - menus 19
  - toolbar 22
- DISABLE\_SCSI\_RESERVE bp.conf entry 331
- DISABLE\_STANDALONE\_DRIVE\_EXTENSIONS 124
- display device configuration 418
- Distributed AML Server
  - \ETC\CONFIG file 525
  - \MPTN\ETC\HOSTS file 525
  - overview 519
- Distributed AML Server (also see Tape Library Multimedia)
- down a device 370
- down drive, setting 234
- drive
  - access permission 277
  - ACS information 412
  - add (see adding)
  - add comment 253
  - changing operating mode 249
  - character device 74, 412
  - cleaning 234
  - cleaning frequency 67, 252
  - control mode 237, 241
  - delete (see deleting)
  - diagnose tests 20
  - dip switches 284



---

- drive status 68
- monitoring use 231
- name 412
- no rewind device 67, 412
- performing diagnostics 79
- qualification tests 20
- robot drive number 69, 75, 412
- robot library, controlling drive 69
- robot number, controlling drive 412
- servicing requests 254
- Sony dip switches 286
- standalone 69, 74, 412
- TLH information 71, 412
- TLM information 71, 412
- type 67, 412
- types and densities 236
- update configuration (see updating)
- virtualization 489
- volume header device 74, 412
- drive cleaning
  - for TLH robots 515
  - managing 342
  - manual 343
  - Media and Device Management
  - menu 251
  - operator-initiated 343
- Drive Name Rule 64
- Drive paths list
  - Bus 243
  - Control 241
  - Device Host 240
  - Drive Index 243
  - Drive Name 240
  - Drive Path 242
  - Lun 243
  - NDMP Host 240
  - Port 243
  - Target 243
- drive\_mount\_notify script 274
- drive\_unmount\_notify script 276
- Drives List, Devices window 24
- Drives status list
  - Assigned Host field 238
  - Comment field 239
  - Control field 237
  - Device Host field 239
  - Device Monitor window 236
  - Drive Index field 240
  - Drive Name field 236

- Drive Path field 239
- Drive Type field 236
- External Media ID field 238
- Media Label field 239
- Ready field 238
- Recorded Media ID field 238
- Request ID field 238
- Shared field 239
- Writable field 238
- drstat command 321

## E

- eject volume from robot
  - multiple volumes 107
- eject volumes from robot
  - menu command 107
- EMM database 5
- EMM server
  - default 46
- empty media access port prior to update 188
- ENABLE\_ROBOT\_AUTH, vm.conf
  - entry 398
- enhanced authorization
  - allowable Media Manager
  - commands 382
  - allowing 382
- Enterprise Media Manager (EMM) Server 3
- Enterprise Media Manager database host
  - recommendations 285
  - requirements 285
- erasing media 159
- examples
  - SAN components 280
  - SSO components configuration 300
- expired media 138
- External Media ID
  - drive status 238
  - pending requests 244

## F

- fibre channel
  - arbitrated loop 280
  - hub 280
  - switch 280
  - switched fabric 280
- file
  - name on tpreq 274
  - positioning to on tape 275
- filter, volume list 440
- find command 19, 106, 233





---

- firmware levels 282, 295
- first media ID, add volume range 131
- First Mount field 116
- first slot number
  - add volumes 131
  - for move volumes 155
- format description for optical 376
- format optical media 482
- fragmented backups 377
- freeze media 119
- frequency-based drive cleaning 251, 341

## G

- get\_license\_key command 287
- global device database host
  - conflict 45

## H

- host
  - activate 21, 50
  - deactivate 21, 50
  - device 4
  - for Device Monitor 248
  - for robotic control 58
  - for volume pool 137, 139
- host name, selection
  - robotic control 408, 411
- Host status 31
- Hosts List, Devices window 30, 32
- HyperTerminal 283

## I

- IBM Automated Tape Library 505
  - (also see Tape Library Half-inch)
- IBM device number 25, 71, 321, 412, 514
- images, expiring with bpexpdate 162
- inject volume into robot
  - add volume 435
  - multiple volumes 188
  - robot inventory 146
- install and configure ADIC software 521
- inventory a robot and report contents 461
- inventory and compare robot contents 182, 463
- inventory and update robot 465
- INVENTORY\_FILTER, vm.conf entry 398

## L

- label
  - media tapes 124
  - new media 157

- optical media 195
- Library Management Unit 485
- Library Manager Control Point daemon (LMCPD) 508
- library sharing 55
- Library Storage Module 485
- library-based cleaning 341
- license keys 279, 287, 490
- LMCP device file 509
- LMCPD 508
- LMU (see Library Management Unit)
- logging 272
- long erase 107, 160
- LSM (see Library Storage Module)
- ltid
  - daemon 265
  - debug logging 265, 270
  - starting 265
  - stopping 266

