VERITAS NetBackup BusinesServer™ 4.5

System Administrator's Guide

for Windows

March 2002
30-000484-011

VERITAS

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.

Copyright

Copyright © 1993-2002 VERITAS Software Corporation. All Rights Reserved. VERITAS, VERITAS SOFTWARE, the VERITAS logo, *Business Without Interruption*, VERITAS The Data Availability Company, VERITAS NetBackup, VERITAS NetBackup BusinesServer, VERITAS Remote Storage for Microsoft Exchange, VERITAS Storage Migrator, and VERITAS Storage Migrator Remote are trademarks or registered trademarks of VERITAS Software Corporation in the U.S. and / or other countries. Other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

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

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
Phone 650–527–8000
Fax 650–527–8050
www.veritas.com

Contents

Audience xxxi
Organization xxxi
Related Documents xxxiii
Accessibility xxxiii
Support for Assistive Technology xxxiv
Using the Keyboard to Navigate in NetBackup xxxiv
Navigating in a NetBackup Tree View xxxiv
Accelerator Keys xxxvii
Mnemonic Keys xxxvii
Using the Keyboard in Dialogs xxxvii
Online Documentation xxxviii
Conventions xxxix
Type Style xxxix
Notes and Cautions xxxix
Key Combinations xxxix
Command Usage xl
Terms xl
Getting Help xli

Chapter 1. Introduction to NetBackup 1
Overview 1
Using the NetBackup Administration Console 3
User Backups, Archives, and Restores 5
Activity Monitor 6

NetBackup Management 6
Reports 6
Policies 6
Storage Units 7
Volumes 8
Catalog 8
Host Properties 9
Media Manager 9
NetBackup Configuration Wizards 9
Getting Started 9
Configure Storage Devices 10
Configure Volumes 10
Configure the Catalog Backup 10
Create a Backup Policy 10
Import Wizard 10
Configure a Shared Drive 10
Menus 10
File Menu 10
Edit Menu 11
View Menu 12
Actions Menu 13
Help Menu 13
Standard and User Toolbars 14
Customizing the Administration Console 14
Shortcut Menus 14
Status Bar 14
Configuring NetBackup Without Wizards 15
NetBackup Online Help 16
Finding a Topic 16
Using Context-Sensitive Help 17

Printing Help 17
Changing Fonts 17
Using Tooltips 17
Using Other Help Features 18
Getting Help While Working in NetBackup Optional Products 18
Online Documents 18
Installing the Documents 20

Chapter 2. Managing Storage Units 21
Introduction to Storage Units 22
Viewing Storage Units and Storage Unit Groups 22
Using the Device Configuration Wizard 23
Storage Unit Considerations 23
Media Manager Storage Unit Considerations 23
Before Adding a Media Manager Storage Unit 24
Disk Storage Unit Considerations 26
NDMP Storage Unit Considerations 26
Maintaining Storage Units 27
Adding a New Storage Unit 27
Changing Storage Unit Properties 28
Deleting Storage Units 28
Storage Unit Properties 29
Storage Unit General Properties Tab 29
Storage Unit Type 29
On Demand Only 29
Storage Unit Type Properties Tab 30
NetBackup Media Server 30
Robot Type 31
Absolute Pathname to Directory 31
Robot Number 31

NDMP Host 31
Density 31
Maximum Concurrent Drives Used for Backup 31
Maximum Concurrent Jobs 32
Maximum Fragment Size 32
Maximum Multiplexing per Drive 32
Configuring Drive Availability Checking 33
Interval Between Status Checks 33
Drive Count Timeout 33
Requeuing Jobs If Required Storage Units are Unavailable 33
Creating and Changing Storage Unit Groups 35

Chapter 3. Managing Backup Policies 39
Using the Policies Utility 40
Tree and Detail Views 40
Menus 42
Standard and User Toolbars 43
Introduction to Backup Policies 44
General Attributes on the Attributes Tab 44
Schedules on the Schedules Tab 44
File List on the Files Tab 45
Client List on the Clients Tab 45
Configuring Backup Policies 45
Example Backup Policies 46
Planning Guidelines for Backup Policies 47
Changing Policies 53
Copying or Moving Policy Information Between Servers 56
Changing Multiple Policies in the Composite View 56
Using the Composite Change Dialog 57
Policy Attributes Tab 58

Policy Type 58
Offhost Backup Method 60
Policy Storage Unit 60
Policy Volume Pool 61
Limit Jobs Per Policy 62
Job Priority 63
Keyword Phrase (Optional) 64
Active. Go Into Effect At 64
Allow Frozen Image Clients 64
Cross Mount Points 64
Collect True Image Restore Information 65
Compression 68
Encryption 70
Collect Disaster Recovery Information 70
Allow Multiple Data Streams 70
Clients Tab 75
Files Tab 77
Specifying the List of Files to Back Up 77
Adding Directives to the File List 80
Verifying the File List 81
Rules for Backup File Paths 83
File-Path Rules for Microsoft Windows Clients 83
File Backups 83
Windows Disk-Image (raw) Backup 85
Microsoft Windows Registry Backup 86
Hard Links to Files (NTFS volumes only) 87
File-Path Rules for OS/2 Clients 89
File-Path Rules for NetWare NonTarget Clients 89
File-Path Rules for NetWare Target Clients 90
File-Path Rules for Macintosh Clients 91

File-Path Rules for Clients Running Extension Products 92
File-Path Rules for UNIX Clients 92
Notes on File Lists for UNIX Clients 93
Symbolic Links to Files or Directories 94
Hard Links to Directories 95
Hard Links to Files 95
UNIX Raw Partitions 96
File List Directives: General Discussion 98
ALL_LOCAL_DRIVES Directive 98
SYSTEM_STATE Directive 99
Directives for Multiple Data Streams 99
Directives for Specific Policy Types 100
File List Directives for Multiple Data Streams 100
NEW_STREAM 101
ALL_LOCAL_DRIVES 104
UNSET and UNSET_ALL 105
Excluding Files From Automatic Backups 106
Schedule Tab 108
Creating or Editing a Schedule on the Attributes Tab 108
Schedule Attributes Tab 109
Name 110
Type of Backup 110
Calendar Schedule Type 112
Frequency Schedule Type 112
Multiple Copies (Inline Tape Copy) 113
Override Policy Storage Unit 114
Override Policy Volume Pool 115
Retention 115
Media Multiplexing 117
Start Window Tab 118

Exclude Dates Tab 121
Calendar Schedule Tab 122
Examples of Automatic-Backup Schedules 125
Example 1 125
Example 2 128
Example 3 133
Example 4 134
Example 5 135
Example 6 136
Considerations for User Schedules 138
Planning User Backup and Archive Schedules 139
Creating Separate Policies for User Schedules 139
Using a Specific Policy and User Schedule 141
Creating a Vault Policy 141
Performing Manual Backups 142

Chapter 4. Using Catalog for Catalog Backups and Verifying, Duplicating, and Importing Images 145

Introduction to the NetBackup Catalogs 146
Where are the Catalog Files? 146
What Method Do I Use to Back Them Up? 146
What Types of Media Can I Use? 146
How Do I Know If a Catalog Backup Succeeded? 147
How Do I Restore The Catalog Backups? 147
Important Precautions to Observe 147
Configuring Catalog Backups 149
Catalog Attributes Tab 150
Media Server 150
Last Media Used 150
Media 1 and Media 2 Areas 150
Catalog Schedule Tab 154

Recommendations 155
Catalog Files Tab 156
Catalog Pathnames 157
Backing Up the Catalogs Manually 159
Protecting Large NetBackup Catalogs 159
Layout of the NetBackup Catalogs 160
Catalog Backup and Restore Concepts 160
Multiple-Tape Catalog Backups 160
Multiple-Tape Catalog Restores 161
Setting up Multiple-Tape NetBackup Catalog Backups 161
Create a Batch File to Initiate the Backups 163
How To Initiate a Multiple-Tape Catalog Backup 163
Managing the NetBackup Catalogs 165
About the Binary Catalog Format 165
Catalog Conversion Utility 165
Binary Catalog File Limitations 165
Determining Catalog Space Requirements 166
File Size Considerations 168
Compressing the Image Catalog 170
Moving the NetBackup Image Catalog 171
Converting the Catalog Format 173
Reduce Restore Times by Indexing the Image Catalog 173
Catalog Index Examples 174
Catalog Index Space Requirements 174
Disabling Catalog Indexing 175
Searching for Backup Images 175
Verifying Backup Images 177
Duplicating Backup Images 178
Promoting a Copy to a Primary Copy 183
Expiring Backup Images 184

Importing Backup Images 184
Viewing Job Results 189

Chapter 5. Viewing NetBackup Reports 191
NetBackup Management Reports Application 192
Reports Window 193
Customizing the Window 193
Standard and User Toolbars 194
Report Contents Pane 194
Status Bar 194
Shortcut Menus 194
Reports Settings 195
Date/Time 195
Client 195
Media Server 195
Job ID 195
Media ID 195
Volume Pool 195
Verbose Listing 196
Report Descriptions 197
Status of Backups Report 197
Client Backups Report 198
Problems Report 199
All Log Entries Report 200
Media Lists Report 201
Media Contents Report 203
Images on Media Report 206
Media Logs Report 208
Media Summary Report 208
Media Written Report 209

Using the Troubleshooting Wizard With Reports 209

Chapter 6. Monitoring NetBackup Activity 211

Introduction to the Activity Monitor 212

Menu Bar 212

Shortcut Menus 213

Standard and User Toolbars 213

Status Bar 214

Activity Monitor Topology 214

Topology Connections 215

Selecting Topology Objects 216

Jobs Tab 217

Using Filters to Customize the Jobs List Output 217

Viewing Job Details 221

Services Tab 225

Processes Tab 228

Drives Tab 230

Using the Troubleshooting Wizard 231

Media Mount Errors 232

Queued Media Mount Errors 232

Cancelled Media Mount Errors 233

Managing the Jobs Database 233

Jobs Retention Period Options 234

BPDBJOBS_OPTIONS Environment Variable 235

bpdbjobs Command Line Options 235

bpdbjobs Debug Log 236

Chapter 7. Configuring Host Properties 237

Viewing Host Properties 238

Changing Settings in the Properties Tabs 238

Interpreting the Initial Settings 238

Changing Property Settings 239
Selecting Multiple Hosts 239
Getting Help on Property Settings 240
Required Permissions 240
Master Server Properties 241
General Tab 241
Global NetBackup Attributes Tab 242
Wakeup Interval 242
Schedule Backup Attempts 242
Duration to Retain Logs 243
How Long to Keep TIR Information 243
Enforce Media Mount Timeout After 243
Maximum Jobs per Client 244
Maximum Backup Copies 245
Interval for Status Reports 245
Days to Keep Vault Files 245
Compress Catalog After 245
Administrator E-mail Address 245
Retention Periods Tab 246
Value 246
Units 246
Retention Periods List 246
Schedules List 246
Impact Report Button 247
Reset Button 247
Reset All Button 247
Set to Defaults 247
Note on Redefining Retention Periods 249
Universal Settings Tab 249
File Browse Timeout 249

Restore Retries 250
Client Read Timeout 250
Disallow Server File Writes 250
Allow Non-reserved Ports 251
Enable Performance Data Collection 251
Required Network Interface 251
Preferred Group 252
Server Sends Mail 253
Client Sends Mail 254
E-mail Address for Administrator of this NetBackup Client 254
Servers Tab 254
Host 254
Master Server 254
Additional Servers 255
Global Operations 255
Timeouts Tab 256
Client Connect Timeout 256
Initial Browse Search Limit 256
Disallow Client Browse and Restore 257
Disallow Client Restore 257
Backup Start Notify Timeout 257
Backup End Notify Timeout 257
Logging Tab 258
Enable Logging 258
Global Logging Level 258
BPSCHED Logging 259
BPBRM Logging 259
BPTM Logging 259
BPDM Logging 259
BPRD Logging 259

BPDBM Logging 259
Vault Logging 259
Verbose Logging Level 260
Authorization Tab 260
User 260
Domain\Group 260
Host 260
Local/Network 260
User must be an OS Administrator 261
Firewall Tab 261
Add Button 261
Delete Button 261
Use Reserved Ports 261
Use Non-reserved Ports 261
Use BPCD 261
Use VNETD 262
Client Attributes Tab 262
Clients List 262
Add Button 262
Delete Button 263
Maximum Data Streams 263
Connect on Non-reserved Port 263
No Callback 263
List Restore 263
Free Browse 264
GDM Tab 267
GDM Server 267
Dashboard Port Window 267
Media Servers Tab 268
Additional Servers 268

Add to All Lists 268
Remove From All Lists 268
Bandwidth Tab 269
Bandwidth Settings for These NetBackup Client Machines 269
From IP Address 269
To IP Address 269
Bandwidth 269
Add Range Button 270
Remove Range Button 270
Restore Tab 270
General Server Tab 271
Delay on Multiplexed Restores 271
Re-read Interval 272
Must Use Local Drive 272
Use Random Port Assignments 272
Timeout in Queue 272
Queue 272
Client Port Window 273
Client Reserved Port Window 273
Server Reserved Port Window 274
Server Port Window 274
Media Tab 274
Allow Media Overwrite 274
Allow Multiple Retentions Per Media 275
Disallow Backups Spanning Media 276
Disable SCSI Reserve 276
Disable Standalone Drive Extensions 276
Disable Job Logging 276
Media ID Prefix 276
Media Unmount Delay 277

Media Request Delay 277
UNIX Server 277
Apollo Restore Timeout 277
Maximum Restore Apollo arg Characters 278
NFS Access Timeout 278
Media Server Properties 278
Client Properties 279
Exchange Tab 280
Mailbox for Message Level Backup and Restore 280
Client Name Tab 281
Client Name 281
General Client Tab 282
Keep Status of User-directed Backups, Archives, and Restores 282
Random Ports 282
Client Port Window 282
Client Reserved Port Window 283
Logging Tab 283
OTM (Open Transaction Manager) Tab 283
Enable OTM During Backups 284
Cache File 284
Initial Cache Size 284
Maximum Cache Size 285
Busy File Wait 285
Busy File Timeout 285
Individual Drive Snapshots 285
Global Drive Snapshot 286
Logging Level 286
Error Control 286
Synchronization Timeout 287
Cached Files 287

Guidelines for Setting OTM Cache 288
Using OTM with Databases 290
Timeouts Tab 292
User Directed Timeout 292
Encryption Tab 292
Encryption Permissions 292
Encryption Strength 293
Encryption Libraries 293
Encryption Keyfile 293
Lotus Notes Tab 294
Path 294
.INI File 294
Exclude Tab 295
Client 295
Policy 295
Delete Policy 296
Schedule 296
Files and Directories 296
Copy 296
Paste 296
Delete List Item 296
Edit List Item 296
Add List Item 297
Include Tab 297
Files / Directories 298
Copy 298
Paste 298
Add List Item 298
Edit List Item 298
Exclude and Include Lists for Specific Policies or Schedules 298

Syntax Rules for Exclude and Include Lists 300
Traversing Excluded Directories 302
PC Client Settings Tab 303
Maximum Error Messages for Server 303
General Level Troubleshooting 303
Troubleshooting - TCP Level 303
Windows Client Tab 304
Wait Time Before Clearing Archive Bit 304
Perform Incrementals Based on Archive Bit 304
Time Overlap 305
Communications Buffer Size 305
Perform Default Search for Restore 305
Case Sensitive Exclude List 305
Network Tab 306
NetBackup Client Service Port (BPCD) 306
NetBackup Request Service Port (BPRD) 306
Announce DHCP Interval 306
Client Settings Tab (UNIX) 307
Do Not Compress Files Ending With 307
Add to All Lists 307
Remove from All Lists 307
Frozen Image Configuration 307
UNIX Client2 Tab 308
Do Not Reset File Access Time 308
Megabytes of Memory 308
Locked File Action 309
Busy File Settings 309
Host 309
Working Directory 309
Operator’s E-mail Address 309

Process Busy Files 310
File Action File List 310
Action Taken On Busy File 310
Retry Count 310
NetWare Tab 310
Backup Migrated Files (Files will be Moved to the Hard Drive) 311
Uncompress Files Before Backing Up 311

Chapter 8. Managing NetBackup 313
Powering Down and Rebooting NetBackup Servers 314
Managing NetBackup Services 314
NetBackup Request Manager Service 315
NetBackup Database Manager Service 315
NetBackup Device Manager Service 315
NetBackup Volume Manager Service 316
NetBackup Client Service 316
Administering NetBackup Licenses 317
Administering a Remote Master Server 320
Adding a NetBackup Server to a Server List 320
Choosing a Remote Server to Administer 323
If You Cannot Access a Remote Server 323
Using the Remote Administration Console 324
Managing Client Restores 326
Server-Directed Restores 326
Allowing Redirected Restores 326
How NetBackup Enforces Restore Restrictions 326
Allowing All Clients to Perform Redirected Restores 327
Allowing a Single Client to Perform Redirected Restores 328
Allowing Redirected Restores of Specific Client's Files 328
Redirected Restore Examples 329

Improve Search Times by Creating an Image List 333
Configuring NetBackup Ports 334
Server and Client Connections: General Case 336
Backups 336
Restores 340
Using vnetd to Enhance Firewall Protection 344
Multiplexing 347
Multiple Data Streams 347
Configuring Ports for Backups and Restores 349
Configuration Example 350
Administration Client Connections 352
Configuring Ports When Using an Administration Client 355
Configuration Example 356
NetBackup-Java Console Connections 359
Running the NetBackup-Java Console on a UNIX Platform 359
Running the NetBackup-Java Console on a Windows Platform 359
Configuring Ports When Using the NetBackup-Java Console 361
Global Data Manager Connections 364
Configuring Ports When Remotely Administering More than One Master Server . . 366
Configuration Example 367
Load Balancing 368
Adjust Backup Load on Server 369
Adjust Backup Load on Server Only During Specific Time Periods 369
Adjust Backup Load on Client 369
Reduce Time To Back Up Clients 369
Give Preference To a Policy 369
Adjust Load Between Fast and Slow Networks 369
Limit the Backup Load Produced By One or More Clients 370
Maximize Use of Devices 370

Prevent Backups From Monopolizing Devices 370

Chapter 9. Enhanced Authentication and Authorization 371

Common Configuration Elements 372

Configuration Files 372

methods.txt 372

methods_allow.txt 373

methods_deny.txt 374

names_allow.txt 375

names_deny.txt 376

authorize.txt 377

Library Files 378

Commands 378

bpauthorize 379

bpauthsync 379

vopie_util 379

Processes 379

vopied Daemon 379

vopie Files 380

temp File 382

Enhanced Authentication 383

Using vopie Enhanced Authentication 383

vopie Enhanced Authentication Examples 384

Using noauth Rather than vopie Authentication 387

Troubleshooting Authentication 391

Enhanced Authorization 391

Enhanced Authorization Process 391

Gaining Access to a Server 392

Gaining Access to a Client 393

Configuring NetBackup Enhanced Authorization 394

Enabling NetBackup Enhanced Authentication 394
Adding an Authorized User 395
Using the Administrative Console to Specify Preferred Groups (optional) . . 396
Example Configuration 397

Chapter 10. Additional Configuration 401
Multiplexing 402
When to Use Multiplexing 402
How to Configure Multiplexing 403
Maximum Multiplexing Per Drive for Storage Unit 403
Media Multiplexing for a Schedule 403
Other Configuration Settings to Consider Using Multiplexing 406
Demultiplexing 406
Using Multiple NetBackup Servers 408
Dynamic Host Name and IP Addressing 408
Setting up Dynamic IP Addresses and Host Names 410
Configuring the NetBackup Server 411
Configuring a Dynamic Microsoft Windows Client 412
Configuring a Dynamic Macintosh NetBackup Client 413
Configuring a Dynamic UNIX NetBackup Client 413
Bandwidth Limiting 414
Read This First 414
How Bandwidth Limiting Works 415
Configuration 415
Rules for IP Address Ranges 415
Rules for Setting Bandwidth Values 417
Examples 417
Example 1 417
Example 2 418
Example 3 418

Specifying the Locale of the NetBackup Installation 418

Appendix A. NetBackup Commands 421

Appendix B. Reference Topics 629

Rules for Using Host Names in NetBackup 630

Qualifying Host Names 630

How NetBackup Uses Host Names 630

Policy Configuration 630

Image Catalog 631

Error Catalog 631

Scheduler 631

Special Considerations For Domain Name Service (DNS) 631

Factors Affecting Backup Time 633

Total data 633

Transfer rate 633

Device delays 634

Determining NetBackup Transfer Rate 634

Network-Transfer Rate 634

Network-Transfer Plus End-of-Backup-Processing Rate 635

Total-Transfer Rate 635

Examples 635

Using the Performance Monitor 636

How NetBackup Builds Its Automatic-Backup Worklist 637

Building the Worklist (Queue) 638

Prioritizing the Worklist 639

Guidelines for Setting Retention Periods 640

Guidelines for Setting Backup Frequency 640

Determining Backup Media Requirements 641

Incremental Backups Overview 642

Retention Requirements 643

Backup and Restore Times 644
Determining Files Due for Backup on Windows Clients 645
Determining Files Due for Backup on UNIX Clients 646
Storage Management Overview 648
Storage Units 648
Media Manager 649
Retention 649
Volume Pools 650
Media Management Concepts 650
NetBackup and Media Manager Catalogs 650
Volume Database 650
Media Catalog 651
Device Catalogs 651
Media States 652
How NetBackup Selects Media in a Robot 653
Spanning Media 654
How NetBackup Uses Media in Standalone Drives 654
Media Selection Using Standalone Drive Extensions 654
Disabling Standalone Drive Extensions 655
Spanning Media 655
Keeping Standalone Drives in the Ready State 656
Hardware Compression 657
Media Format 657
Non-QIC Tape Format 657
QIC Tape Format 657
Fragmented Backups 658
Spanning Tapes 658
Multiplexing Format 658
Labeling Media 659
Mounting and Unmounting Media 659

Automatic Media Suspend Or Device Down 660
Planning Worksheets 660

Appendix C. UNIX Reference Topics 671
Cross Mount Points 671
Collect True Image Restore Information 671
Exclude and Include Lists on UNIX Clients 674
Creating an Exclude List on a UNIX Client 674
Creating an Include List on a UNIX Client 677
Schedules for User Backups or Archives 678

Appendix D. NetBackup Notify Scripts 679
backup_notify.cmd 680
backup_exit_notify.cmd 680
bpstart_notify (UNIX clients only) 681
bpstart_notify.bat (Microsoft Windows clients only) 683
bpend_notify (UNIX clients only) 685
bpend_notify.bat (Microsoft Windows clients only) 688
dbbackup_notify.cmd 690
diskfull_notify.cmd 690
restore_notify.cmd 691
session_notify.cmd 691
session_start_notify.cmd 692
userreq_notify.cmd 692

Appendix E. Intelligent Disaster Recovery 693
Supported Windows Editions 694
Requirements for IDR 694
Overview of IDR Use 695
About the DR Files 695
Configuring NetBackup Policies for IDR 696

Preparing the IDR Bootable Media 697
Choosing the Bootable Media 697
Creating Bootable Diskettes 698
Creating a Bootable CD Image 701
Updating IDR Media 704
Updating Disaster Recovery Diskettes 704
Updating a Disaster Recovery CD 706
Using drfile.exe To Create or Update a DR File 706
Recovering Your Computer 706
Step 1: Boot Your Computer 707
Step 2: Run Windows NT Setup (applies only to Windows NT) 707
Step 3: Run the Disaster Recovery Wizard 708
Preparing Emergency IDR Bootable Diskettes 712
Notes on Altering Hard Drive Partition Sizes 712
Notes on Recovering Specific Platforms 713
Recovering the Dell PowerEdge 6100/200 with RAID 713
Recovering IBM Computers 714
Recovering Compaq Computers 714
IDR Frequently Asked Questions 714

Appendix F. Using the Backup Exec Tape Reader Option 717

Determining if Your Configuration can Use the Backup Exec Tape Reader Option Effectively 717
Installing the Backup Exec Tape Reader Option 718
Before Upgrading to NetBackup 719
Backup Exec Tape Reader and Typical Backup Exec Installations 719
Backup Exec Tape Reader Option and Complex Backup Exec Installations 720
Backup Exec Tape Reader Option Installation where Backup Exec is Not Present . . 721
Associating Backup Exec Catalogs and Data Files with NetBackup 721
Backup Exec Tape Reader Option Install Examples 722

Uninstalling the Backup Exec Tape Reader Option 723
Converting Backup Exec Catalogs to NetBackup Catalogs 724
How beconv Updates the Media Manager Volume Database 724
Converting All Media 727
Converting Media in a Specific Robot 727
Converting a Single Piece of Media or a Group of Media 728
Using beconv with the -auto_correct Option 729
Using beconv with the Show_mappings Option 730
Using beconv with the -check_consistency Option 730
Importing Uncataloged Backup Exec Media Using NetBackup 732
Making Fresh Backup Exec Media Known to Backup Exec and NetBackup 732
Generating and Converting Backup Exec Catalogs to NetBackup Catalogs 733
Importing Backup Exec Media Belonging to a Spanned Set Where all the Media Belonging to the Spanned Set are Present 733
Importing Backup Exec Media Belonging to a Spanned Set Where all the Media Belonging to the Spanned Set are not Present 734
Updating the Media Manager Volume Database with Respect to Backup Exec Media . 734
When to Run bephyinv 734
How bephyinv Works 734
When bephyinv is Unable to Update the Media Manager Volume Database Correctly 736
Running bephyinv for a Single Piece of Media 737
Examples 737
Browsing Backup Exec Files for Restore 744
Restoring Backup Exec Files 745
Backup Exec Restore Options 747
Access to Restore Target 747
Limitations 747
General Limitations 748
Client Restore Limitations 748

Glossary **749**

Index **777**

About This Guide

This guide describes how to configure and manage the operation of VERITAS NetBackup BusinesServer on a Windows NT or Windows 2000 Server and applies to all supported platforms and operating systems (VERITAS NetBackup is referred to as NetBackup in this guide). See the *NetBackup Release Notes* for a list of the hardware and operating system levels that NetBackup supports.

To determine the version of installed software, check the *install_path*`\NetBackup\Version.txt` file. Where *install_path* is the directory where NetBackup is installed (`C:\Program Files\VERITAS` by default).

Audience

This guide is intended for system administrators and assumes a good working knowledge of the Windows NT or 2000 operating system on the platform where the product is used. In this guide, a system administrator is defined as a person with Windows 2000 or NT system administrator privileges and responsibilities. A client user is anyone that uses the client interfaces to back up, archive, or restore files.

Organization

This guide contains the following chapters:

- Chapter 1, “Introduction to NetBackup,” is an overview of the product. Read this chapter first to get an idea of what NetBackup does and how to set it up.
- Chapter 2, “Managing Storage Units,” explains how to configure NetBackup to use the storage devices in your network.
- Chapter 3, “Managing Backup Policies,” explains how to configure NetBackup policies. A policy defines the backup characteristics for a group of clients that have the same or similar backup requirements.

- Chapter 4, “Using Catalog for Catalog Backups and Verifying, Duplicating, and Importing Images,” explains how to manage and back up the NetBackup internal databases or *catalogs*. NetBackup 4.5 now uses a binary format for new catalogs. Catalogs created in previous releases can be converted from ASCII format to binary using the `cat_convert` catalog conversion utility.

  Catalog is also used to search for specific backup images in order to verify, duplicate, or import a specific backup image.

- Chapter 5, “Viewing NetBackup Reports,” explains how to run reports in order to obtain information about NetBackup activities.
- Chapter 6, “Monitoring NetBackup Activity,” explains how to monitor and control NetBackup jobs, processes, and services.
- Chapter 7, “Configuring Host Properties,” describes the Master Server, Media Servers and Client properties and how to change the settings.
- Chapter 8, “Managing NetBackup,” contains various topics regarding managing NetBackup operations.
- Chapter 9, “Enhanced Authentication and Authorization,” discusses configuring your system to use the enhanced authentication and authorization available in this release.
- Chapter 10, “Additional Configuration,” explains how to configure features and parameters that seldom, if ever, require changing.

In addition to these chapters, there are the following appendices.

- Appendix A, “NetBackup Commands,” explains NetBackup commands that must be run in an MS-DOS window.
- Appendix B, “Reference Topics,” contains useful reference information.
- Appendix C, “UNIX Reference Topics,” provides further information about configuration that applies specifically to UNIX servers and clients.
- Appendix D, “NetBackup Notify Scripts,” provides information about scripts that collect information and provide notification of events.
- Appendix E, “Intelligent Disaster Recovery,” explains how to use Intelligent Disaster Recovery for Windows. This is a separately-priced option for NetBackup BusinesServer.
- Appendix F, “Using the Backup Exec Tape Reader Option,” discusses installing and using the Backup Exec Tape Reader option to read media written by Backup Exec.

Following the appendices is a glossary of terms useful when using and discussing NetBackup.

Related Documents

Other documents that will be useful are listed below. For a complete list of documents pertaining to NetBackup, see the *NetBackup Release Notes*.

- *NetBackup Release Notes*

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

- *NetBackup BusinesServer Getting Started Guide for Windows*

  Gives you the information you need to quickly get Windows NT NetBackup server software installed and running.

- *NetBackup Installation Guide - PC Clients*

  Gives you the information you need to quickly get NetBackup PC client software installed and running on the clients.

- *NetBackup BusinesServer Media Manager System Administrator's Guide for Windows*

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

- *NetBackup User's Guide - Microsoft Windows*

  Explains how to configure, and use NetBackup to perform backups, archives, and restores from Microsoft Windows NT/2000, 98, and 95 clients.

- *NetBackup Troubleshooting Guide for Windows*

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

Accessibility

NetBackup contains features that make its graphical user interface (GUI) usable by people who are vision impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input
- Using the keyboard to navigate the NetBackup application
- Online documentation

Support for Assistive Technology

Text that appears in the NetBackup application interface is accessible through an application programmer's interface (API) to assistive technologies such as voice or assistive device input products and to speech output products.

Using the Keyboard to Navigate in NetBackup

You can use your keyboard to navigate the NetBackup application:

- Move from one window element to another using window navigation keys. Using the **TAB** key to move from one pane to another is an example of a window navigation key. For more information, see "Navigating in a NetBackup Tree View."
- Perform common actions quickly using accelerator keys. Accelerator keys allow you to perform an action without first accessing the menu. For example, simply enter **CTRL+N** to create a new policy. For more information, see "Accelerator Keys."
- Mnemonic keys are indicated by an underlined letter and allow you to select items using only the keyboard. For example, enter **Alt+h** to access the help menu in NetBackup. For more information, see "Mnemonic Keys."

  Mnemonic keys are indicated by an underlined letter.
- You can also use the keyboard to select control elements in a dialog. For more information, see "Using the Keyboard in Dialogs."

Navigating in a NetBackup Tree View

Use the following keys or key combinations to navigate through the NetBackup Console window.

Keyboard Input	Result
TAB or **F6**	Move forward between panes in the active NetBackup Console window.
SHIFT+TAB or **SHIFT+F6**	Move backwards between panes in the active NetBackup Console window.
CTRL+TAB or **CTRL+F6**	Move forward between NetBackup Console windows.
CTRL+SHIFT+TAB or **CTRL+SHIFT+F6**	Move backwards between NetBackup Console windows.

Keyboard Input	Result
PLUS SIGN (**+**) on the numeric keypad	Expand the highlighted item.
MINUS SIGN (**-**) on the numeric keypad	Collapse the highlighted item.
Asterisk (*****) on the numeric keypad	Expand the entire tree below the first item in the active NetBackup Console window.
UP ARROW	Gives focus to the next item up in the pane.
DOWN ARROW	Gives focus to the next item down in the pane.
SHIFT+UP ARROW	Select the next item up in the pane.
SHIFT+DOWN ARROW	Select the next item down in the pane.
PAGE UP	Move to the top item visible in a pane.
PAGE DOWN	Move to the bottom item visible in a pane.
HOME	Move to the first item in a pane.
END	Move to the last item in a pane.
RIGHT ARROW	Expand the highlighted item. If the highlighted item does not contain hidden items, behaves like DOWN ARROW.
LEFT ARROW	Collapse the highlighted item. If the highlighted item does not contain expanded items, behaves like UP ARROW.
ALT+RIGHT ARROW	Move to the next item.
ALT+LEFT ARROW	Move to the previous item.
ALT+SPACEBAR	Display the NetBackup Console window menu.

Keyboard Input	Result
PLUS SIGN (**+**) on the numeric keypad	Expand the highlighted item.
MINUS SIGN (**-**) on the numeric keypad	Collapse the highlighted item.
Asterisk (*****) on the numeric keypad	Expand the entire tree below the first item in the active NetBackup Console window.
UP ARROW	Gives focus to the next item up in the pane.
DOWN ARROW	Gives focus to the next item down in the pane.
SHIFT+UP ARROW	Select the next item up in the pane.
SHIFT+DOWN ARROW	Select the next item down in the pane.
PAGE UP	Move to the top item visible in a pane.
PAGE DOWN	Move to the bottom item visible in a pane.
HOME	Move to the first item in a pane.
END	Move to the last item in a pane.
RIGHT ARROW	Expand the highlighted item. If the highlighted item does not contain hidden items, behaves like DOWN ARROW.
LEFT ARROW	Collapse the highlighted item. If the highlighted item does not contain expanded items, behaves like UP ARROW.
ALT+RIGHT ARROW	Move to the next item.
ALT+LEFT ARROW	Move to the previous item.
ALT+SPACEBAR	Display the NetBackup Console window menu.

Accelerator Keys

Accelerator keys allow you to use NetBackup from the keyboard, rather than using the mouse. Accelerators are used to perform common actions quickly. Accelerator keys are either a single keystroke or two or more keystrokes that can be pressed in succession (rather than holding them simultaneously). If available, accelerator keys are shown to the right of the menu item they perform.

For example, to find an file, enter **CTRL+F**.

Mnemonic Keys

A mnemonic is a keyboard equivalent for a mouse click that is used to activate a component such as a menu item. A mnemonic can be used to select a menu item by pressing the **<Alt>** key to go into menu pull-down mode, pressing a single key to open a menu and another key to select a menu item.

Example: **<Alt>** to go into menu pull-down mode, **<a>** key to access the Actions menu and **<m>** to activate the Change Master Server command. Mnemonics are case insensitive. Keys can be pressed sequentially instead of simultaneously.

Using the Keyboard in Dialogs

Select or choose controls that have an underlined letter in their titles by typing **ALT+** the underlined letter at any time when the dialog is active. Use the **TAB** key to move forward between controls. Add the **SHIFT** key to reverse the direction. Use the arrow keys to move within a list box, groups of option controls, or groups of page tabs. Options that are unavailable appear dimmed and cannot be selected.

The following conventions are typically used in NetBackup dialogs:

- Command buttons (also known as push buttons)

  Command buttons initiate an immediate action. One command button in each dialog box carries out the command you've chosen, using the information supplied in the dialog. This normally is labeled **OK**. Other command buttons let you cancel the command or choose from additional options.

- Command buttons marked with an ellipsis (...)

  Command buttons marked with an ellipsis (...) open another dialog so you can provide more information or confirm an action. Command buttons marked with an arrow display a menu.

- Command buttons marked with a dark border

  A dark border initially indicates the default button. Press **ENTER** at any time to choose the button with a dark border. Use **TAB** to move the keyboard focus to the next control. When you move to a command button it temporarily takes the dark border,

but when the keyboard focus is not on a command button the dark border returns to the default button. Press **SPACEBAR** to choose the command button you selected with **TAB**. Use **ESC** to immediately choose the Cancel button if there is one.

- Check boxes

  Check boxes may be selected or cleared to turn an option on or off. Check boxes may have two states (checked and unchecked) or three states (checked, unchecked, and indeterminate).

  Use **TAB** to move between boxes and **SPACE** to change the check box to the next state. Typing the mnemonic key for a check box also will move the focus to the box and change its state.

- Option controls (also known as radio buttons)

  Option controls are used to select only one option from a group of options. (Like check boxes, option buttons may represent two or three states.) Use the arrow keys to select the next or previous buttons within the group. Typing the mnemonic key for an option control moves the focus to the control and selects it.

- Tabbed pages

  Tabbed pages are used to fit many options into a single dialog. Each page contains separate groups of controls such as check boxes or option controls. Use **TAB** to move the focus to the tab for the currently visible page. Type the mnemonic key for a page tab to move the focus to the tab and display its page.

Online Documentation

In addition to online help, NetBackup provides copies of related NetBackup manuals in Adobe Portable Document Format (PDF) on the NetBackup CD-ROM. For a complete list of NetBackup documents see the *NetBackup Release Notes*.

Conventions

The following explains typographical and other conventions used in this guide.

Type Style

Typographic Conventions

Typeface	Usage
`Bold fixed width`	Input. For example, type **`cd`** to change directories.
`Fixed width`	Paths, commands, filenames, or output. For example: The default installation directory is `/opt/VRTSxx`.
Italics	Book titles, new terms, or used for emphasis. For example: *Do not* ignore cautions.
Sans serif (italics)	Placeholder text or variables. For example: Replace *filename* with the name of your file.
Serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the **Password** field.

Notes and Cautions

Note This is a Note. Notes are used to call attention to information that makes using the product easier or helps in avoiding problems.

Caution This is a Caution. Cautions are used to warn about situations that could cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, holding down the **Ctrl** key while pressing another key. Keyboard command sequences are indicated by connecting the keys with a plus sign. For example:

Press Ctrl+t

Command Usage

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

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

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

`command` *arg1* | *arg2*

the user can use either the *arg1* or *arg2* variable.

Terms

The terms listed in the table below are used in the VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

Term	Definition
Microsoft Windows, Windows	Terms used as nouns to describe a line of operating systems developed by Microsoft, Inc. A term used as an adjective to describe a specific product or noun. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI. Where a specific Windows product is identified, then only that particular product is valid with regards to the instance in which it is being used. For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`.
Windows servers	A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and Windows 2000.
Windows clients	A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE.

Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

`http://www.support.veritas.com/`

VERITAS Customer Support has an extensive technical support structure that enables you to contact technical support teams that are trained to answer questions to specific products. You can contact Customer Support by sending an e-mail to support@veritas.com, or by finding a product-specific phone number from the VERITAS support web site. The following steps describe how to locate the proper phone number.

1. Open `http://www.support.veritas.com/` in your web browser.
2. Click **Contact Support**. The *Contacting Support Product List* page appears.
3. Select a product line and then a product from the lists that appear. The page will refresh with a list of technical support phone numbers that are specific to the product you just selected.

Introduction to NetBackup 1

This chapter provides an introduction to NetBackup and contains the following topics:

- Overview
- Using the NetBackup Administration Console
- Configuring NetBackup Without Wizards

Overview

NetBackup provides high-performance backups and restores for a variety of computer types, including Microsoft Windows, NetWare, IBM, UNIX, and Macintosh.

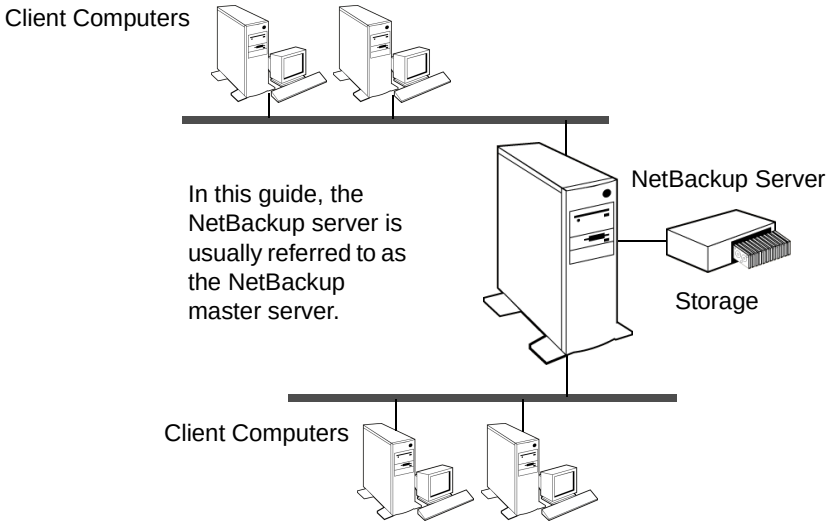
Administrators can set up schedules for automatic, unattended backups for clients anywhere in the network. These backups can be full or incremental and are managed entirely by the NetBackup server (also referred to as the NetBackup master server).

Users can start backups and restores from the computer where they are working. A user can also archive files. An archive operation backs up a file and then deletes it from the local disk if the backup is successful. Once started, user operations are managed by the NetBackup server.

NetBackup's Media Manager software manages the media and storage devices. Robots require no intervention on the part of the administrator, operator, or the user. Standalone drives (those not in a robot) that contain appropriate media also require no intervention.

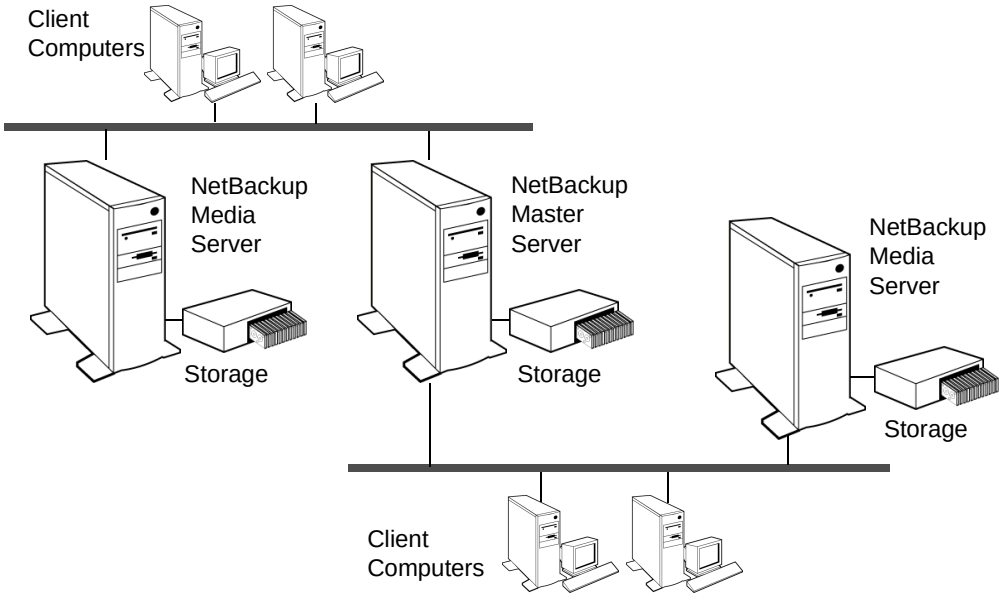
NetBackup includes both the server and client software:

- Server software is on the computer that manages the storage devices.
- Client software is on the computer whose data you want to back up. A server also has client software and can be backed up like other clients.



NetBackup servers and clients can be any one of a number of computer types as described in the data sheets and release notes for the product.

NetBackup supports both master and media servers. The master server manages the backups, archives, and restores. Media servers provide additional storage by allowing NetBackup to use the storage devices that they control. Media servers can also increase performance by distributing the network load.



During a backup or archive, the client sends backup data across the network to a NetBackup server that has the type of storage specified for the client. The storage requirement is specified during NetBackup configuration (for example, 4 mm tape).

During a restore, users can browse and then select the files and directories that they want to recover. NetBackup finds the selected files and directories and restores them to the disk on the client.

Using the NetBackup Administration Console

The NetBackup Administration Console provides a Windows-based interface through which the administrator can manage NetBackup.

▼ To start the NetBackup Administration Console

1. Log on to the Windows workstation as a member of the user group authorized for NetBackup administration.

2. Go to **Programs** > **VERITAS NetBackup** > **NetBackup Administration Console**. The NetBackup Administration Console appears.

The NetBackup Administration Console is the starting point for administering NetBackup. The left pane in the console contains a node for each major area of NetBackup administration. Clicking a node displays information related to that node in the right pane. The menus contain commands relevant to the selected node.

Note If there is more than one NetBackup server, it is possible to run the NetBackup Administration Console on more than one server at a time. However, if more than one person is making changes to the configuration, the results will be unpredictable.

Master Server

The information in the NetBackup Administration Console applies to this server only.

Activity Monitor

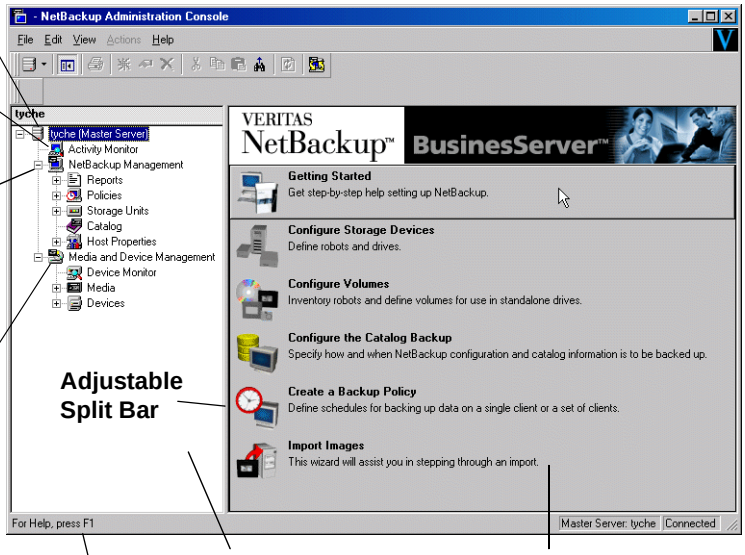
Displays information about NetBackup jobs and provides some control over the jobs.

NetBackup Management

Contains utilities for creating and viewing reports, for configuring policies, storage units, catalog backups, and a utility for configuring master server, media server, and client properties.

Media and Device Management

Contains utilities for managing the media and devices that NetBackup uses to store backups. (See the *NetBackup Media Manager System Administrator's Guide*.)



Adjustable Split Bar

Tree View

Consists of utilities.

Details Pane

Contains configuration wizards and details specific to the utility selected.

Tooltips

Turn on under **View** > **Customize** utilities.

In addition to the NetBackup Administration Console, there are some operations that can be performed by entering commands in an MS–DOS window. The commands are explained in Appendix A.

The following sections describe the utilities and menus that appear in the NetBackup Administration Console.

User Backups, Archives, and Restores

Use **Backup, Archive, and Restore** to perform backups and archives for this client, and restores for this and other clients.

Users can back up, archive, and restore files, directories, and raw partitions that reside on their own client computer. A user can restore files at any time but can back up and archive only during the time periods that the administrator defines with the schedules. Users can also view the progress and final status of the operations they perform.

Note An archive is a special type of backup. During an archive, NetBackup first backs up the selected files then deletes them from the local disk if the backup is successful. In this manual, references to backups also apply to the backup portion of archive operations (except where otherwise noted).

Activity Monitor

Use the Activity Monitor to monitor and control NetBackup jobs, services, processes, and drives.

NetBackup Management

This manual describes the items listed under **NetBackup Management** in the NetBackup Administration Console tree.

Reports

Use **Reports** to compile information for verifying, managing, and troubleshooting NetBackup operations.

For more information see Chapter 5, “Viewing NetBackup Reports” on page 191.

Policies

Use **Policies** to create and specify the backup policies which define the rules for backing up a specific group of one or more clients. For example, the backup policy specifies when automatic backups will occur for the clients and when users can perform their own backups. The administrator can define any number of backup policies, each of which can apply to one or more clients. A NetBackup client must be covered by at least one backup policy and can be covered by more than one.

The properties of a backup policy include:

- General attributes that define the:
  - *Priority* of backups for this policy relative to backups for other policies.
  - *Storage unit* to use for backups of clients covered by this policy.

- *Volume pool* to use for backups performed according to this policy. A volume pool is a set of volumes that the administrator can assign to specific backup policies or schedules. For example, it is possible to have one volume pool for weekly backups and another for quarterly backups.

- List of client computers covered by the policy.
- List of files to include in automatic backups of the clients. It is also possible to specify a list of files to exclude from automatic backups. The file list or exclude list does not affect user backups because the user selects the files.
- Schedules that control when backups and archives can occur for the clients.

As mentioned above, each backup policy has its own set of schedules. These schedules control when automatic backups start and also when users can start a backup or archive. Each schedule is unique with attributes that include:

- Type of schedule. Specify schedules for automatic full or incremental backups or user backups or archives. There are also schedule types that apply only when separately-priced options are installed (for example, a backup schedule for Microsoft Exchange or Oracle databases).
- Backup window. For automatic full or incremental backup schedules, this is the time period when NetBackup can start automatic backups of clients covered by this policy. For user schedules, this is the time period when users can start a backup or archive of their own client.
- Frequency. How often automatic backups can occur.
- Retention. How long NetBackup keeps the data that is backed up by this schedule.
- Storage unit. The storage unit for the data that is backed up by this schedule. This setting, if used, overrides the storage unit specified at the backup policy level.
- Volume pool. The volume pool to use when saving data backed up by this schedule. This setting, if used, overrides the volume pool specified at the backup policy level.

The administrator can also manually start a backup schedule for an automatic full or incremental backup. Manual backups are useful if, for example, a client system is down and misses its scheduled backup.

Storage Units

Use **Storage Units** to display storage unit information and provide commands for managing NetBackup storage units.

The devices that Net Backup uses to store backups are called storage units. A storage unit is a group of one or more storage devices of a specific type and density that attach to a NetBackup server. The media can be removable (such as tape) or a directory on a hard disk. Removable media can be in a robot or a standalone drive.

The devices in a removable-media storage unit (such as a tape drive) must attach to a NetBackup master or media server and be under control of Media Manager. The administrator first sets up Media Manager to use the drives, robots, and media and then defines the storage units. During a backup, NetBackup sends data to the storage unit specified by the backup policy. Media Manager then picks an available device within the storage unit.

When the storage unit is a directory on a hard disk, the administrator specifies the directory during configuration and NetBackup sends the data to that directory during backups. Media Manager is not involved.

Storage units simplify administration because once they are defined, the NetBackup configuration points to a storage unit rather than to the individual devices it contains. For example, if a storage unit contains two drives and one is busy, NetBackup can use the other drive without administrator intervention.

For more information see Chapter 2, “Maintaining Storage Units” on page 27.

Volumes

The removable media on which NetBackup stores data are called volumes. These media (for example, 4 mm cartridge tapes) have been assigned media IDs and other attributes so their content, location, and usage can be tracked. The attribute assignment occurs when the administrator adds media to Media Manager and can be done automatically or manually. The system administrator’s guide for Media Manager explains how to add volumes.

NetBackup master servers keep a media catalog with records about the volumes where backups are stored. Media Manager controls the mounting of volumes on the devices and keeps a volume database with records that indicate where the volumes are located once assigned to a Media Server.

Note When the storage unit is on magnetic disk, volumes are not specified. NetBackup sends the backup to the file path specified during setup of the storage unit and records the location in the NetBackup media catalog. The operating system manages the actual writing of data.