## M

- making advanced configuration
  - changes 363
- MAP\_CONTINUE\_TIMEOUT, vm.conf entry 400
- MAP\_ID, vm.conf entry 399
- master server 4
- maximum barcode lengths 351
- maximum concurrent drives for backup 288
- maximum mounts
  - add volume 132
  - change volumes 165, 458
- media
  - density 245
  - formats 375
  - freeze 119
  - mount and unmount 370
  - recycling 172
  - replacing 170
  - selection algorithm 371, 373
  - servers 4
  - spanning 372, 374
  - unfreeze 119
  - unsuspend 119
- media ID
  - generation rules 210, 354, 432, 466
  - prefix for update robot 194
  - style for new volumes 130
- media ID, add volume 130



- 
- Media management window
    - displaying 104
    - menus 19, 105
    - toolbar 107
  - Media Manager
    - overview 1
    - allowable characters 308
    - authentication/authorization
    - security 379
    - best practices 304
    - configuration file 387
    - hosts, overview 3
    - security 44, 378, 381
    - volume daemon (see nbemm)
  - media pool (see volume pool)
  - media server 299
  - media settings tab 176
  - media type
    - 4MM 310
    - 4MM\_CLN 311
    - 8MM 310
    - 8MM\_CLN 311
    - 8MM2 310
    - 8MM2\_CLN 311
    - 8MM3 310
    - 8MM3\_CLN 311
    - DLT 310
    - DLT\_CLN 311
    - DLT2 310
    - DLT2\_CLN 311
    - DLT3 310
    - DLT3\_CLN 311
    - DTF 310
    - DTF\_CLN 311
    - for new volume 128
    - HC\_CLN 310
    - HC2\_CLN 310
    - HC3\_CLN 310
    - HCART 310
    - HCART2 310
    - HCART3 310
    - QCART 310
    - REWR\_OPT 310
    - when not an API robot 197
    - WORM\_OPT 310
  - media type mappings (API robots) 212
  - MEDIA\_ID\_BARCODE\_CHARS, vm.conf entry 400
  - MEDIA\_ID\_PREFIX, vm.conf entry 401
  - MM\_SERVER\_NAME, vm.conf entry 403
  - mount media 370
  - mount requests, pending 254
  - move volume group 169
  - move volumes
    - logical move 350
    - methods available 151
    - multiple volumes 442, 445
    - overview 151, 349
    - physical move 349
    - single volume 442, 443
    - update volume configuration 151
    - volume group 448
  - mtlib command, IBM 510
  - multiplexed backups 377
  - multiplexing (MPX) tape format 377
- N**
- naming conventions 308
  - nbemm 263, 299
    - daemon 267
    - starting 267
    - stopping 267
  - nbemm/DA, definition 299
  - NDMP configurations 286, 331
  - NDMP host credentials
    - add (see adding)
  - NDMP hosts 48
  - NetBackup
    - authentication 378
    - authorization 378
    - patches 40
    - pool 110, 115
    - volume pool 141, 421
    - wizards 8
  - NetBackup Administration Console 7
  - NetBackup and Media Manager databases 5
  - NetBackup Catalog 6
  - NetBackup Enterprise Server 122, 248
  - NetBackup Server 122, 248
  - NetBackup Vault
    - date returned 456
    - date sent 456
    - session ID 458
    - slot 457
    - vault name 455
  - no rewind device 67, 412
  - number of platters 130
  - number of volumes 129



---

## O

- odld daemon 268
- Offline 31
- online help
  - tpconfig 410
  - vmadm 421, 424
- operating mode of drive, changing 249
- operating system changes 283
- optical disk
  - format 376
  - format and label 482
  - partner ID 116
  - platter side 116
  - usage 276
- Optical Disk Library (ODL) daemon 268
- optical partner (see Partner ID)
- optical volumes 130, 131, 134, 153
- overview of
  - barcodes 350
  - daemons 263
  - drive cleaning 340
  - Media Manager 1
  - robots 308
  - shared drives 279
  - vmadm 419
  - volume groups 344
  - volume pools 344