Catalog

Use **Catalog** to create and configure a special type of backup NetBackup requires for its own internal databases. These databases, called catalogs, are on the NetBackup server's disk and have setup information as well as critical information on client backups. The catalog backups are set up and tracked separately from other backups to ensure recovery in case of a server crash.

Catalog is also used to search for a backup image in order to verify the contents of media with what is recorded in the NetBackup catalog, to duplicate a backup image, to promote a backup image from a copy to the primary backup copy, to expire backup images, or to import expired backup images or images from another NetBackup server.

For more information see Chapter 4, “Using Catalog for Catalog Backups and Verifying, Duplicating, and Importing Images.”

Host Properties

Use **Host Properties** and its subnodes to customize NetBackup configuration options. In most instances, no setting changes are necessary. However, **Host Properties** settings allow the administrator to customize NetBackup to meet specific site preferences and requirements for master server, media servers, and clients.

All configuration options are described in Chapter 7, “Configuring Host Properties” on page 237.

Media Manager

The software that manages the removable media and storage devices for NetBackup is called Media Manager. This software is part of NetBackup and is installed on every NetBackup server. The administrator can configure and manage media through the NetBackup Administration Console.

The *NetBackup Media Manager System Administrator’s Guide* contains information on Media Manager.

NetBackup Configuration Wizards

The easiest way to configure NetBackup is to use the configuration wizards. The wizard selection visible in the Results pane varies depending on what is selected in the left portion of the screen.

Getting Started

Use the **Getting Started Wizard** if you are configuring NetBackup for the first time. It leads you through the necessary steps and other wizards to get you up and running with a working NetBackup configuration.

Configure Storage Devices

Use the **Device Configuration Wizard** to guide you through the entire process of configuring a device and storage unit.

Configure Volumes

Use the **Volume Configuration Wizard** to guide you through the entire process of configuring removable media.

Configure the Catalog Backup

Use the **NetBackup Catalog Backup Wizard** to set up your catalog backups, which are essential to recovering your data in case of a failure.

Create a Backup Policy

Use the **Backup Policy and Configuration Wizard** to add a backup policy to your configuration.

Import Wizard

Use the **Import Wizard** to import NetBackup images in a two-part process.

Configure a Shared Drive

Use the **Configure Shared Drive Wizard** to configure NetBackup to use a new shared drive or to reconfigure an existing shared drive.

Menus

The following sections describe menus in the NetBackup Administration Console.

File Menu

- **Change Server:** Use to display the configuration for another NetBackup master server. The name of the current server appears in the status bar.
- **New Console:** Opens a new NetBackup Administration Console.
- **New Window from Here:** Opens another window in addition to those that are already open. If you are currently in Activity Monitor and select **New Window From Here**, the new window will open to Activity Monitor.

- **Backup, Archive, and Restore:** Opens the client interface, Backup, Archive, and Restore for the selected server.
- **MS SQL Client:** Shortcut to access the SQL server NetBackup client if it is installed on the selected host.
- **Print Setup:** Displays a dialog to enter printer specifications.
- **Print:** Displays a dialog where you can enter the specifications for printing a report. You can specify the range of pages to be printed, the number of copies, the destination printer, and other printer setup options.
- **Send:** Sends the active document through electronic mail. This command displays a mail window with the active document attached to it. Click the **Send** button to send the message.
- **Export:** Displays a dialog in which to specify a file to save the configuration properties of the selected clients or servers.
- **Close Window:** If more than one NetBackup window is open, **Close Window** closes only the current window. You will not exit NetBackup. If only one NetBackup window is open, you will exit NetBackup.
- **Exit:** Closes the NetBackup application and all NetBackup Administration Consoles or windows opened through NetBackup.

Edit Menu

- **Undo:** Reverses the last editing action, if possible.
- **Cut:** Deletes the selected items and places them on the clipboard. This command is unavailable only when something is selected.
- **Copy:** Copies selected items to the clipboard.
- **Paste:** Pastes the contents of the clipboard into the selected policy attributes, client list, file list, or schedule.
- **New:** Displays a dialog where you can specify criteria for a new policy, schedule, client, or file.
- **Change:** Displays a dialog where you can specify changes to the selected policy attributes, client, file, or schedule.
- **Delete:** Deletes the selected policy, client, file, or schedule.

- **Find:** Opens the Find dialog where you can specify criteria for finding an item in a list in the window. Press **Help** for instructions. For information on using the Find dialog, click **Help**.

- **Find Next:** Finds the next line in the list that matches the search criteria.
- **Find Previous:** Finds the line that was found during the preceding search.
- **Find All:** Finds all lines that match the specified search criteria.

View Menu

- **Toolbar:** Displays or hides the standard NetBackup toolbar.
- **Status Bar:** Displays or hides the status bar that appears at the bottom of the window.
- **Tree:** Displays or hides the nodes in the left pane of the NetBackup Administration Console.
- **Previous Pane:** Returns to previously selected dialogs, moving backwards.
- **Next Pane:** Returns to previously selected dialogs, moving forwards.
- **Customize:** Displays the Customize dialog to customize the toolbars and set other display preferences.
- **Options:** Use to customize NetBackup utilities in the Options dialog.
- **Refresh:** Updates the detail pane with new information retrieved from the master server(s).
- **Refresh All:** Updates all open windows.
- **Large Icons:** Displays large icons in the lists.
- **Small Icons:** Displays small icons in the list.
- **List:** List items without details.
- **Details:** Display details about each item in the list.
- **Columns:** Opens a submenu that contains commands for changing the order and size of columns:

- **Layout:** Displays a dialog with controls for changing the order and format of each column.
- **Even Size:** Makes each column the same width.
- **Proportional Size:** Keeps column widths in the same relative proportions if you change the window size.
- **Fixed Size:** Makes each column a fixed size according to your settings.
- **Size to Data:** Adjusts the width of each column according to how much data it contains.

◆ **Sort:** Displays a dialog to specify criteria for sorting lists in the window.

Actions Menu

The menu items that appear differ depending upon what utility is selected in the tree view.

Help Menu

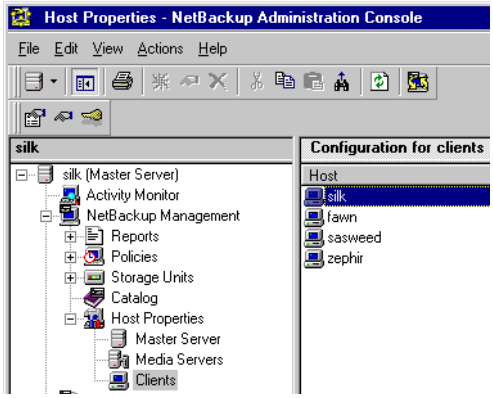
◆ **Help Topics:** Provides online help information.

◆ **VERITAS Web Page:** Displays the VERITAS web page if the system has a browser configured.

◆ **License Keys:** Opens a dialog where you can view and modify the license keys for the local computer.

◆ **About Administration Console:** Displays program information, version number, and copyright.

Standard and User Toolbars



Upon opening the NetBackup Administration Console, a standard toolbar appears by default.

When certain utilities are selected, **Policies** or **Reports**, for example, a second toolbar, called a user toolbar, appears.

The buttons on the toolbars provide shortcuts for menu commands. Slowly drag the pointer over a button to display a button description label.

To display or hide the standard NetBackup toolbar, click **View** > **Toolbar**.

Select **View** > **Customize** > **Toolbars** > **User** to display or hide the user toolbar.

Customizing the Administration Console

The **View** menu has options for customizing the window to suit your preferences. For example, the **Customize** command opens a dialog with options for adding more toolbars or adding buttons to existing toolbars. See the online help for more information on **Customize**, **Options**, and other commands on the **View** menu.

Shortcut Menus

Clicking the right mouse button when the pointer is over a pane in the window, displays a popup menu with commands that apply to what is currently selected.

Status Bar

The status bar appears at the bottom of the window. You can choose whether to display it by clicking **Status Bar** on the **View** menu. When Tooltips are enabled, the left side of the status bar shows help messages when the pointer is over a toolbar button or menu command. The right side of the status bar indicates the master server where you are managing policies.

To enable tool tips, click **View** > **Customize**. On the Toolbars tab, select **Show Tooltips**.

Configuring NetBackup Without Wizards

The easiest way to configure NetBackup is to use the configuration wizards provided.

If you are configuring NetBackup for the first time, choose the Getting Started Wizard. This wizard steps you through the other wizards and leaves you with a working NetBackup configuration. You can also run a test backup. This wizard starts automatically after installation is complete and you can start it again later through NetBackup Assistant.

If you prefer not to use the available wizards, the following steps explain how to configure NetBackup by using the NetBackup Administration Console. Complete instructions are not given here, but each step provides references for more information if you require it.

1. Start the NetBackup Administration Console if it is not already started.

2. Complete the addition of storage devices.

   The Device configuration wizard is the preferred way to do this. To perform configuration without using the wizard, see the *Media Manager System Administrator's Guide*.

3. Define the media that you will use.

   For instructions, see the *Media Manager System Administrator's Guide*.

4. Ensure that the NetBackup Database Manager service is active.

   This service must be running so that NetBackup can update its catalogs with the new setup information.

   You can start and stop this service through the NetBackup Activity Monitor or by using the Services application on the Windows NT Control Panel. We suggest that you configure all NetBackup services so they start automatically each time you start the server.

5. Set up the NetBackup storage units that will contain the storage devices that NetBackup will use to store its backups.

6. Verify the NetBackup catalog backup configuration. The NetBackup catalogs are on the server's disk and have configuration information as well as critical information on client backups.

   a. Specify the media to use.

   b. Make any necessary changes to the backup paths. The default paths to the catalogs are added automatically.

7. Set up the backup policies for the clients that you are backing up.

8. Changing the NetBackup host properties if the defaults are not appropriate for your environment.

9. Start the NetBackup Request Manager service.

   You can start and stop this service through the NetBackup activity monitor or by using the Services application on the Windows NT Control Panel. It is recommended that you configure all NetBackup services so they start automatically each time you start the master server.

   The configuration is now complete. Test it as follows:

   a. If you created user-directed backup or archive schedules, test them by performing a backup or archive from a client. Check the log on the client to see if the operations were successful. If the backup was successful, restore the same files. This verifies the basic backup and restore capabilities.

      For instructions on performing user-directed operations, start the NetBackup user interface on the client and follow the instructions that are given in the user's guide or the online help.

   b. To test the automatic backup schedules, you can either wait until they are due or run them manually from the master server. After the automatic schedules have run, check the Backup Status report to ensure that the backups completed successfully for all clients.

10. Perform any required additional configuration.

NetBackup Online Help

NetBackup provides help for all its windows and dialogs. If you are familiar with Windows help, you will find it easy to use NetBackup help. The following explains the main features of the help system.

Finding a Topic

The NetBackup Administration Help Topics window provides a path to all available help topics. You can display this window from any of the NetBackup windows by clicking **Help**. In dialogs, click **Help** to get help on the items within the dialog. If the dialog help is not what you need, click **Help Topics** at the top of the help window.

The Help Topics window has three tabs:

- **Contents** tab where you can browse through the list of available topics to find the one you want.
- **Index** tab where you can either type an index term or browse the list.
- **Find** tab where you can search for words and phrases.

Using Context-Sensitive Help

- F1 key

In most NetBackup Windows and dialogs, you can click or tab to an item and then press F1 to display help specific to the item.

- **?**

If a dialog has a **?** in the title bar, click **?** then the item to display help specific to the item.

- Help button

Dialogs usually have a Help button that displays help information specific to the dialog.

Printing Help

To print a help topic, click **File** > **Print Topic**.

To print the help that is in a popup help window, click the right mouse button while the pointer is in the popup, then click **Print Topic** on the popup menu.

To print a group of related topics, select a book on the Contents tab of the Help Topics window and click **Print**.

Changing Fonts

To change the size of the display font, click **Options** > **Font** > **Small**, **Normal**, or **Large**.

Using Tooltips

The tooltips feature gives you quick help on toolbar buttons and menu commands. When tooltips are enabled in a window popup help appears whenever you position the pointer over a toolbar button or menu command. The left side of the status bar at the bottom of the window also shows a brief explanation.

To enable tooltips, click **View** > **Customize** > **Toolbars** > **Show Tooltips**.

To display the status bar, click **View** > **Status Bar**.

Using Other Help Features

- Jumps to other topics

Clicking text that is underlined with a solid line takes you to another topic.

- Popup topics

Clicking text that is underlined with a broken line always displays a popup that contains a brief topic or definition of a term.

- Back button

Click **Back** to go to the last topic that was displayed in this window.

- Close button

Most windows will close automatically when you go to another topic. Some however are for reference and will remain open. Click **Close** in these windows.

Getting Help While Working in NetBackup Optional Products

Use NetBackup online help to get immediate answers to your questions about particular fields, dialogs, windows and views. To access help for optional products, click **Help** (if available) or select help for the product from the NetBackup Help menu.

Online Documents

This product includes online documentation in Adobe® Portable Document Format (PDF) format that can be optionally installed on your computer. To view PDF documents, you must use the Adobe Acrobat Reader. You can download the reader from:

`http://www.adobe.com`

Note that VERITAS assumes no responsibility for the installation and use of the reader.

To view a document, click it in the list below.

Note If a `Cannot find or run the file or program` message appears and the Adobe Acrobat Reader is working properly, it means the document is not installed on your computer.

- *NetBackup Release Notes*

Provides important information about NetBackup server software, such as the platforms and operating systems that are supported and operating notes that may not be in the manuals or the on-line help.

- *NetBackup Installation Guide for PC Clients*

  Gives you the information you need to quickly get NetBackup PC client software installed and running. The PC clients are Windows 2000, Windows NT, Windows 95, Macintosh, IBM OS/2 Warp, and Novell NetWare. This is the first document that you should read after opening the NetBackup PC Client package.

- *NetBackup User's Guide for Microsoft Windows*

  Explains how to use NetBackup on a Windows 2000, NT, 98, or Windows 95 client to perform backups, archives, and restores. This guide also contains some configuration instructions for the NetBackup client software.

- *NetBackup User's Guide for Novell NetWare NonTarget*

  Explains how to use NetBackup NonTarget software on a Novell NetWare server to perform backups and restores. The NonTarget version of NetBackup has a Microsoft Windows interface. This guide also contains some configuration instructions for the NetBackup client software.

- *NetBackup User's Guide for Novell NetWare Target*

  Explains how to use NetBackup target software on a Novell NetWare server to perform backups and restores. The target version of NetBackup has a menu driven interface that runs under DOS. This guide also contains some configuration instructions for the NetBackup client software.

- *NetBackup User's Guide for Mac OS*

  Explains how to use NetBackup on a Macintosh client to perform backups, archives, and restores. This guide also contains some configuration instructions for the NetBackup client software.

- *NetBackup User's Guide - IBM OS/2 Warp*

  Explains how to use NetBackup on an IBM OS/2 Warp client to perform backups and restores. This guide also contains some configuration instructions for the NetBackup client software.

- *NetBackup Troubleshooting Guide for Windows*

  Provides troubleshooting information for configurations where the master server is running NetBackup for Windows Server.

For a complete list of technical documents related to NetBackup, see the Related Documents appendix in the *NetBackup Release Notes*.

Installing the Documents

If the PDF documents were not installed during NetBackup installation, copy them from the `Doc` folder on the NetBackup CD-ROM to:

install_path`\Help\`

Where *install_path* is the folder where you installed the NetBackup software and by default is

`C:\Program Files\VERITAS`

Managing Storage Units 2

The following topics provide useful information for configuring storage units:

- Introduction to Storage Units
- Using the Device Configuration Wizard
- Storage Unit Considerations
- Maintaining Storage Units
- Storage Unit Properties
- Configuring Drive Availability Checking

Introduction to Storage Units

A NetBackup storage unit is a group of one or more storage devices of a specific type and density that attach to a NetBackup server. During a backup or archive, NetBackup stores the backup data on the storage units that you have set up during configuration. You can set up three types of storage units:

- Media Manager

  A Media Manager storage unit uses tape robots, standalone tape drives, or optical disk devices, that are under control of Media Manager. Media Manager controls the allocation and mounting of media (called volumes) in the storage devices.

- Disk

  A disk type storage unit consists of a directory on a hard disk that stores the backup or archive data. NetBackup permits an unlimited number of disk storage units.

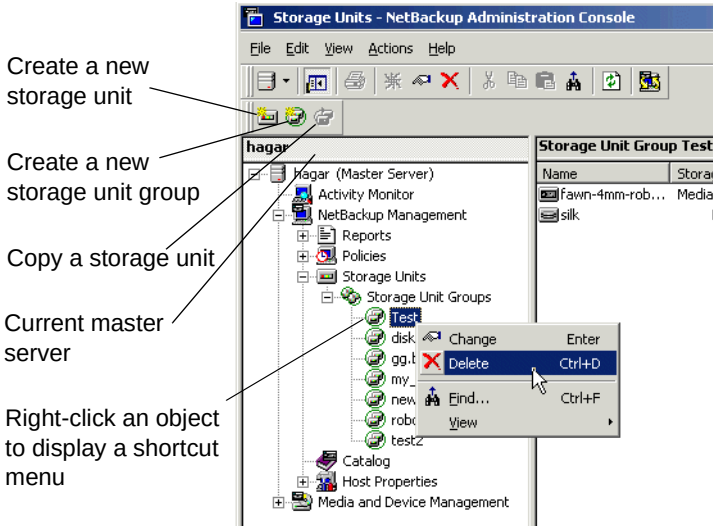
- NDMP

  NDMP storage units are controlled by Media Manager but attach to NDMP hosts and require that you have the NetBackup for NDMP option installed.

Viewing Storage Units and Storage Unit Groups

In the NetBackup Administration Console, select **Master Server > NetBackup Management > Storage Units** to display all the storage units for the selected server. All storage units for the selected server display in the right pane, whether or not the unit is in a storage unit group.

Expand or select **Storage Units > Storage Unit Groups** to display all the storage unit groups created for the selected server.



Select a storage unit group in the left pane to display all the storage units in the group.

To display storage units and storage unit groups for another NetBackup master server, see “ Administering a Remote Master Server” on page 320.

Using the Device Configuration Wizard

The easiest way to configure storage units for the first time is to use the Device Configuration Wizard. This wizard guides you through the entire process, simplifying it by automatically choosing settings that are good for most configurations.

If you are modifying an existing configuration or want access to more settings, see "Maintaining Storage Units" on page 27.

▼ **To use the Device Configuration Wizard**

1. In the NetBackup Administration Console, select **Master Server** or **Media and Device Management**.

2. From the list of wizards in the right pane, click **Configure Storage Devices** and follow the wizard instructions.

Note The wizard will add only one hard disk storage unit if no devices are found.

Storage Unit Considerations

There are three storage types. Each has specific considerations.

Media Manager Storage Unit Considerations

1. NetBackup BusinesServer permits one or two Media Manager storage units:
   - There can be a combined total of two drives in both the storage units.
   - There can be only one robot.

2. Add the storage unit to the server where the drives attach. For a robot on NetBackup BusinesServer, the robotic control must also attach to that server.

3. The number of storage units that you must create for a robot depends on the robot's drive configuration as follows:
   - Drives with the same density on the same media server must be in the same storage unit. For example, if a robot has two drives of the same density on the same media server, add only a single storage unit for the robot. Set the **Maximum Concurrent Drives Used for Backup** setting to 2.

- Drives on different media servers must be in separate storage units.
- Drives with different densities must be in separate storage units. For example, an STK 9710 library configured in Media Manager as a Tape Library DLT (TLD) can have both half-inch cartridge and DLT drives. Here, you must define a separate storage unit for each density.

4. Standalone drives with the same density must be in the same storage unit.

   For example, if a server has two 1/4-inch qscsi drives, add a storage unit with **Maximum Concurrent Drives Used for Backup** set to 2. Media Manager chooses the drive to use when NetBackup sends a backup to this storage unit.

5. Standalone drives with different densities must be in different storage units.

6. A robot and a standalone drive cannot be in the same storage unit.

Before Adding a Media Manager Storage Unit

Before adding a Media Manager storage unit, set up Media Manager to recognize the devices that will be in the storage units. (For device configuration information, see the *Media Manager System Administrator's Guide.*)

As you set up the devices, record the following information from the Media Manager configuration:

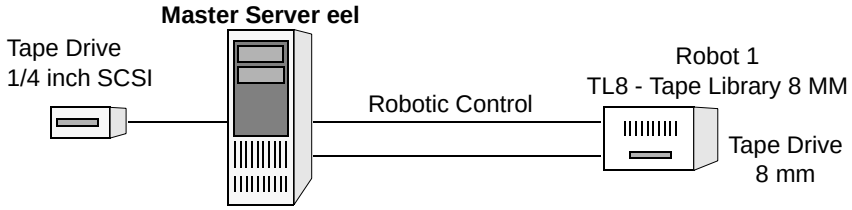
Type of Tape Device	Record the Following Information
Robots	- Robot type - Robot number in Media Manager - Media density for the drives in each robot
Standalone tape drives	- Media density of each drive - How many drives of each media density are on the NetBackup server

The following example shows the type of information required by NetBackup for various Media Manager storage unit configurations.

For step-by-step instructions on how to specify this information to NetBackup, see "Adding a New Storage Unit" on page 27.

Example

The following figure shows a master server containing one drive in a robot and a 1/4 inch SCSI tape drive that is a standalone.



Note TL8 - Tape Library 8MM is the NetBackup name for a device type, not a vendor model number. You must use the NetBackup name when configuring a storage unit. (See “Robot Type” on page 31.)

Each of these devices can be a storage unit and the NetBackup settings required to define these storage units are as follows:

- 8 mm tape drive in the robot

Storage Unit Configuration Setting	Value
Media Server	eel
Robot Type	TL8 - Tape Library 8MM
Robot Number	1
Number of Drives	1
Density	8mm - 8mm cartridge

For robots, you must specify the type and number of the robot in which the drives reside.

NetBackup BusinesServer requires that the robotic control be on the same server as the drives.

- SCSI 1/4 inch tape drive

Storage Unit Configuration Setting	Value
Media Server	eel
Robot Type	None
Robot Number	None
Number of Drives	1
Density	qscsi - 1/4 inch cartridge

Disk Storage Unit Considerations

A disk type storage unit consists of a directory on a hard disk that stores the backup or archive data. NetBackup permits an unlimited number of disk storage units.

The following is an example path in a Windows file system: `D:\NetBackup\backups`. A disk type storage unit is useful for testing and is useful during busy periods because it allows quick backups. However, you must be careful that it does not fill up your disk.

Before using a disk storage unit, configure the disk as explained in your operating system documentation. To calculate the approximate disk space that NetBackup requires as it creates backups, use the following formula:

(largest backup size x (number of backups + 1))

+

Space for the restores that are concurrent with backups

NDMP Storage Unit Considerations

NDMP storage units are controlled by Media Manager but attach to NDMP hosts and require that you have the NetBackup for NDMP option installed. See the *NetBackup for NDMP System Administrator's Guide* for more information.

Maintaining Storage Units

The following sections contain information on creating and maintaining storage units:

- "Adding a New Storage Unit" on page 27
- "Changing Storage Unit Properties" on page 28
- "Deleting Storage Units" on page 28

Adding a New Storage Unit

There are two methods to create a new storage unit: create a new one, or copy an existing storage unit.

▼ To create a new storage unit

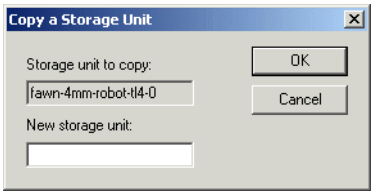
1. If your site has more than one master server, select **File** > **Change Server** to choose the server with the configuration that will use the storage unit.
2. In the NetBackup Administration Console, select **Master Server** > **NetBackup Management** > **Storage Units**. Storage unit information appears in the right pane.
3. Click **Actions** > **New** > **New Storage Unit**. The Add a New Storage Unit dialog appears.
4. Type a unique name for the new storage unit that describes the type of storage you are defining. Click **OK**.
5. Complete the fields on the Add New Storage Unit property tabs.

   The options are described in "Storage Unit Type Properties Tab" on page 30.
6. Click **OK** to add the storage unit to the configuration.

▼ To create a storage unit by copying an existing storage unit

1. If your site has more than one master server, select **File** > **Change Server** to choose the server with the configuration that will use the storage unit.
2. In the NetBackup Administration Console, select **Master Server** > **NetBackup Management** > **Storage Units**. Storage unit information appears in the right pane.

3. Select a storage unit in the right pane.



4. Click **Actions** > **Copy Storage Unit**. The Copy a Storage Unit dialog appears.

5. Type a unique name for the new storage unit that describes the type of storage you are defining.

6. Click **OK**. The Add New Storage Unit dialog appears.

7. Complete the fields on the Copy Storage Unit property tabs.

   The options are described in “Storage Unit Type Properties Tab” on page 30.

Changing Storage Unit Properties

We suggest that you make changes only during periods when you are not expecting backup activity for policies that will be affected by the changes. This allows time for you to make adjustments before backups begin and ensures an orderly transition from one configuration to another. Regardless of your timing, NetBackup is designed to prevent serious problems or failures from occurring.

▼ To change storage unit properties

1. If your site has more than one master server, select **File** > **Change Server** to choose the server with the configuration that will use the storage unit.

2. In the NetBackup Administration Console, select **Master Server** > **NetBackup Management** > **Storage Units**. Storage unit information appears in the right pane.

3. Double-click the storage unit you wish to change from those listed in the right pane. Hold down the Control or Shift key to select multiple storage units.

4. Complete the fields on the Change Storage Unit property tabs.

   The options are described in “Storage Unit Type Properties Tab” on page 30.

Deleting Storage Units

Deleting a storage unit from the NetBackup configuration does not prevent you from restoring files that were written to that storage unit.

▼ **To delete storage units**

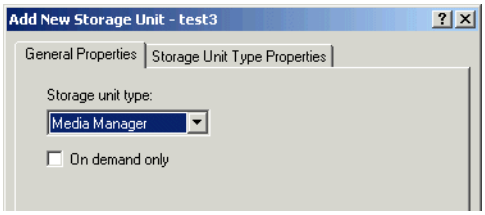
1. If your site has more than one master server, select **File** > **Change Server** to choose the server with the configuration that will use the storage unit.
2. In the NetBackup Administration Console, select **Master Server** > **NetBackup Management** > **Storage Units**. Storage unit information appears in the right pane.
3. Select the storage unit you wish to delete from those listed in the right pane. Hold down the Control or Shift key to select multiple storage units.
4. Click the delete button on the toolbar . A confirmation dialog appears.
5. Click **OK**.
6. Modify any policy that uses a deleted storage unit to use another storage unit.

Storage Unit Properties

Specify general properties when adding a storage unit.

Storage Unit General Properties Tab

Storage Unit Type



Specifies the type of storage that this storage unit will use:

- Disk: A directory on a hard drive
- Media Manager: A robot or standalone tape drive
- NDMP

On Demand Only

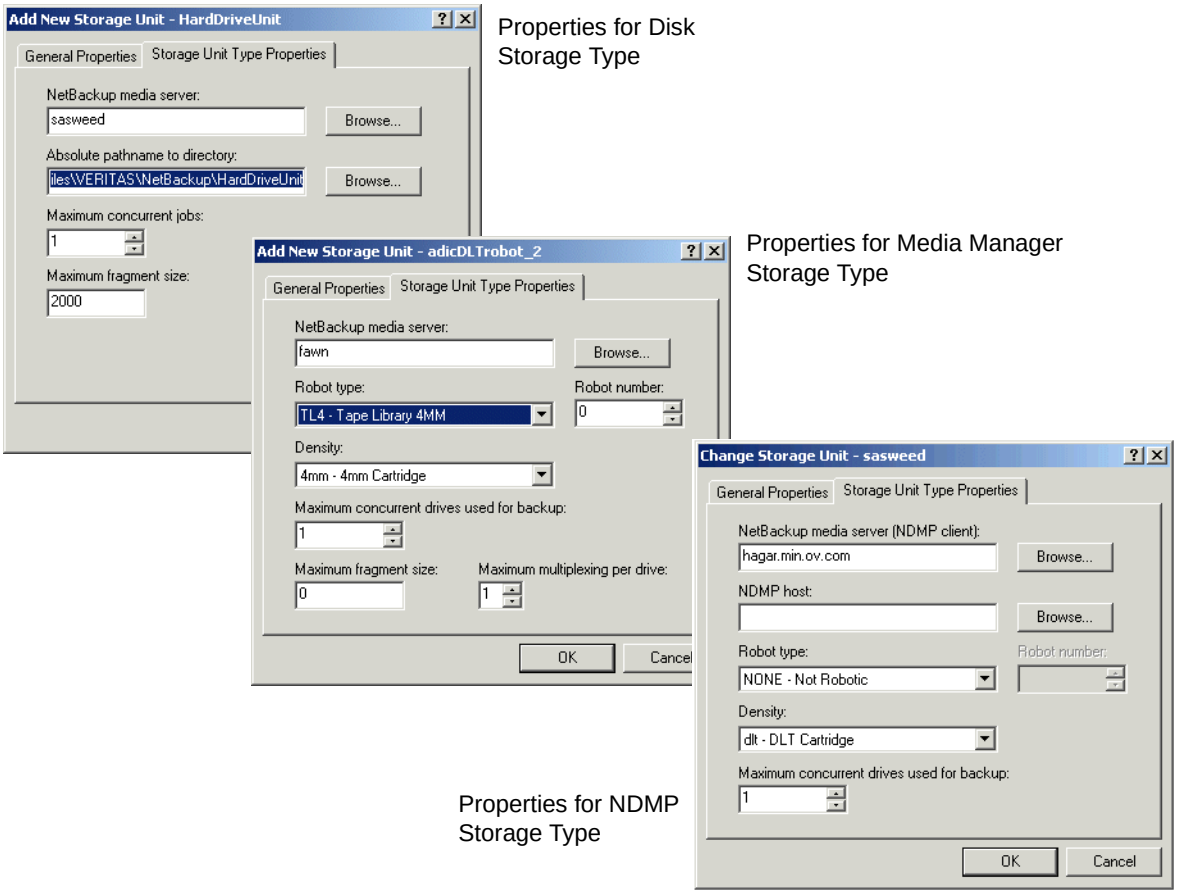
Specifies whether the storage unit is available *only* on demand (that is, only when a policy or schedule is explicitly configured to use this storage unit). Clear the box to make the storage unit available to any policy or schedule.

The default for disk storage units is that **On Demand Only** is checked. The default for all other storage types is that **On Demand Only** is clear.

Note If you make all storage units on demand only, designate a specific storage unit for each policy or schedule. Otherwise, NetBackup will be unable to find a storage unit to use.

Storage Unit Type Properties Tab

Specify the following properties when adding a storage unit. The properties depend on whether the type of storage unit.



NetBackup Media Server

Specifies the name of the NetBackup media server where the drives in the storage unit attach or the name of the server that is controlling the hard disk storage unit. Enter the name that is used for that server in the NetBackup server list.

Robot Type

Specifies the type of robot (if any) that the storage unit contains. The drop-down list uses NetBackup designations for each robot type that NetBackup supports, including a **NONE-Not Robotic** selection.

For the specific vendor types and models that correspond to each robot type, see the Supported Peripherals section of the NetBackup *Release Notes*.

Absolute Pathname to Directory

Specifies the absolute pathname to the file system that will store the backups. Use any location on the disk, providing there is sufficient space available.

The following rule applies to the path you specify:

In addition to the platform-specific file path separators (/ and \) and colon (:) within a drive specification on Windows, use only alphabetic (ASCII A - X, a - z), numeric (0-9), plus (+), minus (-), underscore (_), or period (.) characters. Do not use a minus as the first character.

Robot Number

This is the same robot number used in the Media Manager configuration. For more information on robot numbers, see the *Media Manager System Administrator's Guide*.

NDMP Host

Specifies the NDMP host whose data will be sent to this storage unit.

Density

Specifies the media density that the storage unit will be using.

Maximum Concurrent Drives Used for Backup

Specifies the number of drives that NetBackup can use at one time for backups in this storage unit. Type the desired number in the box:

- For a storage unit that contains only standalone drives, specify a number that is less than or equal to the number of drives that are in this storage unit. NetBackup BusinesServer supports a maximum of two drives. For example, a robot with two drives or a standalone drive and a robot with a single drive.

- For a robot, specify a number that is less than or equal to the number of drives that attach to the NetBackup media server for the storage unit.

Assume you have two standalone drives of the same density and you specify `1`. In this instance, both drives are available to NetBackup but only one drive can be used for backups. This leaves the other drive available for restores and other nonbackup operations (importing, verifying, and duplicating backups).

Maximum Concurrent Jobs

Specifies the maximum number of backups that NetBackup can concurrently send to this disk. For example, if there are three backup jobs for this storage unit and **Maximum Concurrent Jobs** is set to two, the first two jobs start and the third one waits.

Maximum Concurrent Jobs equates to the **Number of Drives** setting for a Media Manager storage unit. The jobs are not multiplexed.

The number to enter depends on the available disk space and the server's ability to comfortably run multiple backup processes.(See "Limit Jobs Per Policy" on page 62.)

Maximum Fragment Size

Specifies the largest fragment size (in megabytes) that NetBackup can create when storing backups.

- For Media Manager storage units, type a value of 50 or larger. To specify unlimited fragment size, type 0 (default).
- For hard disk storage units, the value can range from 20 to 2000 (default). The **Maximum Fragment Size** setting is normally used to ensure that the backup does not exceed the maximum size allowed by the file system.

Note If you change the fragment size, you can still restore backups that were written with the previous fragment size.

For more information, see "Fragmented Backups" on page 658.

Maximum Multiplexing per Drive

Specifies the maximum number of backups that NetBackup can multiplex onto any single drive in the storage unit:

- Specify any value from 1 through 8. The default is 1, which disables multiplexing and allows only one backup job at a time per drive.

- For values greater than 1, NetBackup sends concurrent, multiple backups from one or several clients to a single drive and multiplexes the backups onto the media.See “Multiplexing” on page 402 for more information.

Configuring Drive Availability Checking

NetBackup periodically checks each storage unit to determine the status of its drives and attempts to use a storage unit only if it has drives available. The following topics explain the configuration settings associated with this feature.

Interval Between Status Checks

The NetBackup host property, **Re-read Interval,** determines how often NetBackup checks storage units for available drives. (See “Re-read Interval” on page 272.)

Drive Count Timeout

When NetBackup checks for drive availability, it also counts the drives that are available for backups. This information is then used to prevent scheduling too many jobs for the number of drives.

The only setting associated with counting drives is the length of time that the scheduler waits for the count to complete. If you have problems with timeouts, you can extend the time that the scheduler waits by using the NetBackup host property, **BPTM Query Timeout**. (See “BPTM query timeout” on page 272.)

Requeuing Jobs If Required Storage Units are Unavailable

By default, a job fails (status code 219) if a required storage unit is unavailable when a job starts or, for some reason, becomes unavailable during a backup. However, you can configure NetBackup to requeue jobs for either of these conditions. To configure NetBackup to requeue jobs, use the following NetBackup host properties.

For specific information on values and defaults, see “General Server Tab” on page 271.

- **Wait in Queue** causes active jobs to enter the requeued state if the required storage unit becomes unavailable (for example, a drive goes down). The jobs will then run when the storage unit becomes available. A job fails if the **Timeout in Queue** time expires or its backup window closes before the storage unit becomes available.

- **Queue on Error** causes jobs to enter the requeued state when scheduled, if the required storage unit is not available. The jobs will then run when the storage unit becomes available. If this property is not selected, the job fails with a 219 status. This property requires that the **Wait In Queue** entry also exist or the job will fail immediately anyway with a 219 status if the storage unit is not available.
- **Timeout in Queue** determines how long a requeued job waits for an unavailable required storage unit.

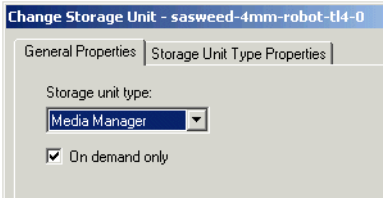
Creating and Changing Storage Unit Groups

Storage unit groups allow you to identify specific storage devices as a group. A storage unit group name can be specified in a policy, just as individual storage units can be specified. When a storage unit group is used in a policy, only the storage units specified in the group will be candidates for the backup.

NetBackup uses the first storage unit listed if the storage unit is available. If the first one is not available, NetBackup attempts to use the second storage unit listed, and so forth down the list.

The only exception is in the case of a client that is also a media server with locally connected storage units. The locally available storage units take precedence over the defined sequence of storage unit groups.

You may have set up a storage unit to be **On Demand Only**. If the storage unit is part of a storage unit group that is needed by a policy, the **On Demand Only** option is satisfied and the device will be used. (See “Policy Storage Unit” on page 60.)



▼ To create a new storage unit group

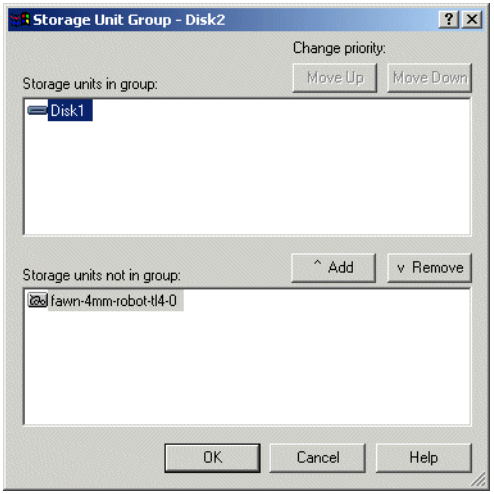
1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Storage Units**.

2. Right click **Storage Unit Groups** and select **New Storage Unit Group**.

3. Enter the storage group name in the **Add a New Storage Unit Group** dialog and click **OK**.

   Use alphabetic (ASCII A-Z a-z), numeric (0-9), plus (+), minus (-), underscore(_), or period (.) characters. Do not use a minus as the first character or leave any spaces between characters.

4. A dialog appears with the name of the new storage unit group.



   a. To add storage units to the group, select the storage units from the **Storage units not in group** list. Click **Add**.

   b. To remove storage units from the group, select the storage units from the **Storage units in group** list. Click **Remove**.

   c. Storage units are listed in order of priority. (The units at the top of the list having the highest priority in the group.) To change the priority of a storage unit, select the storage unit and click **Move Up**or **Move Down**.

5. Click **OK**.

▼ To change a storage unit group

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Storage Units** > **Storage Unit Groups**.

2. Double-click the storage unit group you wish to change.

3. To add storage units to the group, select the storage units from the **Storage units not in group** list. Click **Add**.

4. To remove storage units from the group, select the storage units from the **Storage units in group** list. Click **Remove**.

5. To change the priority of a storage unit, select the storage unit and click **Move Up**or **Move Down**.

6. Click **OK**.

▼ To delete a storage unit group

1. In the NetBackup Administration Console, select **Master Server** > **NetBackup Management** > **Storage Units** > **Storage Unit Groups**.

2. Select the storage unit group you wish to delete from those listed in the right pane. Hold down the Control or Shift key to select multiple storage units.

3. Click the delete button on the toolbar . A confirmation dialog appears.

4. Click **OK**.

Managing Backup Policies 3

Backup policies define the rules that NetBackup follows when backing up clients. A backup policy can apply to one or more clients. Every client must be covered by at least one backup policy. The best approach to configuring backup policies is to divide clients into groups according to their backup and archiving requirements, then create a policy for each group.

This chapter explains how to configure backup policies. The first section introduces policies and gives policy planning guidelines. The remaining sections detail configuration instructions:

- Using the Policies Utility
- Introduction to Backup Policies
- Configuring Backup Policies
- Example Backup Policies
- Planning Guidelines for Backup Policies
- Changing Policies
- Policy Attributes Tab
- Files Tab
- Schedule Tab
- Creating a Vault Policy
- Performing Manual Backups

Using the Policies Utility

The **Policy** utility contains tools for configuring and managing backup policies:

- Tree and Detail Views
- Menus
- Standard and User Toolbars

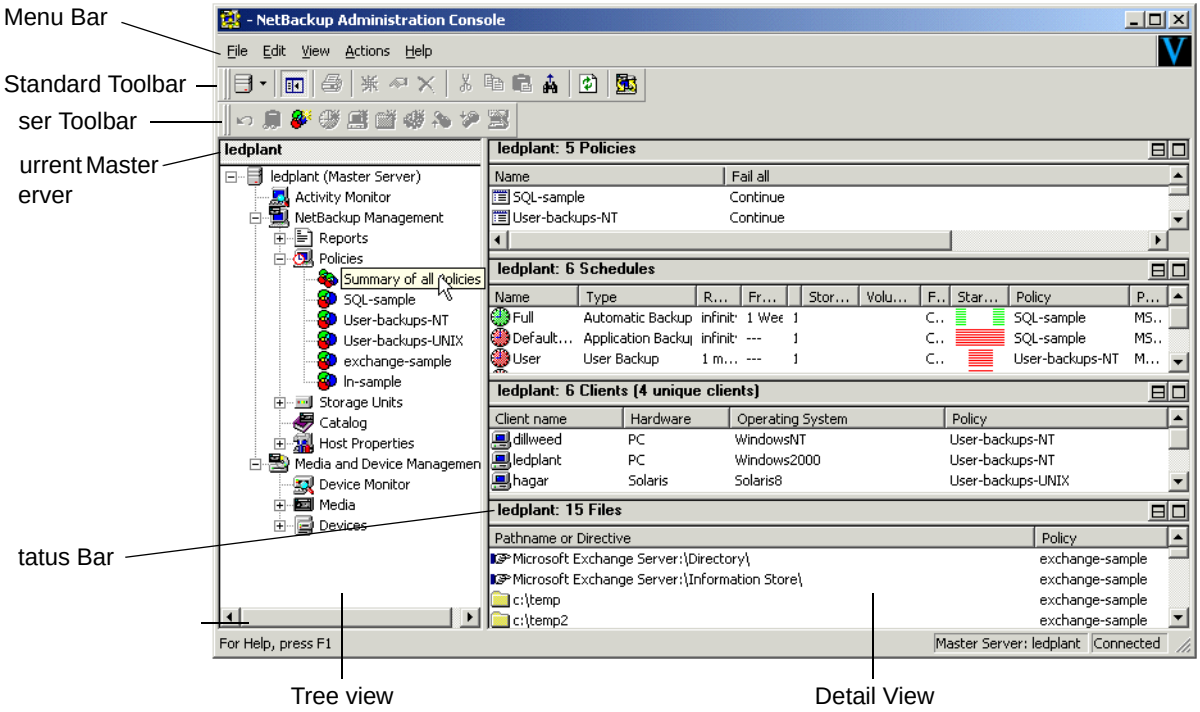
For general information on the NetBackup Administration Console, see “Using the NetBackup Administration Console” on page 3.

Tree and Detail Views

The left pane is a hierarchical view of the backup policies on the master server that you are currently managing. The right pane is a detail view that displays information pertaining to the item selected.

To display information about all policies on the current master server, double-click **Summary of All Policies**. A summary of all polices appears in the right pane, broken down into detail panes displaying **Polices**, **Schedules**, **Clients**, and **Files**.

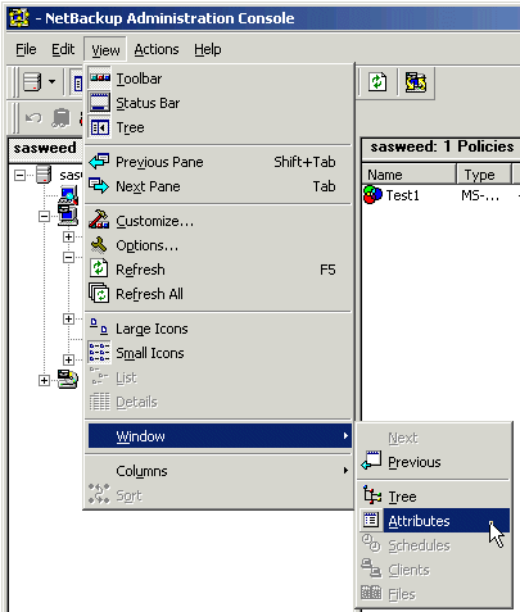
To display the general attributes for a specific policy, select that policy in the left pane. The right pane shows the general attributes for that policy only. Double-click on a policy to display the attributes in tabs, available for editing.


Menu Bar
Standard Toolbar
ser Toolbar
urrent Master
erver
tatus Bar
Tree view
Detail View
- NetBackup Administration Console
File Edit View Actions Help
ledplant
ledplant (Master Server)
Activity Monitor
NetBackup Management
Reports
Policies
Summary of all policies
SQL-sample
User-backups-NT
User-backups-UNIX
exchange-sample
In-sample
Storage Units
Catalog
Host Properties
Media and Device Managemen
Device Monitor
Media
Devices
ledplant: 5 Policies
Name
Fail all
SQL-sample
Continue
User-backups-NT
Continue
ledplant: 6 Schedules
Name
Type
Policy
Full
Automatic Backup
SQL-sample
Default...
Application Backu
SQL-sample
User
User Backup
User-backups-NT
ledplant: 6 Clients (4 unique clients)
Client name
Hardware
Operating System
Policy
dillweed
PC
WindowsNT
User-backups-NT
ledplant
PC
Windows2000
User-backups-NT
hagar
Solaris
Solaris8
User-backups-UNIX
ledplant: 15 Files
Pathname or Directive
Policy
Microsoft Exchange Server:\Directory\
exchange-sample
Microsoft Exchange Server:\Information Store\
exchange-sample
c:\temp
exchange-sample
c:\temp2
exchange-sample
For Help, press F1
Master Server: ledplant
Connected

Menus

The Menu bar consists of **File**, **Edit**, **View**, **Actions**, and **Help**. See Chapter 1 for a description of the items found on these menus.

The following table describes an additional option available on the **View** menu when **Policies** is selected:

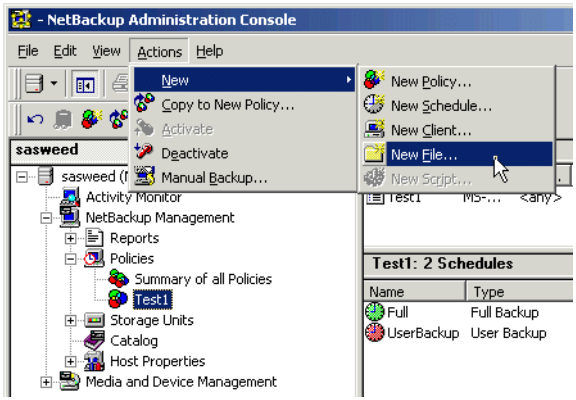


Additional View Menu Option for Policy

Window Commands for selecting various panes in the window.

- **Next**: Makes the next section of the Backup Policy Management window active. For example, if the Attributes section of the right pane is currently active, clicking this command makes the Schedules section active.
- **Previous**: Makes the previous section of the Backup Policy Management window active. For example, if the Attributes section of the right pane was active, clicking this command returns the focus to that window.
- **Tree**: Makes the left pane of the window active.
- **Attributes**: Makes the Attributes section of the right pane active.
- **Schedules**: Makes the Schedules section of the right pane active.
- **Clients**: Makes the Clients section of the right pane active.
- **Files**: Makes the Files section of the right pane active.

The following table describes options available on the **Actions** menu when **Policies** is selected.

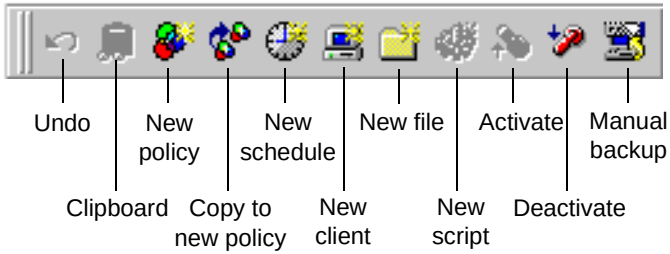


Actions Menu

Menu	Commands
New	Displays a dialog to create and configure one of the following: a new policy, a new schedule, a new client, a new file, or a new script.
Copy to New Policy	Copies the properties of a selected policy and displays them in a dialog so you can change them as necessary for a new policy.
Activate	Activates the policy that is selected in the left pane of the window. A policy must be active for NetBackup to run automatic backups or allow user backups or archives. This setting has no effect on restores.
Deactivate	Deactivates the selected policy (see **Activate** above).
Manual Backup	Displays a dialog where you can start a manual backup of schedules and clients for a specific policy.

Standard and User Toolbars

For information on the standard toolbar, see “Using the NetBackup Administration Console” on page 3.



Introduction to Backup Policies

Backup policies are configured on four tabs, as described in the following sections.

General Attributes on the Attributes Tab

The general attributes on the Change Policy Attributes tab determine the basic characteristics of all the backups that NetBackup performs according to a policy. These include:

- Whether the policy is active and what date and time the policy will go into effect (so NetBackup can use it for backups).
- The type of backup policy, which primarily defines the type of clients the policy is set up to include.
- The priority that NetBackup gives to the backups for this policy relative to other policies.
- The storage unit that NetBackup uses by default when backing up clients covered by this policy. This setting can be overridden for individual schedules by specifying a storage unit for the schedule.

Schedules on the Schedules Tab

The schedules determine when the backups occur. Each schedule also includes criteria, such as how long to retain the backups.

There are two basic categories of schedules, automatic and user, and there are different types of schedules within these categories:

- *Automatic schedules* back up the file list on all clients in the policy according to the timetables set up in the schedules. For example, you can set one schedule for daily incremental backups and another for weekly full backups. An incremental backup includes only files that have changed since the last backup. A full backup includes all files in the file list regardless of whether they have changed.
- *User schedules* specify the times when users can start user backups and archives from the clients. A user archive is a special type of backup that deletes the files from the user disk if the backup is successful. An archive is useful for freeing disk space while still keeping a copy for future use.

File List on the Files Tab

The file list names the files and directories that NetBackup includes in automatic backups of clients covered by a policy.

NetBackup uses the same file list for all clients that it backs up according to this policy. All the files do not need to exist on all the clients, as NetBackup will back up the files that it finds.

Client List on the Clients Tab

The client list names the computers that will be backed up according to a policy. A client must be covered by at least one backup policy and can be covered by more than one. Having a client in more than one backup policy is useful, for example, to back up different sets of files on the client according to different rules.

Configuring Backup Policies

The easiest way to set up a backup policy is use the Backup Policy Configuration Wizard. This wizard guides you through the setup process, simplifying the process by automatically choosing default values that are good for most configurations.

Note The wizard cannot be used, however, to configure a calendar-based schedule or a Vault policy.

▼ **To create a backup policy using the wizard**

1. In the NetBackup Administration Console, select **Master Server** or **NetBackup Management**.
2. From the list of wizards in the right pane, click **Create a Backup Policy**.

See the *NetBackup Installation Guide* for step-by-step instructions.

▼ To create a backup policy without using the wizard

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**. If your site has more than one master server, choose the master server that contains the policy you want to modify. (See “ Administering a Remote Master Server” on page 320.)

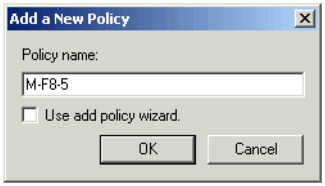
2. Click the New Policy button on the toolbar .