## P

- partially-configured devices 49
- pending actions
  - notation 255
  - overview 255
  - resolving 259
- pending requests
  - Barcode field 245
  - Density field 245
  - External Media ID field 244
  - Host Name field 244
  - Mode field 245
  - Recorded Media ID field 244
  - Request ID field 244
  - Time field 245
  - Volume Group field 245
- permissions, for device access 277
- physical inventory utility 354
- positioning tape files 275
- PREFERRED\_GROUP, vm.conf entry 401
- pre-labeling media 369

- PREVENT\_MEDIA\_REMOVAL, vm.conf entry 402
- preview volume configuration update 187
- print device configuration 84
- printing
  - device configuration 418
  - volumes report 439
- processes
  - check with vmps 271
  - robotic 264
  - robotic control 264

## Q

- quick erase 107, 160

## R

- RANDOM\_PORTS, vm.conf entry 402
- rdevmi 301
- reactive cleaning 340
- reading tape files 274
- ready status 238
- recommended method of configuring devices 48
- reconfiguring devices in a SSO
  - configuration 363
- Recorded Media ID
  - drive status 238
  - pending requests 244
- recycle media 172
- refresh rate, changing 247
- relabel
  - used media 157
- remote device management 41
- RemoteStorage 110, 115
- remove a server from a configuration 365
- removing tape files 275
- replace media 170
- replacing a device in a SSO
  - configuration 363
- requests
  - assigning 256
  - denying 260
  - display pending 254
  - example assignment 257
  - identification number
    - drive status 238
    - pending requests 244
  - overview 254
  - resubmitting 259
  - user tape 273



---

REQUIRED\_INTERFACE, vm.conf  
     entry 403  
 RESERVATION CONFLICT status 329  
 reset  
     mount time 252  
 residence, update volume configuration 186  
 retention period, expiring backups with  
     bpexpdate 162  
 rewinding tape files 275  
 right-click shortcut menus 10, 34, 120, 246  
 robot  
     add (see adding)  
     attributes 311  
     barcode rules 202, 477  
     barcode update 149, 460  
     control host 58, 411  
     delete (see deleting)  
     destination for move volume 154  
     device file 56, 411  
     device host 53  
     diagnose tests 20  
     drive number 69, 75  
     for new volume 129  
     inventory 134, 175  
     inventory and compare contents 182, 463  
     number 53, 411  
     performing diagnostics 79  
     process 264  
     qualification tests 20  
     remote control host 411  
     robotic daemons 270  
     sharing without SSO 299  
     show robot contents 461  
     type 53, 411  
     update configuration (see updating)  
     update volume configuration 184, 465  
 robot number  
     for add drive 412  
     for add robot 411  
 robot type  
     ACS 309  
     ODL 309  
     TL4 309  
     TL8 309  
     TLD 309  
     TLH 309  
     TLM 309  
     TSH 309  
 robotic  
     cleaning 340  
     control host 58, 408, 411  
     control process 264  
     device file 56  
     drive 412  
     library 69  
     test utilities 320, 499  
 robotic control path (see robotic device file)  
 robotic inventory  
     advanced options 176  
     filtering 501, 518  
 Robots List  
     Devices window 29  
     Media window 112  
 robtest 321, 384, 498, 526, 527

**S**

SAN media server 4, 299  
 SAN Shared Storage Option (see SSO)  
 scan host 300, 301  
 scratch pool 423  
     adding 138  
     changing to 424  
     overview 347  
 scripts  
     drive\_mount\_notify 274  
     drive\_unmount\_notify 276  
     vmps 271  
 SCSI Long Erase 160  
 SCSI pass-thru command 48, 141  
 SCSI pass-thru path 141  
 SCSI Quick Erase 159  
 SCSI reserve/release  
     break a reservation 325  
     controlling use of 331  
     crawlreleasebyname option 328  
     error recovery 328  
     in NetBackup 325, 326  
     limitations 329, 331  
     overview 324  
     PEND status 329  
     requirements 331  
     RESERVATION CONFLICT 325, 329  
 SCSI-to-fibre  
     bridges 283  
     mapping 282  
 SERVER, vm.conf entry 44, 403  
 Servers  
     EMM Server 3