3. Type a unique name for the new policy in the **Add a New Policy** dialog.

   Use alphabetic (ASCII A-Z a-z), numeric (0-9), plus (+), minus (-), underscore(_), or period (.) characters. Do not use a minus or period (.) as the first or last character. Do not leave any spaces between characters.

   If you decide you’d like to use the Backup Policy Configuration Wizard to configure the policy, select **Use add policy wizard**.

   See the *NetBackup Installation Guide* for step-by-step instructions on using the Backup Policy Configuration Wizard.



4. Click **OK**.

Example Backup Policies

The following figure shows the clients, file list, and schedules for two example backup policies.

- Example 1 specifies that files in

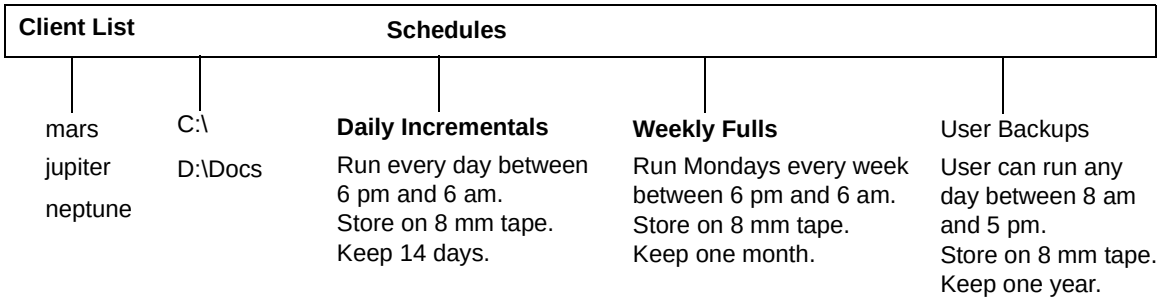
  ```
  C:\
  D:\Docs
  ```

  ```
  /usr
  /home
  ```

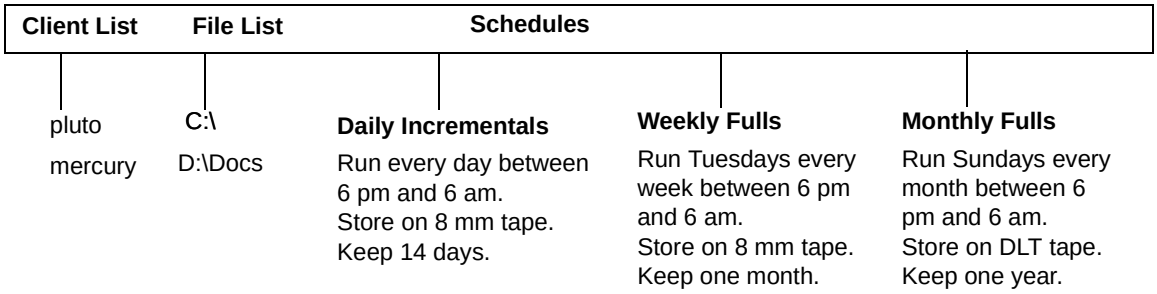
  be backed up for the clients named mars, jupiter, and neptune. This policy has daily, and weekly automatic schedules and a user backup schedule. All backups go to 8 mm tape.

- Example 2 has different scheduling requirements. One difference is that this policy has monthly fulls that go to DLT tape.

Example Backup Policy 1



Example Backup Policy 2



Planning Guidelines for Backup Policies

Backup policies allow you to meet the needs of a wide variety of clients in a single NetBackup configuration. However, taking full advantage of backup policies requires careful planning before starting your configuration. The following procedure provides planning guidelines. The planning worksheets in this manual may also be helpful. (See “Planning Worksheets” on page 660.)

1. Divide clients into groups according to the types of work they perform.

   Clients used for similar tasks usually have a high level of commonality in their backup requirements. For example, most clients in an engineering department create the same types of files at similar levels of importance.

   In some instances, you can create a single policy for each group of clients. In other cases, you will have to further subdivide the clients and cover them in separate policies, based on their backup requirements as explained in later this procedure.

The table below is the initial grouping for our example. We assume these clients are in the same work group and the initial plan is to cover them all in the same backup policy.

Clients
mercury
mars
jupiter
neptune

2. Gather information about each client. Include information relevant to the backups such as the names, size, and number of files.

   In our example client list, mercury is a file server and has a large amount of data. To avoid excessively long backup times, we include mercury in a separate policy called S1 and the workstations in a policy called WS1. Later, we may find that we need more than one policy for mercury, but we will evaluate other factors first. For now, the backup policies are as follows:

Policy	Clients
S1	mercury (file server)
WS1	mars jupiter (workstations) neptune

3. Create backup policies to accommodate special storage requirements.

   The storage unit and volume pool settings apply to all files that are backed up by the policy. If files have special storage unit and volume pool requirements, create separate policies for them, even if other factors, such as schedules, are the same.

In the example below, we create a separate policy (S2) for `D:\h002\DevExp` and `D:\h002\DesDoc` on mercury because those files go on DLT tape. Other files on mercury go on 8 mm tape. If it is necessary to keep backups for some files on separate media, create a policy that specifies a unique volume pool for those backups. Then, add the media for that volume pool.

Policy	Clients	Files	Desired Storage

S1	mercury	`C:\`
		`D:\User`
		`D:\h001`
		`E:\h002\Projects`
			8 mm

S2	mercury mercury	`E:\h002\DevExp` `E:\h002\DesDoc`	DLT

4. Create additional backup policies if one set of schedules does not accommodate all clients and files. Factors to consider are:

   - Best times for backups to occur. To back up different clients on different schedules, create more policies. For example, create different policies for night-shift and day-shift clients. In our example, we can back them all up during the same hours so additional policies are not necessary.

   - How frequently the files change. For example, if some files change very infrequently in comparison to other files, back them up on a different schedule. To do this, create another policy that has an appropriate schedule and then include the files and clients in that policy.

     In our example (see the next table), we place `C:\` on mercury in a different policy (S3). The `C:\` drive on the workstations is also in a separate policy (WS2).

   - How long backups have to be retained. Each schedule has a retention setting that determines how long NetBackup keeps files that are backed up by the schedule. Because the schedule backs up all the files in the file list, it is best if all files have similar retention requirements. Do not, for example, include files whose full backups must be retained forever, in a policy where full backups are retained for only four weeks.

     In our example (see the next table), we place `E:\h002\DesDoc` on mercury in a different policy (S4). This is done because `E:\h002\DesDoc` requires full backups every 12 weeks and those backups must be retained for a much longer time than the other files on mercury.

Policy	Clients	Files	Frequency of Change	Desired Storage	Auto[1] Backup Frequency
S1	mercury	D:\User D:\h001 E:\h002\Projects	high	8 mm	Daily Incr Weekly Full 4 Weeks Full
S2	mercury	E:\h002\DevExp	high	DLT	Daily Incr Weekly Full 4 Weeks Full
S3	mercury	C:\	low	8 mm	Daily Incr 4 Weeks Full
S4	mercury	E:\h002\DesDoc	high	DLT	Daily Incr Weekly Full 4 Weeks Full 12 weeks Full
WS1	mars jupiter neptune	D:\User D:\Programs D:\User D:\Programs D:\User D:\Programs D:\Util	high	8 mm	Daily Incr Weekly Full 4 Weeks Full
WS2	mars jupiter neptune	C:\ C:\ C:\	low	8 mm	Daily Incr 4 Weeks Full

5. Create separate policies for clients that require different general-attribute settings than other clients. Some general-attribute settings to consider are:

   - **Policy Type**. There are several types of backup policies and you must use the correct one for the client. For example, include Windows NT and Windows 2000 clients in an MS-Windows NT policy.
   - **Compression**. Set this attribute if you want a client to compress its backups before sending them to the server. Note that the time to compress can increase back up time and make it unsuitable to use for all clients.
   - **Policy Priority**. Use this attribute to control the order in which NetBackup starts its backups. The client in the higher priority policy is backed up first.

   There are also other general attributes that are explained later in this chapter. In our example, no extra policies are required because of general attribute settings.

6. Create separate policies as necessary to maximize the benefits of multiplexing.

   Using multiplexing for slower clients that produce small backups is a strategy for maximizing drive utilization. However, higher-performance clients that produce long backups are likely to fully utilize drives and not benefit from multiplexing.

7. Evaluate total backup times for each schedule and further subdivide your policies to reduce backup times to an acceptable level.

   Compute the approximate backup time by multiplying the speed of the device by the amount of data in the backup. For example, if your backup device transfers data at 800 kilobytes per second, it takes 0.7 hours to back up 2 gigabytes.

   The variable that is easiest to control here is the amount of data in the backup. NetBackup imposes no limits on backup size, but try to keep backups to less than 2 gigabytes. In addition to reducing backup time, shorter backups usually mean less time to recover files that are near the end of the backup.

   In our example, it so happens that backing up `D:\User`, `D:\h001`, and `E:\h002\Projects` on mercury takes too much time so we create a new policy for `E:\h002\Projects`. This new policy (S5) has the same requirements as S1 but we can now back up `E:\h002\Projects` separately thus reducing backup time. The next table shows the final set of backup policies.

   In addition to reducing the backup time for each policy, backing up the files with separate policies can reduce the total backup time for the server mercury. NetBackup processes files within a file list serially and in the order they appear in the file list. However, separate policies are processed in parallel if enough drives are available and the maximum jobs attributes are set to allow it. (See “Setting the Number of Streams That Can Run Concurrently” on page 73 for an explanation of maximum jobs settings that also applies to this discussion.)

Note For best performance with multiple data streams, use only one data stream to back up each physical device on the client. Multiple concurrent streams from a single physical device can adversely affect backup times.

Policy	Clients	Files	Frequency of Change	Desired Storage	Auto Backup Frequency
S1	mercury	`D:\User` `D:\h001`	high	8 mm	Daily Incr Weekly Full 4 Weeks Full
S2	mercury	`E:\h002\DevExp`	high	DLT	Daily Incr Weekly Full 4 Weeks Full
S3	mercury	`C:\`	low	8 mm	Daily Incr 4 Weeks Full
S4	mercury	`E:\h002\DesDoc`	high	DLT	Daily Incr Weekly Full 4 Weeks Full 12 Weeks Full
S5	mercury	`E:\h002\Projects`	high	8 mm	Daily Incr Weekly Full 4 Weeks Full

WS1	mars
	
	jupiter
	
	neptune
		`D:\User`
		`D:\Programs`
		`D:\User`
		`D:\Programs`
		`D:\User`
		`D:\Programs`
		`D:\Util`
			high	8 mm	Daily Incr
					Weekly Full
					4 Weeks Full

WS2	mars jupiter neptune	`C:\` `C:\` `C:\`	low	8 mm	Daily Incr 4 Weeks Full

Changing Policies

Try to make changes to policies only during periods when there is no expected backup activity for the affected policies and clients. Preventing this potential conflict lets you make adjustments before backups begin and ensures an orderly transition from one configuration to another. Regardless of your timing, NetBackup is designed to prevent serious problems or failures from occurring.

▼ To add or change schedules in a policy

1. If your site has more than one master server, choose the master server that contains the policy you want to modify. See "Administering a Remote Master Server" on page 389.

2. Expand **Master Server** > **NetBackup Management** > **Policies**.

3. Select the policy name in the left pane.

4. Perform one of the following actions:

   - To add a schedule, select **Actions** > **New** > **New Schedule**. The Add New Schedule dialog appears.
   - To change an existing schedule, double-click the schedule name in the right pane.

5. Complete the entries in the Attributes tab, Start Window tab, Exclude Dates tab, and Calendar Schedule tab (if Calendar Schedule Type is selected on the Attributes tab). (See "Schedule Tab" on page 108.)

6. If this is the last schedule, click **OK**. To add more schedules, click **Add** and repeat step 5. Click **Close** to cancel changes that have not been added.

▼ To add or change clients in a policy

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

2. Select the policy name in the left pane.

3. Perform one of the following actions:

   - To add a new client, select **Actions** > **New** > **New Client**. The Add New Client dialog appears.
   - To change an existing client, double-click the client name in the right pane.

4. Complete the entries in the Add New Client or Change Client dialog. (See "To add a client to a policy" on page 75.)

▼ To add or change files in a policy

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

2. Select the policy name in the left pane.

3. Perform one of the following actions:
   - To add a new file, select **Actions** > **New** > **New File**. The Add New File dialog appears.
   - To change an existing path to a file, double-click the pathname in the right pane.

4. Complete the entries in the Add New File or Change File dialog.
   - If you are unfamiliar with how to specify file paths for your clients, read "Rules for Backup File Paths" on page 83 before proceeding.
   - If you are using directives in the file list, see "Adding Directives to the File List" on page 80.

5. After adding the new pathname or making changes to an existing pathname:
   - In the Add a New File dialog, click **Add**. The new entry appears in the list. After defining all new pathnames or directives, click **Insert**.
   - In the Change File dialog, click **OK**.

▼ To delete schedules, files, or clients from a policy

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

Note Do not confuse **Cut** and **Delete**. **Cut** copies the selected information to the clipboard, from where you can later paste it. Delete does not copy to the clipboard.

2. Select the policy name in the left pane.

3. In the right pane, select the item you'd like to delete and click the delete button on the toolbar ✕. A confirmation dialog appears.

4. Click **Yes**.

Note Deleting a client from the NetBackup configuration does not delete NetBackup client software from the client. Previous backups for that client can also be recovered up until their expiration date.

Also, deleting a file only deletes the file from the list of files designated for automatic backup. It does not delete the actual file from the disk.

▼ To cut/copy and paste items

You can copy or cut and paste the following items:

- Copy and paste (not cut) attributes
- Copy and paste (not cut) entire policies
- Copy, cut and paste Schedules, Files, and Clients

When the clipboard contains an entire policy:

- If you select a policy and do the paste, the contents of the clipboard is pasted into the selected policy.
- If you paste to a single type of item within a policy, only that type of information is pasted (for example, files).

  When the clipboard contains a single type of item you can paste it either to a policy or the same type of item within a policy. For example, if the clipboard contains files, you can select a policy or just the files within the policy and do the paste (the same information is pasted either way).

The following is a general procedure (variations are possible):

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**. In the left pane, select the policy from which you want to copy or move items.
2. In the right pane of the window, select the item (files, clients or schedules).
3. Select **Edit** > **Copy** or **Edit** > **Cut**. Both the **Copy** and **Cut** commands copy the selected items to the clipboard.
4. In the left pane, select the policy where you want to paste or move the items.
5. In the right pane, click the area where you will paste the contents of the clipboard: attributes, clients, schedules, or files.

   To view the contents of the clipboard, **Edit** > **Clipboard**.

Note If there are items with the same name, they are replaced with the contents of the clipboard when you paste in the next step. If there are schedules that do not match the policy type, they are deleted or renamed (the action is indicated in a dialog).

6. On the **Edit** menu, click **Paste**.

Copying or Moving Policy Information Between Servers

You can paste all or part of a policy to another server by changing to that server after copying the information to the clipboard. However, for the configuration to work you must complete the rest of the configuration on that server (for example, add the storage unit and volume pool).

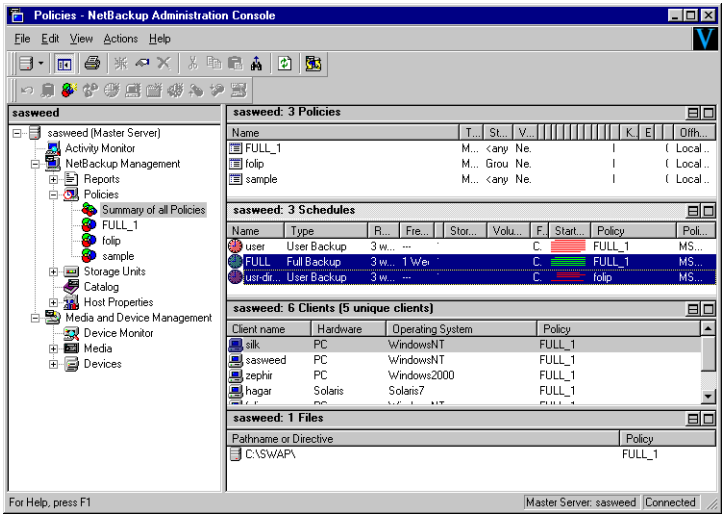
Changing Multiple Policies in the Composite View

1. In the NetBackup Administration Console, expand **Master Server > NetBackup Management > Policies** > **Summary of All Policies**. The right pane displays the attributes, schedules, files, and clients in all policies.

2. In the right pane, hold down the Shift key and select the items you want to change.

3. Select **Edit** > **Change**.

   See the following section, “Using the Composite Change Dialog” on page 57.



Using the Composite Change Dialog

The following topics explain how to interpret and change properties in the dialogs when editing attributes, schedules or clients in the composite view.

Interpreting the Initial Settings

If the property has a text field where you can specify a value, the check box for the property is clear and the text field is:

- Gray with a value if the property has the same value for all selected machines.
- Clear if the property does not have the same value for all selected machines.

If the property has only a check box and not a value, the check box is in one of the following states:

- Selected (checked) if the attribute is selected for all selected machines.

- Clear if the property is clear on all selected machines.

- Gray check if the property is set differently on the selected machines.

Changing the Settings

If the property has a text field in which to specify a value:

- Select the associated check box and type the value in the field, to set the property to the same value for all selected clients.
- Clear the associated check box (the field changes to gray) to leave the property unchanged.

If the property has only a check box:

- Select the check box to set the property on all selected machines.
- Clear the check box to clear the property on all selected machines.
- Set the box to a gray check to leave the property unchanged.

At any time you can:

- Cancel changes by clicking the **Cancel** button.
- Click **OK** to apply all changes and close the dialog.

Policy Attributes Tab

The general policy attributes on the Attributes tab determine the basic characteristics of all the backups that NetBackup performs according to this backup policy.

▼ To set the general policy attributes

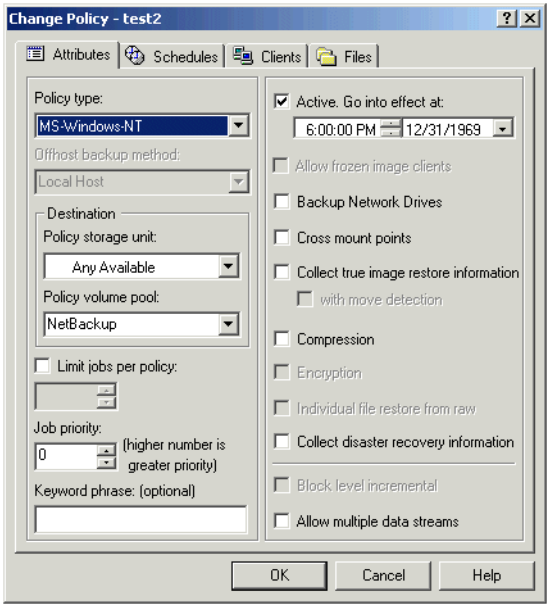
1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

2. Double-click the policy name in the left pane. The Change Policy dialog appears, containing four policy attribute tabs: Attributes, Schedules, Clients, Files.

3. Select a tab and make any changes.
   - See the following section for changes to the Attributes tab
   - See “Clients Tab” on page 75.
   - See “Files Tab” on page 77.
   - See “Schedule Tab” on page 108.

4. Click **OK** to save the changes, then click **Close** to close the Change Policy or New Policy dialog.

The following sections describe the configuration options in the Attributes tab. Options are configurable depending on the type of policy and the options installed. For example, **Encryption** is available only when the NetBackup Encryption option is installed.



Policy Type

Determines the type of clients that can be in the policy and, in some cases, the types of backups that can be performed on the clients. Select the type of policy from the drop-down list. See the following table for a description of each policy type.

If you change the policy type for an existing policy that contains schedules that are invalid for the new policy type, NetBackup prompts you, then either deletes the invalid schedules or, if possible, changes them to an equivalent type.

Policy Types

Policy Type	Description
Lotus-Notes	Use when the policy will have only clients with the NetBackup for Lotus Notes option. See the guide for that option for information on setting up this policy type.
MS-Windows-NT	Use when the policy will have only Windows 2000 or NT clients.
MS-Exchange-Server	Use when the policy will have only clients with the NetBackup for MS-Exchange option. See the guide for that option for information on setting up this policy type.
MS-SQL-Server	Use when the policy will have only clients with the NetBackup for MS-SQL Server option. See the guide for that option for information on setting up this policy type.
NetWare	Use when the policy will have only NonTarget NetBackup Novell NetWare clients (this version uses a Microsoft Windows interface).
NDMP	Use when the policy will have only clients with the NetBackup for NDMP option. This policy is available only when the NetBackup NDMP is installed and licensed. See the guide for that option for information on setting up this policy type.
OS/2	Use when the policy will have only NetBackup OS/2 clients.
Oracle	Use when the policy will have only clients with the NetBackup for Oracle option. See the guide for that option for information on setting up this policy type.
Standard	Use when the policy will have any combination of the following: - Windows 98 or 95 clients. - Macintosh clients. - NetBackup Novell NetWare clients that have the target version of NetBackup software. - UNIX clients, except those covered by other special policies such as Oracle.
Vault	Available only when Vault is licensed. Use as a policy type to schedule and run a Vault job.
Note: The following policy types apply only to UNIX clients.	
Informix-On-BAR	Use when the policy will have only clients that are running the NetBackup for Informix option. See the guide for that option for information on setting up this policy type.

Policy Types (continued)

Policy Type	Description
Sybase	Use when the policy will have only clients with the NetBackup for Sybase option. See the guide for that option for information on setting up this policy type.

Offhost Backup Method

Specifies the backup method for the policy.

For more details on offhost backup, refer to the *NetBackup ServerFree Agent System Administrator's Guide.*

Policy Storage Unit

Specifies the default storage unit for backups of this policy. NetBackup uses the default storage unit for all schedules that do not specify another storage unit. A schedule-level storage unit (when specified) overrides the policy default. (See "Override Policy Storage Unit" on page 114.)

Select the policy storage unit from the drop-down list. You can also indicate **Any Available**. If you select **Any Available**, NetBackup tries locally-attached storage units first, and if none are found, the storage units are tried in alphabetical order. NetBackup uses the first storage unit that meets the following requirements:

- The storage unit must not be designated as *On Demand Only*
- The storage unit must have available drives
- The storage unit must have media available in the required volume pool

The only exception is in the case of a client that is also a media server with locally connected storage units. The locally available storage units take precedence over the sequence based on alphabetical order.

Example

Assume that all schedules but one can use a Tape Stacker 8MM. The schedule that is the exception requires a Tape Library DLT. Here, you specify Tape Stacker 8MM at the policy level and specify the following on the schedules:

- For schedules that can use the Tape Stacker 8MM, clear **Override Policy Storage Unit**. When these schedules run, NetBackup uses a Tape Stacker 8MM.

- For the schedule that requires DLT, select **Override Policy Storage Unit** and select Tape Library DLT. When this schedule runs, NetBackup overrides the policy default and uses the DLT library.

Notes on Specifying a Storage Unit

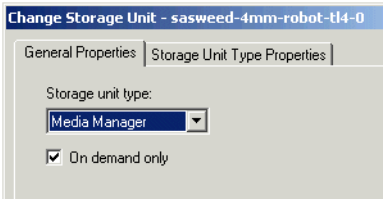
- If your site has only one storage unit or there is no preference for storage:
  - Specify *Any Available* for the policy storage unit *and*
  - Do not specify a storage unit at the schedule level

  However, in this instance, ensure that you do not configure all storage units to be *on demand only*, or NetBackup will be unable to find an available storage unit for the backups.
- If you designate a specific storage unit and it is not available (for example, because it is down for maintenance), backups will not run for policies and schedules that require the storage unit.
- If your NetBackup configuration has several storage units and you want a policy to use *more than one but not all* of the storage units, perform the following:

  a. When you configure volumes in Media Manager, define a volume pool and volumes that are available only to the desired storage units.

  b. For the policy, set **Policy Volume Pool** to the volume pool defined in step a.

  c. For all policies, set **Policy Storage Unit** to *Any Available*.
- You may have set up a storage unit to be **On Demand Only**. If the storage unit is part of a storage unit group that is needed by a policy, the **On Demand Only** option is satisfied and the device will be used. (See “On Demand Only” on page 29.)



Policy Volume Pool

Specifies the default volume pool for backups of this policy and NetBackup uses it for all schedules that do not specify another volume pool. A schedule-level volume pool (when specified) overrides the policy default. (See “Override Policy Volume Pool” on page 115.) If you do not name a volume pool for either the policy or the schedule, NetBackup uses the *NetBackup* pool.

Select the desired volume pool name from the drop-down list. The list displays all previously configured volume pools.

Example

Assume that you want all schedules but one to use the *backups* pool. The exception in this case is a user-archive schedule that requires the *archive* pool.

Here, set **Policy Volume Pool** to *backups* When you set up the schedules for the policy, set **Override Policy Volume Pool** as follows:

- For schedules that use the *backups* volume pool, clear **Override Policy Volume Pool**.
- For the schedule that requires the *archive* volume pool, select **Override Policy Volume Pool** and specify *archive* for the pool name.

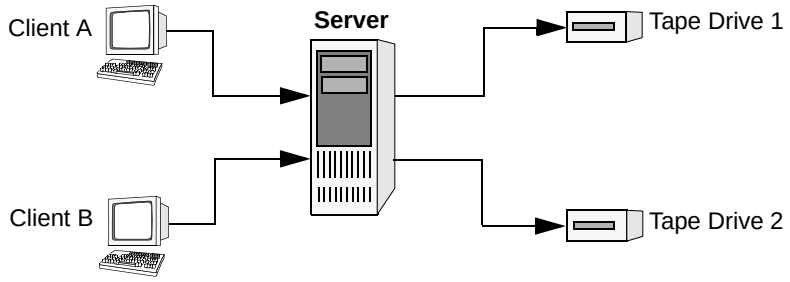
Notes on Volume Pools

- This setting is optional for Media Manager type storage units and is not available for Disk type storage units.
- It is possible to configure a scratch pool from which NetBackup can automatically transfer volumes when another volume pool does not have media available.

For more information on volume pools, see the *System Administrator's Guide for Media Manager.*

Limit Jobs Per Policy

If the **Limit Jobs Per Policy** check box is clear (default), the maximum number of backup jobs that NetBackup will perform concurrently for this policy can be up to 8. To specify a lower limit, select the check box and specify a value from 1 to 8.



Client A and Client B backups can occur concurrently and to different devices

Notes on Limit Jobs Per Policy

The number of concurrent backup jobs that NetBackup can perform depends on:

- Number of storage devices available and multiplexing limits. To process more than one backup job at a time, your configuration must include more than one storage unit, or a storage unit with enough drives to perform more than one backup at a time, or storage units configured to multiples. With removable media devices such as tape drives, this depends on the total number of drives in the storage units. With magnetic disk, the storage device is defined as a file path and the available disk space determines how many paths are possible.
- Server speed. Too many concurrent backups interfere with the performance of the server. The best number depends on the hardware, operating system, and applications that are running.
- Network loading. The available bandwidth of the network determines how many backups can occur concurrently. If you encounter loading problems, consider backing up over multiple networks or using compression.

  A special case exists when backing up a client that is on the same machine as the server. Here, network loading is not a factor because you do not use the network. Client and server loading, however, is still a factor.
- Multiplexing. If you use multiplexing, set **Limit Jobs Per Policy** high enough to support the specified level of multiplexing.

  Lower values can limit multiplexing within a policy if there are jobs from different schedules within that policy. For example, if **Limit Jobs Per Policy** is at 2 and an incremental backup schedule is due to run for four clients, only two are backed up at a time, regardless of multiplexing settings.
- **Limit Jobs Per Policy** does not prevent concurrent jobs if the jobs are from different policies.

  For example, if there are three policies and each has its **Limit Jobs Per Policy** at 2, NetBackup can start two jobs from each policy and have a total of six running at one time.

Job Priority

Specifies the priority that NetBackup assigns to automatic-backup jobs for this policy. When a drive becomes available, NetBackup assigns it to the first client in the highest priority policy.

To set the priority, type any positive integer in the **Job Priority** text box. Higher values have higher priority. The default is 0.

Keyword Phrase (Optional)

Specifies a keyword phrase that NetBackup will associate with all backups or archives for this policy. Users on Windows NT/2000 and UNIX clients can then optionally list or restore only the backups that have this phrase associated with them (see the appropriate NetBackup user's guide). The user interfaces on other NetBackup clients do not support keyword phrases.

You can use the same keyword phrase for more than one policy. This makes it possible to link backups from related policies. For example, you can use one keyword phrase for full backups and another for incremental backups.

The phrase can be a maximum of 128 characters in length. All printable characters are permitted including spaces and periods. By default, there is no keyword phrase.

Users on Windows NT/2000 and UNIX clients can also specify a keyword phrase for a user backup or archive. A user phrase overrides the policy phrase.

Active. Go Into Effect At

To activate the policy, select the **Active** box. The policy must be active for NetBackup to run automatic-backup schedules or allow user backups or archives.

The **Go Into Effect** field specifies when this policy may begin scheduling backups. If today is Monday and you enter Wednesday at 12:00 AM, the policy will not run until after that time. This is useful for configuring a series of policies in advance of when you want them to become active.

To deactivate a policy, remove the check from the **Active** box. To resume backups, recheck the **Active** box, making sure that the **Go Into Effect** date and time is set to the current time or the time when you want to resume backups.

Allow Frozen Image Clients

The **Allow Frozen Image Clients** checkbox specifies whether or not clients included in this policy must be configured for frozen image backups. The frozen image feature is part of NetBackup ServerFree Agent, which can be configured from UNIX servers only.

Cross Mount Points

Note The **Cross Mount Points** attribute applies only to certain policy types and NetBackup allows you to select it only in those instances.

Controls whether NetBackup crosses file system boundaries during a backup or archive on UNIX clients or whether NetBackup enters volume mount points during a backup or archive on Windows clients. “UNIX Reference Topics” on page 671 provides additional information for using this setting with UNIX clients.

Collect True Image Restore Information

Note **True Image Restore Information** applies only to certain policy types and NetBackup allows you to select it only in those instances.

Specifies that NetBackup will start collecting the information required to restore directories to contain what they had at the time of any incremental (or full backup) that the user chooses to restore. Files that were deleted before the time of the selected backup are not restored. Otherwise, for example, a restore based on the date of an incremental includes all files backed up since the last full backup, including those that were deleted sometime during that period.

NetBackup starts collecting the true-image restore information beginning with the next full or incremental backup for the policy. The true-image restore information is collected for each client regardless of whether any files were actually changed.

NetBackup does not provide true-image restores based on the time of a user backup or archive. It does, however, use the backups from user operations for a true-image restore, if they are more recent than the latest automatic full or incremental.

To have true-image incremental backups include files that were moved, renamed, or newly installed in the directories, you must also select **With Move Detection**.

With Move Detection

Specifies that NetBackup also collect the information required to detect files and directories that have been moved, renamed, or newly installed and then include those files and directories in incremental backups for this policy.

Without move detection, NetBackup skips these files and directories because their archive bits are unchanged. With move detection, NetBackup compares path names with those from the previous full or incremental backup. If a name is new or changed, the file or directory is backed up.

The following are examples where using move detection backs up files that would not otherwise be backed up:

- A file named `C:\pub\doc` is moved to or installed in `C:\spec\doc`. Here, the archive bit is unchanged but `C:\spec\doc` is new in the `C:\spec\` directory and is backed up.

- A directory named `C:\security\dev\` is renamed as `C:\security\devices\`. Here, the archive bit is unchanged but `C:\security\devices\` is a new directory and is backed up.

NetBackup starts collecting information required for move detection beginning with the next full or incremental backup for the policy. This first backup after setting the attribute, always backs up all files, even if it is an incremental.

Move detection takes space on the client and the backup can fail if there is not enough disk space available.

Example of What Happens During True-Image Restores

The following table shows the files backed up in the `C:\home\abc\doc` directory during a series of backups between 12/01/2001 and 12/04/2001. Assume that **True Image Restore Information** was selected for the policy that did the backups.

Day	Type of Backup	Files Backed Up in C:\user\doc						
12/01/2001	Full	file1	file2	dirA\fileA	dirB\fileB	file3		
12/02/2001	Incremental	file1	file2	dirA\fileA	----------	------		
12/03/2001	Incremental	file1	file2	dirA\fileA	----------	------		
12/04/2001	User backup	file1	file2	dirA\fileA	----------	------	dirC\fileC	file4
12/04/2001	Incremental	file1	file2	----------	----------	------	----------	file4
Note Dashes (------) indicate that the file was deleted prior to this backup.								

Also, assume that you are going to restore the 12/04/2001 version of the `C:\user\doc` directory.

- If you do a regular restore, the restored directory has all files and directories that ever existed in `C:\user\doc` from 12/01/2001 (last full backup) through 12/04/2001:

```
file1
file2
dirA\fileA
dirB\fileB
file3
dirC\fileC
file4
```

- If you do a true-image restore of the 12/04/2001 backup, the restored directory has only the files and directories that existed at the time of the incremental backup on 12/04/2001:

  ```
  file1
  file2
  file4
  ```

  NetBackup does not restore *any* of the files deleted prior to the 12/04/2001 incremental backup.

  The restored directory does not include the `dirA` and `dirC` subdirectories, even though they were backed up on 12/04/2001 with a user backup. NetBackup did not restore these directories because they did not exist at the time of the incremental backup, which was the reference for the true-image restore.

Notes On True-Image Restores and Move Detection

- Because the additional information that NetBackup collects for incrementals is the same as for a full backup, incremental backups take much more disk space when you are collecting true-image restore information. Adding move detection requires even more additional space.
- You can set the period of time that NetBackup keeps the true-image restore information by setting **How Long to Keep TIR Information** on the Global NetBackup Attributes properties tab. (See "How Long to Keep TIR Information" on page 243.)
- Incremental backups are slower for a policy where true-image restore information is being collected.
- You can perform true-image restores only on directories that were backed up by a policy for which NetBackup is collecting true-image restore information.

  If you intend to restore an entire file system or disk by using a true-image restore, ensure that all the desired directories are backed up by a policy that is collecting true-image restore information.
- For true-image restores, you can list and select only directories. In true-image restore mode, the client-user interface does not show individual files or let you select them. The NetBackup user's guides explain this further and provide instructions for performing true-image restores.
- A true-image restore preserves files that are currently in the directory but were not present when the backup was done. In our previous example, assume you created a file named file5 after the incremental backup occurred on 12/04/2001, but before doing the restore. In this case, the contents of the directory after the restore is:

  ```
  file1
  file2
  file4
  ```

```
file5
```

Compression

Note NetBackup allows you to select **Compression** for the policy types where it applies.

Specifies that software compression be used for backups of this policy. Select the box to enable compression (the default is no compression).

Advantages of Using Compression

Compression reduces the size of a backup by reducing the size of files in that backup. In turn, this decreases the amount of media required for storage. Because the compression and subsequent expansion is performed on the client, compression also decreases the amount of data going over the network and therefore the network load.

Disadvantages of Using Compression

Disadvantages of compression are that it increases computing overhead on the client and also increases backup time (due to the time required to compress the files). The lower transfer rate associated with compression on the client reduces the ability of some tape devices (notably 8 mm) to stream data, thus causing more wear on those devices than would otherwise occur.

The savings in media and network resources, however, still make compression desirable unless total backup time or client computing resources become a problem. If total backup time is a problem, consider multiplexing. The NetBackup multiplexing feature backs up clients in parallel, thus reducing the total time to back them up.

How Much Compression Can You Expect?

The degree to which a file can be compressed depends on the types of data. A backup usually involves more than one type of data. Examples include stripped and unstripped binaries, ASCII, and repeating non-unique strings. If more of the data is favorable to compression you obtain more compression.

Note When compression is not used, it is normal to receive slightly more data at the server than is on the client (on UNIX, this is as shown by `du` or `df`) due to client disk fragmentation and file headers added by the client.

Compression Specifications

Types of data that compress well:	Programs, ASCII files, and unstripped binaries (typically 40% of the original size).
Best-case compression:	Files composed of repeating, nonunique strings can sometimes be compressed to 1% of their original size.
Types of data that do not compress well:	Stripped binaries (usually 60% of original size).
Worst-case compression:	Files that are already compressed become slightly larger if compressed again. On UNIX clients, if this type of file exists and it has a unique file extension, exclude it (and other others with the same extension) from compression by adding it under the NetBackup host UNIX Client tab.
Effect of file size:	File size has no effect on the amount of compression. It takes longer, however, to compress many small files than a single large one.
Client resources required:	Compression requires client computer processing unit time and as much memory as the administrator configures.
Effect on client speed:	Compression uses as much of the computer processing unit as available and affects other applications that require the computer processing unit . For fast CPUs, however, I/O rather than CPU speed is the limiting factor.
Effect on total backup time:	On the same set of data, backups can take three or more times as long with compression.
Files that are not compressed:	NetBackup does not compress: Files that are equal to or less than 512 bytes, because that is the tar block size. On UNIX clients, files ending with suffixes specified with the `COMPRESS_SUFFIX = .`*suffix* option in the `bp.conf` file. On UNIX clients, files with the suffixes as shown below:

Compression Specifications (continued)

.arc or .ARC	.gz or GZ	.iff or .IFF	.sit.bin or .SIT.bin
.arj or .ARJ	.hqx or .HQX	.pit or .PIT	.tiff or .TIFF
.au or .AU	.hqx.bin or .HQX.BIN	.pit.bin or .PIT.BIN	.Y
.cpt or .CPT	.jpeg or .JPEG	.scf or .SCF	.zip or .ZIP
.cpt.bin or .CPT.BIN	.jpg or .JPG	.sea or .SEA	.zom or .ZOM
.F	.lha or .LHA	.sea.bin or .SEA.BIN	.zoo or .ZOO
.F3B	.lzh	.sit or .SIT	.z or .Z
.gif or .GIF	.pak or .PAK		

Encryption

Specifies encryption for backups of clients in this policy.

Note Available only when the NetBackup Encryption option is installed and configured. See the *NetBackup Encryption System Administrator's Guide* for more information.

Collect Disaster Recovery Information

Specifies that you want NetBackup to collect the information required for intelligent disaster recovery when it backs up Windows clients in this policy. (See "Configuring NetBackup Policies for IDR" on page 696.)

Allow Multiple Data Streams

Specifies that, depending on directives in the file list, NetBackup can divide automatic backups for each client into multiple jobs, with each job backing up only a part of the file list. The jobs are in separate data streams and can occur concurrently.

- How many streams (backup jobs) start for each client and how the file list is divided into separate streams is determined by the directives that you specify in the file list. (See "File List Directives for Multiple Data Streams" on page 100.)
- The total number of streams that can run concurrently is determined by the following settings:
  - Number of available storage units
  - Multiplexing settings

- Maximum jobs parameters

(See “Tuning Multiple Data Streams” on page 73.)

Note If **Allow Multiple Data Streams** is in use, and a file system exists in an exclude list for a client, a NetBackup job appears in the Activity Monitor for the file system that was excluded. This is normal behavior and none of the files in the excluded file system will be backed up.

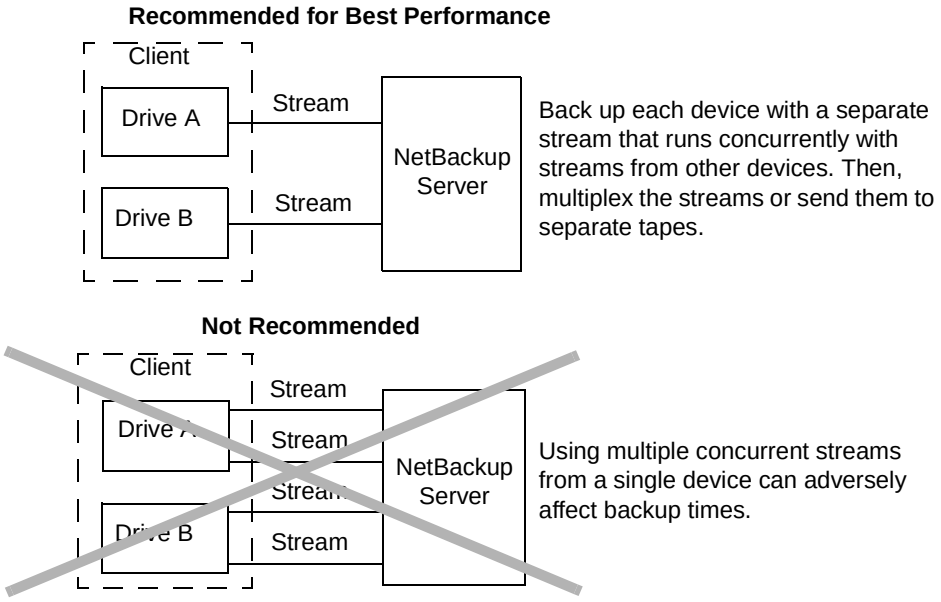
When to Use Multiple Data Streams

Reduce Backup Time

Multiple data streams can reduce the backup time for very large backups. This is achieved by splitting the backup into multiple streams and then using multiplexing, multiple drives, or a combination of the two for processing the streams concurrently.

In addition, configuring the backup so each physical device on the client is backed up by a separate data stream that runs concurrently with streams from other devices can significantly reduce backup times.

Note For best performance, use only one data stream to back up each physical device on the client. Multiple concurrent streams from a single physical device can adversely affect backup times because the heads must move back and forth between tracks containing files for the respective streams.



Reduce Retry Time for Backup Failures

Because the backup streams are completely independent, multiple data streams also provide a form of checkpoint restart. A single failure only terminates a single stream and NetBackup can restart the failed stream without restarting the others. This improves retry time when a backup failure occurs.

For example, assume the backup for a 10 GB partition is split into 5 streams, each containing 2 GB. If the last stream fails after writing 1.9 GB (a total of 9.9 GB backed up), NetBackup retries only the last 2 GB stream. If this 10 GB partition is backed up without multiple data streams and a failure occurs, the entire 10 GB backup must be retried.

The Schedule Backup Attempts global attribute applies to each stream. For example, if it is set to 3, NetBackup retries each stream a maximum of three times.

The Activity Monitor shows each stream as a separate job. Use the job details view to determine the files that are backed up by each of these jobs.

Reduce Administration - More Backups With Fewer Policies

When a configuration contains large file servers with many file systems and volumes, using multiple data streams will provide more backups with fewer policies than are otherwise required.

Tuning Multiple Data Streams

The two aspects of multiple data streams that you can tune are the total number of streams and the number of streams that can run concurrently.

Note For best performance, use only one data stream to back up each physical device on the client. Multiple concurrent streams from a single physical device can adversely affect backup times because the heads must move back and forth between tracks containing files for the respective streams.

Setting the Total Number of Streams

The file list determines the total number of streams that are started. The `NEW_STREAM` directive allows you to explicitly configure a fixed number of streams, or you can have the client dynamically define the streams. (See "File List Directives for Multiple Data Streams" on page 100.)

Setting the Number of Streams That Can Run Concurrently

The number of streams that can run concurrently for a policy or client is determined by the following:

- Storage unit and schedule multiplexing limit
- Number of drives that are available
- Maximum concurrent jobs settings for the policy and client

Each storage unit and each schedule has a maximum multiplex setting. The lower of the two settings is the limit for a specific schedule and storage unit. The maximum number of streams that can be multiplexed is limited to the sum of the multiplexing limits for all drives available in the storage unit and schedule combinations.

For example, assume there are two storage units with one drive in each. MPX on storage unit 1 is set to 3 and MPX on storage unit 2 is set to 5. If MPX is set to 5 or greater in the schedules, then 8 streams can run concurrently.

The maximum jobs settings also limit the maximum number of streams:

- **Maximum Jobs Per Client** (**Host Properties** > **Master Server** > **Global NetBackup Attributes**)
- **Limit jobs per policy** (policy attribute)

- **Maximum Data Streams** (Set the number in **Host Properties** > **Master Server** > **Client Attributes**)

The maximum job settings are interdependent as follows:

- If **Maximum Data Streams** is not set, the lowest value of **Maximum Jobs Per Client** and **Limit Jobs Per Policy** is the limiting factor.
- If **Maximum Data Streams** is set, then NetBackup ignores **Maximum Jobs Per Client** and uses the lowest value of **Maximum Data Streams** and **Limit Jobs Per Policy** as the limiting factor.

Clients Tab

Add, delete, or change clients for a policy on the **Clients** tab. You can also install NetBackup software on UNIX client machines or configure a frozen image backup method.

▼ To add a client to a policy

1. If your site has more than one master server, use **File** > **Change Server** to choose the master server that contains the policy you want to modify.

2. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

3. In the left pane, double-click the policy you wish to change.

4. Select the Clients tab and click **New**.

5. In the highlighted field, type the name of the client you are adding or browse to find and select the client.

   Observe the following rules for assigning client names:

   - The name must be one by which the server knows the client.
   - If the is client in multiple policies, use the same name in each policy.
   - Use a name by which the server knows the client (one that you can use on the server to `ping` or `telnet` to the client).
   - If the network configuration has multiple domains, use a more qualified name. For example, use mars.bdev.null.com or mars.bdev rather than just mars.

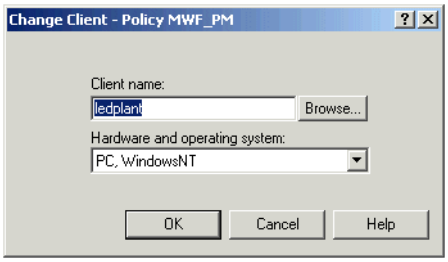
6. Press Enter.

7. If this is the last client, click **OK** to close the Change Policy dialog or select another tab. If you're adding more clients, click **New**. Click to cancel changes that you have not yet added and close the dialog.

▼ To change a client list entry

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

2. In the left pane, double-click the policy you want to change. The Change Client dialog appears.



3. In the **Client Name** field, type or browse to find the name of the client.

4. Click the button to the right of the **Hardware and Operating System** box and select the desired entry.

   Add only clients with hardware and operating systems that this policy supports. For example, do not add a Novell NetWare client to an MS-Windows-NT policy.

5. Click **OK** to save the change or **Cancel** to discard it.

Files Tab

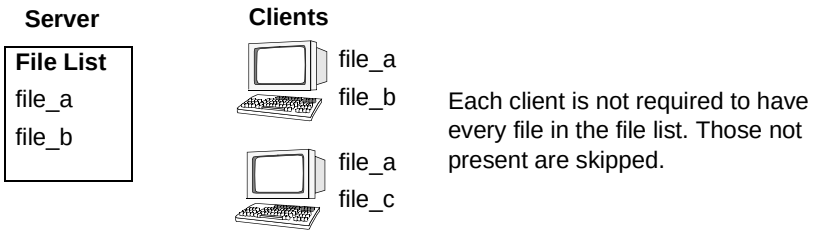
The file list names the files and directories that NetBackup includes in automatic backups of clients covered by a policy. The file list does not apply to user backups or archives— in those instances the user selects the files.

NetBackup uses the same file list for all clients that it backs up according to this policy. All the files do not need to exist on all the clients, as NetBackup will back up the files that it finds. However, at least one of the files should exist on each client. File list entries are processed serially for each client, but it is possible to back up multiple clients in parallel if enough drives are available.

Specifying the List of Files to Back Up

The file list for a policy is the list of files and directories that NetBackup includes in automatic backups (full and incremental) of clients that belong to the policy. NetBackup backs up only the files it finds and does not require that all entries in the list be present on every client. However, each client must have at least one of the files in the file list or the client backup will fail with a status 71.

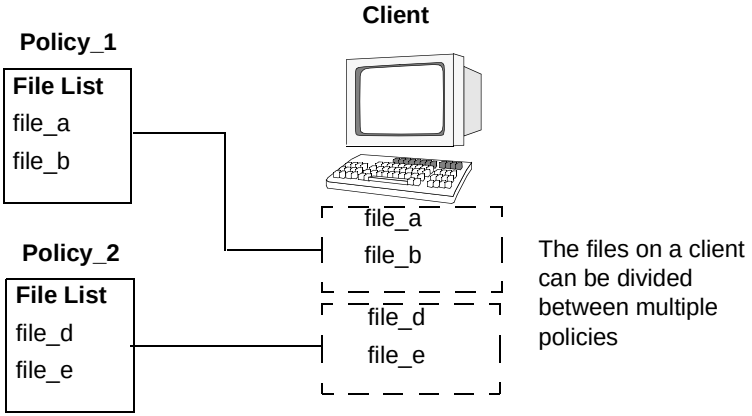
Note The policy file list does not apply to user backups or archives because users select the files before they start the operation.



NetBackup processes file-list entries one at a time. However, NetBackup backs up the files from multiple clients in parallel, assuming multiple storage devices are available and NetBackup attributes are set to allow it. (See “Setting the Number of Streams That Can Run Concurrently” on page 73.)

- The **Maximum Jobs per Client** policy attribute and **Limit Jobs per Policy** global attribute are set to allow it.
- Multiple storage devices are available (or you are using multiplexing).

It is also possible to add a client to multiple policies and then divide the client's files among the file lists. This method has the advantage of backing up different files on a client according to different rules. For example, you can have a different set of schedules for each of them.



Using multiple policies can also reduce the backup time. When all of a client's files are in the same file list, NetBackup processes them serially, and this can take a long time when there are many files. If the files are divided between different policies, NetBackup can process the policies in parallel thus reducing the backup time. The maximum jobs attributes must be set to allow the parallel backups and sufficient system resources must be also available. (See "Setting the Number of Streams That Can Run Concurrently" on page 73 for an explanation of maximum jobs settings that also applies to this discussion.)

Note Understanding disk and controller I/O limitations is important when using multiple policies for a client. For example, if there are two file systems that will overload the client when backed up in parallel, place them in the same policy, schedule them at different times, or set **Maximum Jobs per Client** to 1.

Another way to reduce backup time is to use a single policy that has **Allow Multiple Data Streams** enabled and then add `NEW_STREAMS` directives to the file list. For example:

```
NEW_STREAM
file_a
file_b
file_c
NEW_STREAM
file_d
file_e
file_f
```

This produces two concurrent data streams. One has `file_a`, `file_b`, and `file_c`. The other has `file_d`, `file_e`, and `file_f`. (See "Allow Multiple Data Streams" on page 70.)

Note For best performance, use only one data stream to back up each physical device on the client. Multiple concurrent streams from a single physical device can adversely affect backup times, because the heads must move back and forth between tracks containing files for the respective streams.

The Files tab contains a list of files and directories that NetBackup includes in automatic backups of clients covered by a policy. You may also enter a file list *directive* that causes NetBackup to perform specific actions when processing the files in the list.