- master 4
  - SAN media server 4
- set of allowable characters 308
- shared drives (see SSO)
- shared drives, definition 298
- shared library support 299
- shared media 286
- shared robots, without SSO 299
- shared storage option, key 279, 287
- shared\_drive\_notify script 280
- shortcut menus 10, 34, 120, 246
- show robot contents 179, 461
- slot number
  - add volume 131
  - for move volumes 155
- Sony AIT tape drives 286
- spanning media 372
  - enabling 372, 374
  - tape format 377
- SSO
  - configuration wizards 48
  - configuring non-serialized shared TLM drives 527
  - configuring shared ACS drives 488
  - configuring TLM robot types 525, 526
  - definition 279
  - device allocation host 285, 300, 302
  - Device Allocation Host Summary 261
  - drive operating mode 249, 254
  - hardware requirements 279
  - license key 490
  - scan host 300, 301
  - Shared Drive Summary 261
  - supported robot types 285
  - supported SAN hardware 297
  - supported server platforms 285
  - terminology 298
  - tpconfig 413
  - unsupported robot types 285
  - vm.conf entries 404, 405
- SSO\_DA\_REREGISTER\_INTERVAL, vm.conf entry 404
- SSO\_DA\_RETRY\_TIMEOUT, vm.conf entry 404
- SSO\_HOST\_NAME, vm.conf entry 405
- SSO\_SCAN\_ABILITY, vm.conf entry 238, 242
- standalone drive
  - add drive 69, 74

- standalone extensions, disabling 374
  - tpconfig 412
- Status
  - Host 31
- stopltid command 266
- Storage Area Network (SAN) 4, 279, 281, 286, 294, 299
- storage devices, steps for attaching 36
- supported
  - robot types 285
  - SAN hardware 297
  - server platforms 285
- suspend media 370
- syslogd 272

## T

- table-driven robotics 320
- tape configuration utility (see tpconfig)
- tape format
  - fragmented 377
  - multiplexed 377
  - non-QIC 376
  - QIC/WORM 376
  - spanned tapes 377
- Tape Library (TLD) daemon 268
- Tape Library 4MM (TL4) daemon 269
- Tape Library 8MM (TL8) daemon 269
- Tape Library Half-inch (TLH)
  - adding volumes 515
  - cleaning drives 515
  - configuration example 98
  - configuring robotic control 509
  - control daemon 269, 508
  - daemon 269, 508
  - drive information 71
  - drive mapping 514
  - media requests 508
  - removing tapes 515
  - robot inventory 516
- Tape Library Multimedia (TLM)
  - adding volumes 528
  - allocating drives 521
  - configuration example 100
  - configuring drives 524
  - configuring robotic control 521
  - daemon 270, 520
  - drive information 71
  - drive mapping 524
  - inventory operations 530



---

- media requests 521
- overview 519
- removing tapes 529
- tape spanning 372, 374
- Tape Stacker Half-inch (TSH) daemon 270
- TapeAlert 2, 68, 332, 340
  - log codes 333
  - requirements 332
- tapes and tape files
  - assigning requests 256
  - density 273
  - example of handling a request 257
  - file name 274
  - labels 239
  - mode 245
  - positioning tape file 275
  - reading tape files 274
  - removing tape files 275
  - requesting tapes 273
  - rewinding 275
  - time requested 245
  - using optical disk 276
  - volume pool assignment 274
  - writing tape files 274
- tested SAN components 298
- tl4d daemon 269
- tl8cd daemon 269
- tl8d daemon 269
- tl added daemon 268
- tl added daemon 268
- TLH\_ vm.conf entry 405
- tl added daemon 269
- tl added daemon 269
- TLM\_ vm.conf entry 405
- tl added daemon 270
- tl added 524, 526, 527, 528, 529
- toolbars, viewing and customizing 107
- tpconfig
  - adding drive 412
  - adding NDMP host credentials 417
  - adding robot 410
  - deleting drive 414
  - deleting robots 415
  - menus 409
  - online help 410
  - overview 407
  - printing device configuration 418
  - starting 409
  - stopping 409

- update drive configuration 414
- update robot configuration 413
- tpconfig menus 61
- tpreq, requesting tapes 273
- tpunmount, removing tape files 275
- tshd daemon 270

## U

- unfreeze media 119
- unmount media 370
- unsupported
  - characters 189
  - robot types 285, 286
- unsuspend media 119
- up drive, standard mode (AVR) 234
- update and rescan barcodes 149
- update barcodes 149
- update robot
  - procedure 187, 465
  - update options 469
- update volume configuration
  - when not to use 186
  - when to use 185
- updating
  - barcodes 460
  - drive configuration 414
  - robot configuration 413
- user
  - access to devices 277
  - tape requests 273
- using Media Manager devices with other applications 304