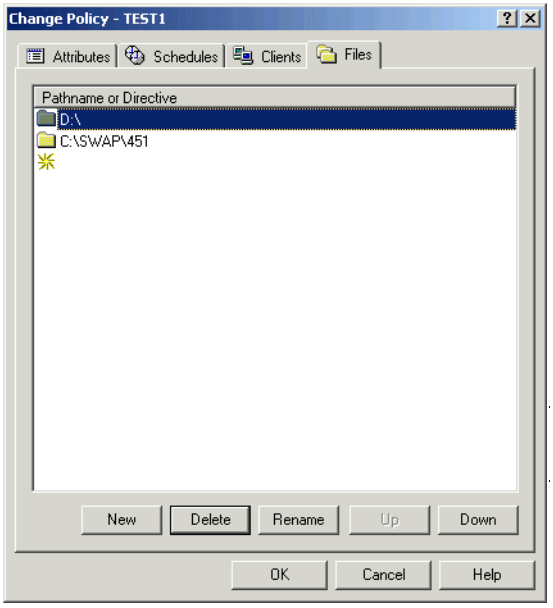
▼ To edit the file list on the Files tab

Note If you are setting up the file list for clients that have NetBackup database agents installed, see the NetBackup guide for the database agent for instructions.

1. In the NetBackup Administration window, expand **Master Server** > **NetBackup Management** > **Policies**.

2. Double-click the policy name in the left pane where you wish to change the file list. The Change Policy dialog appears.

3. Select the Files tab. The title bar shows the policy name.



4. If you are unfamiliar with how to specify file paths for your clients, see:
   - For UNIX clients, see “File-Path Rules for UNIX Clients” on page 92.
   - For PC clients, see “File-Path Rules for Microsoft Windows Clients” on page 83.

Note Path names can have up to 1023 characters.

5. Make required additions and changes as explained in the following topics. Then, verify the file list as explained in “Verifying the File List” on page 81.

6. Add a pathname or directive, if desired. (See “To add a pathname or directive” on page 80.)

7. Click **OK** to save the changesand close the Change Policy dialog.

Adding Directives to the File List

The directives you can use for a policy depend on the policy type. Select the directives by clicking in the **Directive** box and selecting from the list.

Some separately-priced NetBackup options come with one or more templates that contain directives that apply only to the policy types you configure for that option. If two or more templates are installed, the Select Directive dialog also contains a **Directive Set** text box where you can select the template that has the directives you want to use. For example, there can be basic and advanced sets. After you select a template, its directives are available in the **Directive** box.

For information on what directives accomplish, see "File List Directives: General Discussion" on page 98 and "File List Directives for Multiple Data Streams" on page 100 (if the **Allow Multiple Data Streams** general policy attribute is enabled). For separately-priced options, also see the NetBackup guide that came with the option.

▼ To add a pathname or directive

1. In the NetBackup Administration window, expand **Master Server** > **NetBackup Management** > **Policies**.

2. Double-click the policy name in the left pane where you wish to change the file list.

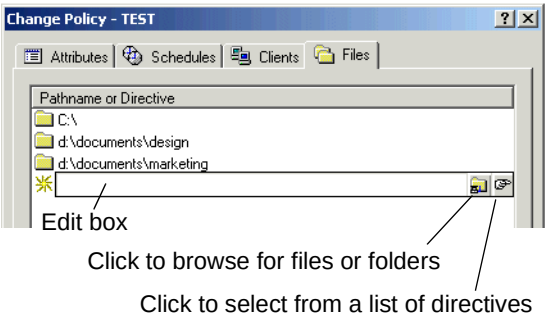
3. In the Change Policy dialog, select the Files tab.

4. To add an entry at the end of the list, click the **New** button.

5. In the Pathname or directive list:

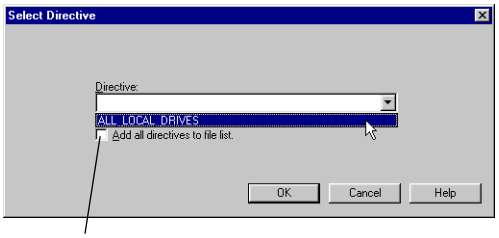
   - To add a path, type the name of the path in the edit box or browse for a file or folder by clicking the folder icon to the right of the edit box.

     Press Return to exit the edit box.



- To add a directive, click the pointer icon to the right of the edit box. Clicking the pointer icon opens the Select Directive dialog.

  Click the arrow next to the Directive field and select a directive. Click **OK** to include the directive to the file list on the Files tab.



If you are using many directives, it can be useful to add the entire set and then edit the file list to move and delete directives as required

6. To change the file list:
   - To move an entry, select the entry, then use the **Up** and **Down** buttons, mouse or keyboard.
   - To delete an entry, select the entry and click **Delete**.
   - To rename an entry, select it and click **Rename**. An edit box opens around the entry in order to modify it.

Verifying the File List

After creating or modifying a file list, complete the following procedure to make sure that the file-path rules for the specified clients are correct.

▼ To verify a file list

1. Check all entries to ensure you have followed the file-path rules for the clients you are backing up. Also, verify the syntax for any directives that are included in the list.

2. For the first set of backups, check the Problems or All Log Entries reports for warning messages (see examples below) and run the `check_coverage` script (located in *install_path*`\NetBackup\bin\goodies`).

   This step can reveal mistakes that result in not backing up files because the files are not found. The status code for a backup does not always indicate an error of this nature because NetBackup does not require all paths in the file list to be present on all clients. This allows you to have a generic list that multiple clients can share. Requiring all entries to match for a successful backup would result in more policies, unless all clients had identical filesystems.

If a path is not found, NetBackup logs a trivial (TRV) or warning (WRN) message, but can still end the backup with a status code 0 (success). This is desirable because it eliminates error status codes for files that are not expected to be on a client. However, it means you must check the logs or use the `check_coverage` script to ensure that files are not missed due to bad or missing file list entries.

The following example shows a log message that appears when files are not found. For information on using `check_coverage`, see the comments in the script.

Example

Assume the file list contains a path named C:`\worklist` that is not present on all clients. Here, NetBackup backs up C:`\worklist` on the clients where it exists. For other clients, the Backup Problems or All Log Entries report shows a message similar to the following:

```
9/1/00 8:28:17 AM carrot freddie Info from client freddie: TRV -
object not found for file system backup: C:\worklist
```

This message would also occur if C:`\worklist` were not the correct path name. For example, if the directory name is C:`\worklists` but you typed C:`\worklist`.

Note If the paths seem correct and the message still appears, ensure there are no trailing spaces in the paths.

Rules for Backup File Paths

The following topics explain the rules for specifying backup file paths for each type of NetBackup client:

- File-Path Rules for Microsoft Windows Clients
- File-Path Rules for OS/2 Clients
- File-Path Rules for NetWare NonTarget Clients
- File-Path Rules for NetWare Target Clients
- File-Path Rules for Macintosh Clients
- File-Path Rules for Clients Running Extension Products
- File-Path Rules for UNIX Clients

File-Path Rules for Microsoft Windows Clients

The following describes the conventions to use when specifying backups for Microsoft Windows clients.

File Backups

Enter one pathname per line.

- Start all pathnames with the drive letter followed by a colon (:) and a backslash (\). The drive letter can be either upper or lower case.

  `c:\`

- Precede each component in the path with a backslash.

  If the last component in the path is a directory, also follow it with a backslash (\). The trailing backslash is not required but serves as a reminder that the file path is a directory instead of a file.

  `c:\users\net1\`

  If the last component is a file, include the file extension and omit the backslash from the end of the name.

  `c:\special\list.txt`

- Upper and lower case letters in the pathname must match those in the actual pathname on the client. The only exception is the drive letter, which can be either upper or lower case.

  `c:\Worklists\Admin\`

- You can use the same wildcard characters as in Windows NT/2000 pathnames:

  ```
  *
  ?
  ```

  The following backs up all files ending with .doc

  ```
  c:\Users\*.doc
  ```

  The following backs up all files named `log01_97`, `log02_97`, and so on.

  ```
  c:\system\log??_97
  ```

- To back up all local drives except for those that use removable media, specify:

  `:\` or `*:\`

  The drives that are not backed up include: floppy disks, CD-ROMs and drives that are located on remote systems but mounted on your system through the network.

The following is an example file list that uses the Microsoft Windows conventions:

```
c:\
d:\workfiles\
e:\Special\status
c:\tests\*.exe
```

Using UNIX Conventions

NetBackup permits you to use UNIX conventions in the file list for Windows clients. This is convenient if your configuration has mainly UNIX clients and you are more comfortable with UNIX conventions.

The rules for the UNIX conventions are the same as explained for Microsoft Windows clients, except that you:

- Start each line with a forward slash (/).
- Omit the colon (:) after the drive letter.
- Specify / to back up all local drives except for those that are removable:

  ```
  /
  ```

The following example uses the UNIX conventions:

```
/c/
/d/workfiles/
/e/Special/status
/c/tests/*.exe
```

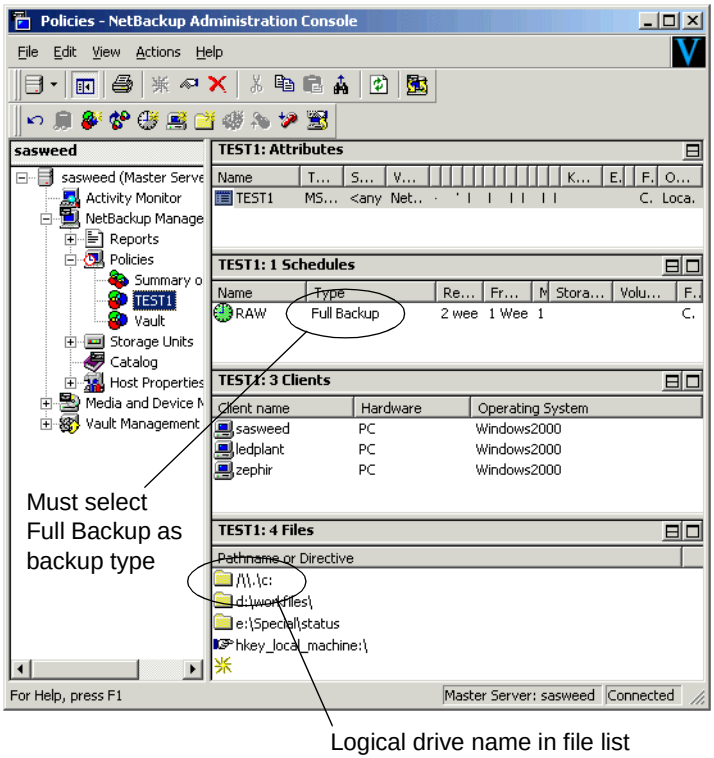
Windows Disk-Image (raw) Backup

On Windows NT/2000 clients, you can back up a logical disk drive as a disk image. That is, NetBackup backs up the entire logical drive on a bit-by-bit basis rather than by directories and files.

When performing a disk-image backup, be sure to select **Full Backup** for the backup type. Any other backup type will not work for backing up a disk-image.

To specify a disk-image backup, add the logical name for the drive to the policy file list. The form in the example would back up drive C.

Disk-images can be included in the same file list with other backups.



Note Before starting a disk-image backup, NetBackup locks the logical drive to ensure that no changes occur during the backup. If there are open files on the logical drive, a disk-image backup is not performed.

Note Before backing up or restoring a disk-image, all applications that use a handle to the partition must be shut down, otherwise the operation will fail. Examples of such applications are Windows Explorer or Norton Antivirus.

To restore the backup, the user first chooses **Select for Restore** > **Restore from Normal Backup**.

When a user lists the backups from which it can choose, the disk image appears as a file with the same name that was specified in the file list. In this example:

```
\\.\c:
```

After selecting the disk image source, the user enters the destination in the following format:

`/\\.\`*drive*`:`

Where *drive* is the location where the partition will be restored. The leading forward slash is important. For details, see the *NetBackup User's Guide for Microsoft Windows*.

Microsoft Windows Registry Backup

Backup for Disaster Recovery

To ensure successful recovery in case of a disk failure, always back up the entire registry. That is, back up the directory that contains the entire registry.

- On Windows NT/2000, this directory is

  `%systemroot%\system32\config`

- On Windows 98 or 95, this directory is

  `%systemroot%`

Where `%systemroot%` is the directory where Windows is installed.

For example, if Windows NT is installed in the `c:\winnt` directory, then including any of the following paths will accomplish the backup

`c:\winnt\system32\config` (backs up the entire `config` directory)

`c:\` (backs up the entire C drive)

`:\` (backs up all local drives except those that are removable)

Caution To ensure a successful recovery of the registry in case of disaster, *do not* include individual registry files or HKEY entries in the same file list that is used to back up the entire registry. If you are using a NetBackup exclude list for a client, do not exclude any registry files from your backups.

See the Disaster Recovery chapter in the *NetBackup Troubleshooting Guide - Windows* for instructions on restoring the registry in the case of a disk failure.

Back Up Individual HKEYs (do not use for disaster recovery)

As mentioned above, do not include HKEY entries in the same policy file list used to back up the entire registry. However, if you want the ability to restore individual keys within the registry, create a separate policy and then specify the desired HKEYs in the file list for that policy. The following is an example HKEY entry for a policy file list:

```
HKEY_LOCAL_MACHINE:\
```

Remember, you cannot perform a disaster recovery by restoring HKEYs. In addition, backups and restores will also be slower than backing up the registry as a whole.

Hard Links to Files (NTFS volumes only)

A hard link is a directory entry for a file. Every file can be considered to have at least one hard link. On NTFS volumes, each file can have multiple hard links; therefore, a single file can appear in many directories (or even in the same directory with different names). The actual file is indicated by a Volume Serial Number (VSN) and a File Index which is unique on the volume. Collectively, the VSN and File Index are referred to as the file ID.

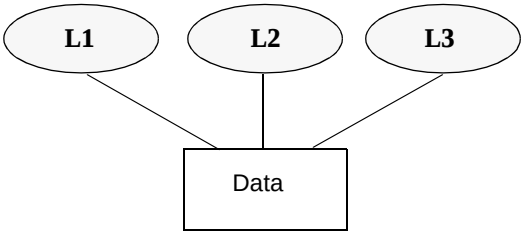
During a backup, if the file list includes hard-linked files, the data is backed up only once, using the first file name reference found in the directory structure. If a second or subsequent file name reference is found, it is backed up as a link to the name of the first file. This means you get only one backup copy of the data, regardless of whether you include one or multiple hard links. You can include any of the paths that are hard links to the data in order to back up the data.

During a restore, if all of the hard-link references are restored, the hard-linked files still point to the same file ID as the other files to which they are linked. However, if you do not restore all the hard links, you can encounter anomalies as shown in the following examples.

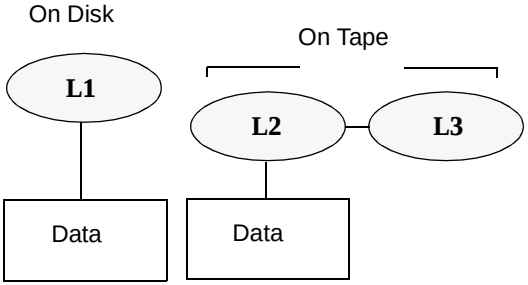
Example 1

Assume there are three hard links named L1, L2, and L3 that are pointing to the same data.

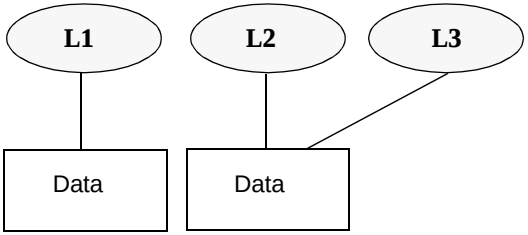
1. The three files are all hard linked to the same data.



2. L2 and L3 are backed up to tape and then deleted from the disk.



3. When L2 and L3 are restored, the data cannot be associated with the original file and are assigned a new file ID.



1. During a backup of L2 and L3, L2 is encountered first and backed up, then L3 is backed up as a link to L2.

2. Next, the original copies of L2 and L3 are both deleted, leaving only L1 on the disk.

3. During a subsequent restore, you restore L2 and L3. The restored files, however, do not point to the same file ID as L1. Instead, they are assigned a new file ID number and the data is written to a new place on the disk. The data in the new location is an exact copy of what is in L1. The duplication occurs because the backup does not associate L2 and L3 with L1.

Example 2

Assume in example 1, that you attempt to restore only L3. Here, NetBackup cannot link L3 to L2 because L2 does not exist. Since the restore can complete only if it can link to L2, L2 is automatically restored by a secondary restore request to the NetBackup server that has the data. If you restore L2 by itself, there is no problem.

File-Path Rules for OS/2 Clients

The requirements for OS/2 clients are the same as for Microsoft Windows clients.

File-Path Rules for NetWare NonTarget Clients

For NetWare systems that are running the NonTarget version of NetBackup client software, specify the pathnames in the form:

/SMDR/TSA/TS/resources/directory/file

Where:

- *SMDR* (Storage Management Data Requestor) is the name of the NetWare file server that is running the SMDR.NLM used for backups. (NLM means NetWare-loadable module.)
- *TSA* (Target Service Agent) is a NetWare software module that prepares the data for back up or restore by the SMDR. There are different types of TSAs, depending on the data. For example, there are TSAs for NetWare file systems and DOS workstations.
- *TS* is the Target Service, which is the NetWare entity that has the data being handled by the selected TSA. For example, with the DOS TSA (tsasms.com) it is a DOS Workstation. In the case of a NetWare file system TSA, it is the system with the NetWare file systems to be backed up.
- *resources* are the specific resources on the target service. For example, it can be NetWare file systems such as BINDERY, SYS, and USER.
- *directory/file* is the directory and file that are in the resource (if it is a path to a specific file).

Observe the following rules for paths:

- Give the server access to each path or the scheduled backup will fail. To provide this access, use the **Allowed Scheduled Access** command on the Backup menu in the NetBackup interface on the NetWare client. For more information, see the *NetBackup User's Guide NonTarget Version - Novell NetWare*.
- Enter one pathname per line.
- Start all pathnames with a slash (/).

- Precede each component in the path with a slash.

  If the last component in the path is a directory, follow it with a slash (/). The trailing slash is not required but is a reminder that the file path is a directory instead of a file.

  ```
  /TILE/TILE.NetWare File System/TILE/SYS/DOC/
  ```

  If the last component is a file, include the file extension and omit the slash from the end of the name.

  ```
  /TILE/TILE.NetWare File System/TILE/SYS/DOC/TEST.TXT
  ```

- All components in a path name must show upper and lower case letters as they appear in the actual pathname on the client.
- Wildcard usage is the same as when specifying files for Windows NT clients.
- To back up all NetBackup for NetWare clients that are in this policy, enter a slash (/) by itself on a line.

  ```
  /
  ```

- To back up an entire NetBackup for NetWare client, enter a slash (/) followed by the client name and a slash.

  ```
  /TILE/
  ```

The following example backs up `SYS`, `BINDERY`, and `USER` file systems under the file system TSA on the client named tile:

```
/TILE/TILE.NetWare File System/TILE/SYS/
/TILE/TILE.NetWare File System/TILE/BINDERY/
/TILE/TILE.NetWare File System/TILE/USER/
```

Note that the **Allowed Scheduled Access** command on the **Backup** menu in the NetBackup interface on the NetWare client must also specify access to these paths. See the *NetBackup User's Guide NonTarget Version - Novell NetWare*.

File-Path Rules for NetWare Target Clients

For NetWare clients that are running the target version of NetBackup client software, use the following format for the file paths:

/*target*/

Where *target* is the name of a target defined on the NetBackup for NetWare client (see the *NetBackup User's Guide for Novell NetWare Target*).

- Enter one target per line.
- Start all target names with a slash (/).
- All target names must be in upper case.

- Wildcard usage is the same as for Windows NT clients.

The following example backs up the targets: `NETWARE`, `SYSTEM`, and `BINDERY`:

```
/NETWARE/
/SYSTEM/
/BINDERY/
```

File-Path Rules for Macintosh Clients

The following explains how to map your Macintosh file and folder names to the names required in the policy file list. Other syntax rules are also explained.

- Enter one pathname per line.
- Specify the Macintosh paths as follows:

  /*volume*/*folders* ... /*file*

  Where:

  - *volume* is the name of the Macintosh volume (disk) where the data is located.

    The first directory in the pathname is always the volume. It is a good idea to use a wildcard (*) in place of the volume because the Macintosh hard disk name is not necessarily the same on each client.

  - *folders* are the names of the Macintosh folders that contain the files to be backed up. If there are multiple folders in the path, separate the names with slashes. The Macintosh folder names map to folders in a Windows path.

  - *file* is the Macintosh file name. Macintosh file names map to the file name in a Windows path.

- Precede each component in the path with a slash.

  If the last component in the path is a directory, follow it with a slash (/). The trailing slash is not required but serves as a reminder that the file path is a directory instead of a file.

  ```
  /Macintosh HD/Graphics/
  ```

  If the last component is a file, include the file extension and omit the slash from the end of the name.

  ```
  /Macintosh HD/Graphics/Checklist
  ```

- Upper and lower case letters in the pathname must match those in the actual pathname on the client.

  ```
  /Macintosh HD/Graphics/
  ```

- Macintosh file and folder names can contain the space character.

- Wildcard usage is the same as for Windows clients. For example:

  `/*/BackMeUp`

  This example refers to the folders or files named `BackMeUp` at the top level of all the mounted volumes on the Macintosh. To specify all mounted volumes on the Macintosh, use:

  `/*`

- Any slash (/) character in a Macintosh file or folder name, maps to a colon (:) character in the pathname on the master server.

  For example, assume there is a file named `Notes 95/09/30`, in the `My Stuff` folder, on the hard disk named `Macintosh HD`. To include this file in automatic backups, specify the following in the file list for the policy:

  `/Macintosh HD/My Stuff/Notes 95:09:30`

Example 1

The following backs up a Macintosh file named `Bldg Layout`, that is in the folder named `New Stuff`, which is in the folder named `Graphics` on the hard disk named `Macintosh HD`.

The following entry adds the `Bldg Layout` file to your backups:

```
/Macintosh HD/Graphics/New Stuff/Bldg Layout
Macintosh HD is the volume, Graphics and New Stuff are folders, and
Bldg Layout is a file.
```

Example 2

The following backs up a folder named `My Stuff` on the hard disk named `Macintosh HD`.

```
/Macintosh HD/My Stuff/
```

File-Path Rules for Clients Running Extension Products

File-path rules for NetBackup clients that are running separately-priced extension products, such as Flashbackup or NetBackup for MS-Exchange, are covered in the NetBackup guide for the extension product.

File-Path Rules for UNIX Clients

The general requirements for pathnames on UNIX clients are as follows:

- Enter one pathname per line. NetBackup supports a maximum path length of 1023 characters on UNIX clients.
- Start all pathnames with a slash (/).
- You can use the following meta or wildcard characters in policy file lists:

  ```
  *
  ?
  [ ]
  ```

  The following are example UNIX file specifications that use this capability:

  ```
  /home/.[a-zA-Z0-9]*
  /etc/*.conf
  ```

- To use meta or wildcard characters literally, precede them with a backslash (\). Assume, for example, that the brackets in the following pathname are used as literal characters:

  ```
  /home/abc/fun[ny]name
  ```

  In the file list, precede the brackets with a backslash as in

  ```
  /home/abc/fun\[ny\]name
  ```

Note A backslash (\) acts as an escape character only if it precedes a meta or wildcard character. NetBackup normally interprets a backslash literally and it is a legal character to use in pathnames.

The following topics provide more information on specifying UNIX file paths to back up.

Notes on File Lists for UNIX Clients

- File paths that cross mount points or that the client mounts through NFS can affect the way that you must configure your backups. Before creating a file list, familiarize yourself with the **Cross mount points** attribute. (Note that only NetBackup DataCenter can back up NFS mounted files.)
- You can back up operating system, kernel, and boot files with NetBackup. You cannot, however, create bootable tapes. Consult your system documentation to create a bootable tape.
- NetBackup never backs up the following:
  - Files or directories in a different file system if you do not set **Cross mount points**.
  - Files or directories with path lengths longer than 1023 characters.
  - Files or directories where the operating system does not return inode information (the `lstat` system call failed).

- Directories that NetBackup cannot `cd` into.
- On a disk managed by Storage Migrator, migrated files or directories where Storage Migrator does not return inode information (`mig_stat` fails). Note that NetBackup BusinesServer does not support Storage Migrator.
- Socket special files (named pipes are backed up).
- Locked files when mandatory locking is enabled by an application that currently has the file open.
- Busy files. If a file is open, NetBackup backs up the last saved version of the file.

◆ Exclude specific files from backups by creating an exclusion list on the client.

◆ On Hewlett-Packard, AIX, Sequent, and Solaris 2.5 (and later) platforms, NetBackup backs up access control lists (ACLs).

◆ NetBackup can back up (and restore) Sun PC NetLink files.

◆ On IRIX 6.x and Digital Alpha platforms, NetBackup backs up extended file attributes.

◆ On IRIX platforms, NetBackup backs up and restores extended attributes attached to XFS file system objects.

◆ On DEC OSF/1 platforms, NetBackup backs up and restores extended attributes attached to files on AdvFS and UFS file systems.

◆ On Hewlett-Packard and Solaris 2.5 (and later) platforms, NetBackup backs up VxFs extent attributes.

◆ If there are one or more trailing spaces in a file list entry and a matching entry is not found on the client, NetBackup deletes trailing spaces and checks again. If a match is still not found, NetBackup skips the entry and logs a message similar to one of the following in the NetBackup All Log Entries or Problems report:

```
TRV - cannot process path pathname: No such file or directory.
Skipping
TRV - Found no matching file system for pathname
```

Symbolic Links to Files or Directories

For symbolic (soft) links, include the file path to the source file in your list in order to back up the actual data. If a file is a symbolic link to another file, NetBackup backs up only the link, not the file to which the link points. This prevents multiple backups of the source file.