## V

- VERBOSE, vm.conf entry 405
- VERITAS Backup Exec 286, 298
- VERITAS Storage Migrator 13, 284, 286, 299
- VERITAS support web site 39
- Virtual Cluster 31
- vm.conf file
  - ACS\_ entries 389
  - ACS\_CSI\_HOSTPORT entries 390
  - ACS\_SEL\_SOCKET entries 389
  - ACS\_SSI\_HOSTNAME entries 390
  - ACS\_SSI\_INET\_PORT entries 391
  - ACS\_SSI\_SOCKET entries 391
  - ACS\_TCP\_RPCSERVICE entries 392
  - ACS\_UDP\_RPCSERVICE entries 392
  - adding SERVER entries 44
  - ADJ\_LSM entries 392



---

- API\_BARCODE\_RULES entries 393
- AUTHORIZATION\_REQUIRED entries 394
- AUTO\_PATH\_CORRECTION entries 398
- AUTO\_UPDATE\_ROBOT entries 394
- AVRD\_PEND\_DELAY entries 395
- AVRD\_SCAN\_DELAY entries 395
- CLEAN\_REQUEST\_TIMEOUT entries 395
- CLIENT\_PORT\_WINDOW entries 396
- CLUSTER\_NAME entries 403
- CONNECT\_OPTIONS entries 396
- DAS\_CLIENT entries 397, 522
- DAYS\_TO\_KEEP\_LOGS entries 397
- ENABLE\_ROBOT\_AUTH entries 398
- INVENTORY\_FILTER entries 398
- MAP\_CONTINUE\_TIMEOUT entries 400
- MAP\_ID entries 399
- MEDIA\_ID\_BARCODE\_CHARS entries 400
- MEDIA\_ID\_PREFIX entries 401
- MM\_SERVER\_NAME entries 403
- overview 387
- PREFERRED\_GROUP entries 401
- PREVENT\_MEDIA\_REMOVAL entries 402
- RANDOM\_PORTS entries 402
- REQUIRED\_INTERFACE entries 403
- SERVER entries 403
- SSO\_DA\_REREGISTER\_INTERVAL entries 404
- SSO\_DA\_RETRY\_TIMEOUT entries 404
- SSO\_HOST\_NAME entries 405
- TLH\_ entries 405
- TLM\_ entries 405
- VERBOSE entries 405
- vmadm
  - overview 419
  - add volume (see adding)
  - barcode update 460
  - change volume's volume pool 452
  - changing
    - media description 451
    - volume expiration date 453
    - volume maximum mounts 458
  - command 419
  - deleting
    - multiple volumes 450
    - single volume 449
    - volume group 451
  - displaying volume configuration 439
  - format optical disk 482
  - inventory and report robot contents 461
  - media configuration, changing
    - description 451
  - moving volume group 448
  - moving volumes (see move volumes)
  - online help 421, 424
  - printing volume configuration 439
  - starting vmadm 419
  - stopping vmd 420
  - verify robot contents 463
  - verify selected robot volumes 460
  - volume configuration
    - barcode rules 477
    - update robot 465
- vmd
  - command 267, 419
  - daemon 267
  - starting 267
    - by command 267, 419
    - using vmadm 419
  - stopping 267, 420
- vmmps script 271
- vmscd
  - daemon 267
- Volume Configuration wizard 11, 12, 47, 134
- volume group
  - add volume 133
  - changing 454
  - changing name 168
  - deleting 156
  - deleting (see deleting)
  - field 245
  - for move volume 155
  - moving 169
  - rules for assigning 345
- Volume Groups list, Media window 111
- volume header device 412
- volume is in a robotic library
  - for move volume 153
  - for new volume 128
- volume pool
  - add volume 134
  - adding 136
  - change assignment 452



---

- changing attributes 139, 421
- changing for a volume 167
- configuring a scratch pool 347
- DataStore pool 110, 115
- deleting 141
- for update robot 201
- host name 137, 139
- HSM pool 110, 115
- NetBackup pool 110, 115
- overview 14, 135, 344
- RemoteStorage pool 110, 115
- Volume Pools list, Media window 109
- volumes
  - adding (see adding)
  - assigned 161
  - changing (see changing)
  - changing configuration (see changing)
  - cleaning count 167
  - deleting (see deleting)
  - description for new volume 131
  - description, changing 451
  - first time mounted 116
  - for move volume 153
  - header device 74
  - list 439
  - maximum mounts allowed 132
  - media ID style 130
  - moving 151, 349
  - moving (see move volumes)
  - moving, actions menu 151
  - platter side 116
  - recycling 172
  - replacing 170
  - without barcodes 2, 104
- Volumes list, Media window 113

**W**

- wizard
  - device configuration 11, 12, 48, 60, 77, 282, 296, 336
  - shared drive configuration 60, 287
  - volume configuration 11, 12
- Writable field 238
- writing tape files 274