Because symbolic links are restored only as a symbolic link to the source file, you must restore the source file along with the link in order to get the data.

Note If NetBackup restores a symbolic link as root, it changes the owner and group back to the original owner and group. When NetBackup restores a UNIX symbolic link as a nonroot user, it sets the owner and group for symbolic links to the owner and group of the person doing the restore. This does not cause problems because when the UNIX system checks permission it uses the owner and group of the file to which the symbolic link points.

Hard Links to Directories

On most UNIX systems, only the root user can create a hard link to a directory. Some systems do not permit hard links and many vendors warn you to avoid using these links.

NetBackup does not back up and restore hard-linked directories in the same manner as it does files:

- During a backup, if NetBackup encounters hard-linked directories, it backs them up multiple times, once for each hard link.
- During a restore, NetBackup restores multiple copies of the hard-linked directory contents if the directories do not already exist on the disk. If the directories exist on disk, NetBackup restores the contents multiple times to the same disk location.

Hard Links to Files

A hard link differs from a symbolic link in that it is not a pointer to another file, but is actually two directory entries pointing to the same inode number.

During a backup, if the file list includes hard-linked files, the data is backed up only once, using the first file name reference found in the directory structure. If a second or subsequent file name reference is found, it is backed up as a link to the name of the first file. This means you get only one backup copy of the data, regardless of whether you include one or multiple hard links. You can include any of the paths that are hard links to the data in order to back up the data.

During a restore, if all of the hard-link references are restored, the hard-linked files still point to the same inode as the other files to which they are linked. However, if you do not restore all the hard links, you can encounter anomalies as shown in the following examples.

Example 1

Assume there are three hard links named L1, L2, and L3 that are pointing to the same data.

1. During a backup of L2 and L3, L2 is encountered first and backed up, then L3 is backed up as a link to L2.

2. Next, the original copies of L2 and L3 are both deleted, leaving only L1 on the disk.

3. During a subsequent restore, you restore L2 and L3. The restored files, however, do not point to the same inode as L1. Instead, they are assigned a new inode number and the data is written to a new place on the disk. The data in the new location is an exact copy of what is in L1. The inode duplication occurs because the backup does not associate L2 and L3 with L1.

Example 2

Assume in example 1, that you attempt to restore only L3. Here, NetBackup cannot link L3 to L2 because L2 does not exist. The restore therefore fails and you see an error message in the progress log. If you restore L2 by itself, there is no problem.

UNIX Raw Partitions

Caution Save a copy of the partition table before performing raw-partition backups so you have it for reference prior to a restore. To restore the raw partition, a device file must exist and the partition must be the same size as when it was backed up. Otherwise, the results of the restore are unpredictable.

Notes On UNIX Raw-Partition Backups

- Use raw-partition backups only if you can ensure that the files are not changed in any way during the backup or, in the case of a database, if you can restore the database to a consistent state by using transaction log files.
- Do not perform archives of raw partitions on any client. An archive backs up the raw partition and then deletes the device file associated with the raw partition. However, the file system does not recover the space used by the raw partition.
- Before backing up file systems as raw partitions, unmount the file system to allow buffered changes to be written to the disk, and to prevent the possibility of the file system changing during the backup. You can use the `bpstart_notify` and the `bpend_notify` scripts to unmount and remount the backed-up file systems.
- The **Cross Mount Points** attribute has no effect on raw partitions. If the root partition is being backed up as a raw partition and has mount points for other file systems, the other file systems are not backed up, even if you select **Cross Mount Points**.
- For disks managed by disk volume managers such as VERITAS VxVm, specify the logical partition names.

- For clients in a FlashBackup policy, refer to the *NetBackup FlashBackup System Administrator's Guide* (file list and cache section) for the differences between Standard and FlashBackup policies.

When to Use Raw-Partition Backups

If there are no file systems to back up and the disks are used in raw mode (such as with some databases), back up the disk partitions as raw partitions. When backing up databases as raw partitions, you can use the `bpstart_notify` and `bpend_notify` scripts to do the preprocessing and postprocessing necessary to back up the databases.

You can also perform a raw-partition backup of a disk partition used for file systems. A disadvantage of this method is that you must restore the entire partition to recover a single file (unless you are using FlashBackup). To avoid overwriting the entire partition, use the redirected restore feature to restore the raw partition to another raw partition of the same size, and then copy individual files to the original file system.

Raw-partition backups are also useful for backing up entire disks. Since the overhead of the file system is bypassed, a raw-partition backup is usually faster. The size of the raw-partition backup will be the size of the entire disk, regardless of whether the entire disk is used.

Specifying UNIX Raw Partitions in the File List

To specify a UNIX raw partition in the policy file list, enter the full path name of the device file. For example, on Solaris:

```
/devices/sbus@1,f8000000/esp@0,800000/sd@2,0:1h
```

Caution Do not specify wildcards (such as `/dev/rsd*`) in paths for raw-partition backups. Doing so can prevent the successful restore of entire devices, if there is overlap between the memory partitions for different device files.

You can include raw partitions in the same file list as other backups. For example:

```
/home
/usr
/etc
/devices/sbus@1,f8000000/esp@0,800000/sd@2,0:1h
```

Note NetBackup does not distinguish between full and incremental backups when backing up a raw partition. The whole partition is backed up in both cases.

Raw-partition backups occur only if the absolute file path in the file list is a block or character special-device file. You can specify either block or character special-device files; although, character special-device files are often faster because they avoid going through

the file system to access disk data. To obtain the optimum backup speed for raw-partition backups, test both a block and character special-device file to ensure the best choice for your platform.

Ensure that you are specifying the actual block- or character-device files. Sometimes, these are links to the actual device files. If a link is specified, only the link is backed up. If the device files are reached while backing up `/dev`, NetBackup backs up only the inode files for the device, not the device itself.

Selecting a Schedule Backup Type for a UNIX Raw Partition

When performing a raw partition backup, be sure to select **Full Backup** for the Type of Backup from the Schedules tab. Any other backup type will not work for backing up raw partitions. (See “Type of Backup” on page 110.)

File List Directives: General Discussion

The file list for a policy can contain directives that cause NetBackup to perform specific actions when processing the files in the list.

The directives that are available depend on the policy type and whether the **Allow Multiple Data Streams** attribute is enabled for the policy. The following is an example of a file list that contains the `NEW_STREAM` directive and is for an MS-Windows-NT policy that has **Allow Multiple Data Streams** enabled:

```
NEW_STREAM
D:\Program Files
NEW_STREAM
C:\Winnt
```

The purpose of the above example is to show how directives look in a file list. The actions that the `NEW_STREAM` directive causes is explained in “File List Directives for Multiple Data Streams” on page 100.

The rules for specifying backup paths in the file list apply regardless of whether directives are used.

ALL_LOCAL_DRIVES Directive

The `ALL_LOCAL_DRIVES` directive applies to the following policy types:

- Standard (except for NetWare target clients)
- MS-Windows-NT
- NetWare (NonTarget clients only)
- OS/2

An exception to the above is that you cannot use `ALL_LOCAL_DRIVES` for NetWare and OS/2 policy types if you are also using **Allow Multiple Data Streams**. (See "ALL_LOCAL_DRIVES" on page 104.)

SYSTEM_STATE Directive

The `System_State:\` directive is only a valid directive when backing up Windows 2000/XP machines. If the machine is not one of these, then `System_State:\` will not have any effect. If the machine is Windows2000\XP, the list of items that get backed up can include:

- Active Directory
- COM+ Class Database
- Cluster Database
- IIS Database
- Registry
- Boot Files and Protected Files
- SYSVOL
- Certificate Server

On a NT machine, the registry gets backed up in the process of regular file system backups. The files the comprise the registry can be found under the following:

```
%SystemRoot%\SYSTEM32\Config
```

At a minimum, the following files are backed up as part of the registry:

- DEFAULT
- SAM
- SOFTWARE
- SECURITY
- SYSTEM

Directives for Multiple Data Streams

If the **Allow Multiple Data Streams** general attribute is set for a policy, you can use the following directives in the file list:

- `NEW_STREAM`
- `ALL_LOCAL_DRIVES`

- UNSET
- UNSET_ALL

The rules for using these directives are explained in “File List Directives for Multiple Data Streams” on page 100.

Directives for Specific Policy Types

Some directives apply only to specific policy types and can appear only in file lists for those policies. NetBackup passes policy-specific directives to the clients along with the file list. The clients then perform the appropriate action according to the directive. The policy types that currently have their own file list directives are:

- NDMP
- Lotus-Notes
- MS-Exchange-Server

The above policy types can be used only when their separately-priced option is installed. For information on these policies and their file list directives, see the NetBackup guide for the option.

Caution Include policy-specific directives only in file lists for the policies that support them or errors can occur.

File List Directives for Multiple Data Streams

If the **Allow Multiple Data Streams** general attribute is set for the policy, the following directives can be used in the file list to control the way that NetBackup creates backup streams:

- “NEW_STREAM”
- “ALL_LOCAL_DRIVES”
- “UNSET and UNSET_ALL”

Note For best performance, use only one data stream to back up each physical device on the client. Multiple concurrent streams from a single physical device can adversely affect backup times because the heads must move back and forth between tracks containing files for the respective streams.

NEW_STREAM

The NEW_STREAM directive is recognized only if **Allow Multiple Data Streams** is set for the policy. NEW_STREAM directives are ignored if **Allow Multiple Data Streams** is not set.

If this directive is used in a file list, the first instance of it must be on the first line. If it appears on the first line, it can also appear elsewhere in the list.

The presence or absence of NEW_STREAM on the first line of the file list determines whether the backup is performed in *administrator-defined* streaming or *auto-discover* streaming mode.

Administrator-defined Streaming Mode

If NEW_STREAM is on the first line of the file list, the backup is performed in administrator-defined streaming mode and the following occurs:

- The backup is split into a separate stream at each point in the file list where the NEW_STREAM directive occurs.
- All file paths between NEW_STREAM directives are in the same stream.
- The end of each stream is defined by the start of a new stream (that is, a NEW_STREAM directive).
- The last stream in the file list is terminated by the end of the file list.

Note In the following examples, we assume that each stream is from a separate physical device on the client. Multiple concurrent streams from a single physical device can adversely affect backup times because the heads must move back and forth between tracks containing files for the respective streams.

For example, consider the file list below:

```
NEW_STREAM
D:\Program Files
C:\Winnt
NEW_STREAM
C:\users
D:\DataFiles
```

This file list has two data streams.

- The NEW_STREAM at the top of the list invokes administrator-defined streaming and starts the first data stream. This stream backs up D:\Program Files and C:\Winnt.
- The second NEW_STREAM starts a second data stream that backs up C:\users and D:\DataFiles.

If you add a file list entry as part of an existing stream, its first backup is according to the next schedule that is due for the policy. If the next backup due is an incremental, then only changed files are backed up. To ensure that a new entry gets a full backup the first time, add it to a new stream. NetBackup performs a full backup of new streams that are added to the file list.

In the previous example, assume you add `D:\Utilities` after `D:\Datafiles`. If an incremental is due that evening, only changed files in `D:\Utilities` are backed up. However, if you add a `NEW_STREAM` directive before `D:\Utilities`, then NetBackup performs a full backup of all files in `D:\Utilities`, regardless of when they were last changed.

Auto-discover Streaming Mode

Auto-discover streaming mode is invoked if `NEW_STREAM` is not the first line of the file list *and* the list contains either the `ALL_LOCAL_DRIVES` directive or wild cards. In this mode, the file list is sent to the client, which preprocesses the list and splits the backup into streams as follows:

- If the file list contains the `ALL_LOCAL_DRIVES` directive, NetBackup backs up the entire client but splits each drive volume (Windows NT) or file system (UNIX) into its own backup stream. See “ALL_LOCAL_DRIVES” on page 104.
- If wild cards are used, the expansion of the wild cards results in one stream per wild card expansion.

If the file list contains neither the `ALL_LOCAL_DRIVES` directive nor wildcards, auto-discover mode is not used and preprocessing is done on the server rather than the client. In this case, each file path in the file list becomes a separate stream.

Auto-discover streaming mode applies to:

- Standard and MS-Windows-NT policy types, except for Macintosh and NetWare clients.
- Clients that are running NetBackup 3.2 or later.

With auto discover, the client determines how many streams are required by preprocessing the file list before the backup begins. The first backup of the policy always includes preprocessing. However, preprocessing does not necessarily occur before every backup and whether it occurs depends on the preprocess interval.

Setting the Preprocess Interval for Auto Discovery

The preprocess interval applies only to auto-discover mode and specifies how often preprocessing occurs. When a schedule is due and auto discovery is used, NetBackup checks whether the previous preprocessing session occurred within the preprocess interval:

- If yes, NetBackup does not run preprocessing on the client.
- If no, NetBackup runs preprocessing on the client and makes required changes to the streams.

If necessary, you can change the interval by using the `bpconfig` command. The default is four hours and is a good value for most sites that run daily backups. If the interval is too long or too short, the following can occur:

- Too long an interval can result in new streams not being added soon enough and backups can be missed. For example, assume the preprocess interval is set to four hours and a schedule has a frequency of less than four hours. Here, it is possible for a new stream to be omitted from the next backup because the preprocessing interval has not expired when the backup is due.
- Too short an interval can cause preprocessing to occur often enough to increase backup time to an unacceptable level. A short interval is most likely to be a problem when there are a large number of clients that the server must contact for preprocessing.

The form of the `bpconfig` command to use for changing the interval is:

install_path`\NetBackup\bin\admincmd\bpconfig` [`-prep` *hours*]

For example:

install_path`\NetBackup\bin\admincmd\bpconfig -prep 12`

You can set the preprocess interval for immediate preprocessing by specifying `-prep 0`. (Preprocessing occurs prior to every backup.) Specifying `-prep -1` sets the preprocess interval to the default value of 4 hours.

The following example sets the preprocess interval to 12 hours. You can determine the current interval by using the `bpconfig` command with the `-L` option:

```
bpconfig -L
```

(output of the above command)

```
Mail Admin:         *NULL*
Wakeup Interval:    9 minutes
Max Jobs/Client:    8
Backup Tries:       2 in 12 hours
Keep Logs:          3 days
Max drives/master:  0
Compress DB Files:  older than 10 days
Media Mnt Timeout:  0 minutes (unlimited)
Postprocess Image:  immediately
Display Reports:    24 hours ago
Keep TIR Info:      1 days
Prep Interval:      12 hours
```

Example - Auto-Discover Streaming Mode

Assume the file list has the following entries:

```
D:\Program Files
C:\Winnt
C:\Users\*
```

For this file list, NetBackup generates:

- One stream for the `D:\Program Files` directory
- One backup for the `C:\Winnt` directory
- One stream for each subdirectory and file in the `C:\Users\*` directory because of the wildcard (*)

  If the `C:\users\` directory has three subdirectories: `tom`, `dick`, and `harry`, but no files NetBackup produces a separate stream for each of them: `C:\users\tom`, `C:\users\dick`, and `C:\users\harry`. This is a total of five streams for the backup.

However, if the wildcard is removed from `/Users`, as in the following, then auto discover is not used.

```
D:\Program Files
C:\Winnt
C:\Users
```

In this mode, NetBackup generates only three streams, one for each of the directories in the list. Preprocessing is done on the server instead of the client.

ALL_LOCAL_DRIVES

The `ALL_LOCAL_DRIVES` directive applies only to Standard (except for NetWare target clients), MS-Windows-NT, NetWare, and OS/2 policies where the clients are running NetBackup 3.2 or later software. If used, this directive must be the only entry in the file list for the policy; that is, no other files or directives can be listed.

The action that the directive causes depends on whether you also enable **Allow Multiple Data Streams** for the policy.

- If **Allow Multiple Data Streams** is enabled, the `ALL_LOCAL_DRIVES` directive is valid only if the policy type is Standard (except for Macintosh and NetWare clients) or MS-Windows-NT. In this instance, NetBackup backs up the entire client and splits the data from each drive (Windows NT) or file system (UNIX) into its own backup stream. NetBackup periodically runs preprocessing on the client to make necessary changes to the streams. See “Setting the Preprocess Interval for Auto Discovery” on page 102.

- If **Allow Multiple Data Streams** is not enabled, NetBackup backs up the entire client and includes all drives and file systems in the same stream.

Caution Do not select **Cross Mount Points** for policies where you use the `ALL_LOCAL_DRIVES` directive.

Example 1

Assume **Allow Multiple Data Streams** is enabled in auto-discover mode and the client is a Windows NT system with two drive volumes, `C:\` and `D:\`. The file list contains:

```
ALL_LOCAL_DRIVES
```

For this file list, NetBackup generates:

- One stream for `C:\`
- One stream for `D:\`

For a UNIX client, NetBackup generates a stream for each file system.

Example 2

Assume **Allow Multiple Data Streams** is not enabled and the client is a Windows NT system with two drive volumes, `C:\` and `D:\`. The file list contains:

```
ALL_LOCAL_DRIVES
```

Here, NetBackup backs up the entire client in one data stream that contains the data from both `C:\` and `D:\`.

UNSET and UNSET_ALL

All policy-specific directives that are passed to a client in a stream are passed in all subsequent streams. (See “Directives for Specific Policy Types” on page 100.) The `UNSET` and `UNSET_ALL` directives change this behavior. These directives are recognized only if **Allow Multiple Data Streams** is set for the policy.

UNSET

Unsets a policy-specific directive so it is not passed with any additional streams. The directive that was unset can be defined again later in the file list and included in the current and later streams.

UNSET_ALL

`UNSET_ALL` has the same effect as `UNSET` but unsets all policy-specific directives that have been defined up to this point in the file list.

Example

Assume you have a file list as shown below. In this file list, the `set` command is a client-specific directive that is passed to the first and all subsequent streams.

```
NEW_STREAM
set destpath=/etc/home
/tmp
/use
NEW_STREAM
/export
NEW_STREAM
/var
```

If you want the `set` command passed to the first two streams but not the last, an `UNSET` or `UNSET_ALL` can be used at the beginning of the third stream to prevent it from being passed to the last stream.

```
NEW_STREAM
set destpath=/etc/home
/tmp
/use
NEW_STREAM
/export
NEW_STREAM
UNSET_ALL
/var
```

Excluding Files From Automatic Backups

On most NetBackup clients, you can exclude specific files from automatic backups by specifying them in an exclude list on the client. You can also create an include list to add back in some of the files by using an include list. The include list is useful, for example, if you want to exclude an entire directory except for one file.

Note Exclude and include lists do not apply to user backups and archives.

The method for specifying files in the exclude and include lists depends on the type of client that you are configuring.

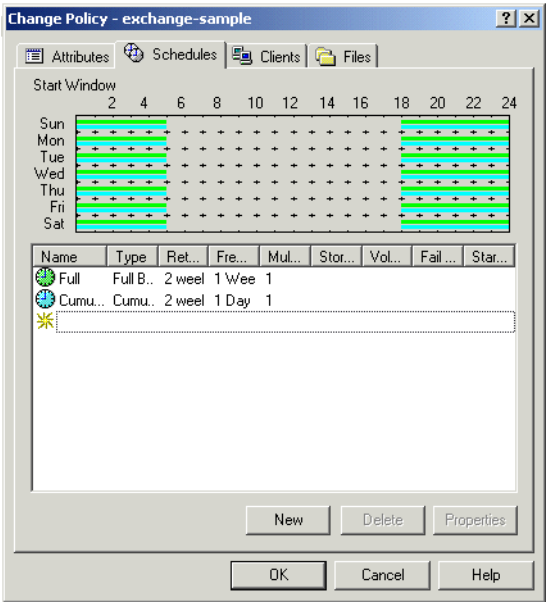
- On Microsoft Windows clients, specify exclude and include lists in the NetBackup Configuration dialog box in the Backup, Archive, and Restore client interface: Start Backup, Archive, and Restore and click **File** > **NetBackup Client Properties**. Go to the **Exclude List** or **Include List** tab. For further instructions, see the NetBackup user's guide for the client.

The **Exclude List** or **Include List** can also be specified through the NetBackup Administration Console on the master server. (See “Exclude Tab” on page 295 and “Include Tab” on page 297.)

- On NetWare target clients, the exclude and include lists are specified when adding the targets. See the NetBackup user’s guide for the client.
- Macintosh, and OS/2 clients do not support exclude and include lists.
- For UNIX clients, see “Exclude and Include Lists on UNIX Clients” on page 674.

Schedule Tab

The policy Schedules tab displays the different time schedules set up for the policy selected.



From the policy Schedules tab:

- Create a new schedule by clicking **New**.
- Double-click an existing schedule to edit the schedule or select the schedule and click Properties.

  Creating or editing a schedule causes another Schedule dialog to appear that contains three tabs: Attributes tab, Start Window tab, and Exclude Dates tab. If the **Calendar** schedule type is selected, a Calendar tab displays.
- Delete an existing schedule by selecting the schedule and clicking **Delete**.

Creating or Editing a Schedule on the Attributes Tab

When creating or editing a schedule, policy schedule attributes appear on three tabs. If the **Calendar** schedule type is selected, an additional tab displays:

- Attributes tab
- Start Window tab
- Exclude Dates tab
- Calendar Schedule Tab

▼ To create or change backup schedules

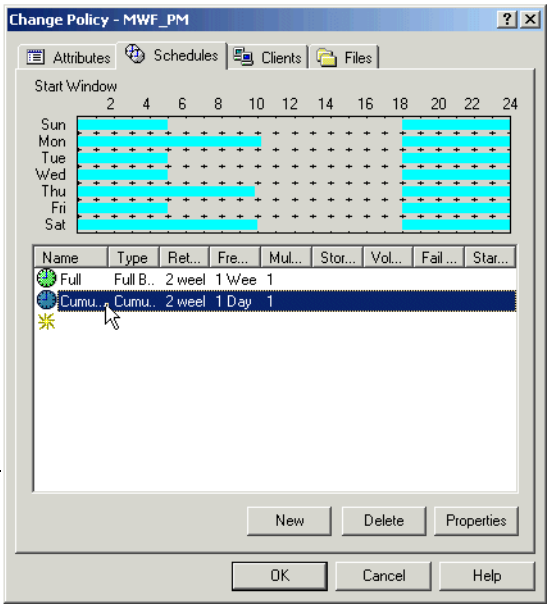
1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.
2. Double-click the policy name where you want to change or add a schedule. The **Change Policy** dialog appears.

3. Select the **Schedules** tab. The tab displays the Start Window and properties of existing schedules. The title bar displays the name of the current policy.

4. Select the schedule you wish to change and click **Properties**.

5. The Change Schedule dialog appears containing the **Attributes**, **Start Window**, and **Exclude Dates** tab.

6. Make your changes and click **OK**.

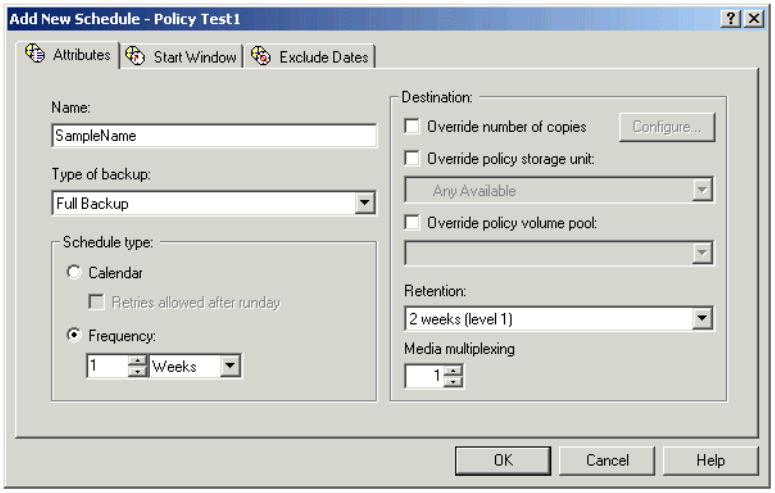


Note "To add or change schedules in a policy" on page 53 also provides information on changing existing policies.

Schedule Attributes Tab

The Attributes tab appears after double-clicking a schedule or clicking the **New** button in the Schedules tab and contains options that define the backup type, when the backup can occur, and how long the backup image is kept. Other attributes such as type of storage and volume pool can also be defined.

Name



Identifies the schedule and appears on screens and messages from NetBackup. Specify a name by typing in the box. The name must be unique and can contain alphabetic (ASCII A-Z a-z), numeric (0-9), plus (+), minus (-), underscore(_), or period (.) characters. Do not use a minus or period as the first character. Do not use a period as the first or last character. Do not or leave spaces between characters.

Type of Backup

Specifies the type of backup that this schedule will control. Click in the field and select from the drop-down list. The list displays only the backup types that apply to the policy you are configuring.

The following is a complete list of possible selections:

- **Full Backup**

Backs up all the files that are specified in the file list for the policy, regardless of when they were last modified or backed up. These backups occur automatically according to the criteria in the schedule. If you use incremental backups, you must also schedule full backups to perform a complete restore. If you're performing a raw partition backup, you must select **Full Backup**.

- **Cumulative-Incremental Backup**

Backs up all files that are specified in the file list and have changed since the last successful full backup. All files are backed up if no prior backup has been done. These backups occur automatically according to the criteria in the schedule. A complete restore in this instance requires the last full backup and the last cumulative incremental.

- **Differential-Incremental Backup**

Backs up all files that are specified in the file list for the policy and have changed since the last successful incremental or full backup. All files are backed up if no prior backup has been done. These backups occur automatically according to the criteria in the schedule. A complete restore in this instance requires the last full backup, the last cumulative incremental, and all differential incrementals that have occurred since the last full backup.

- **User Backup**

Initiated by the user through the interface on the client and backs up all files that the user specifies. Users can start backups only during the times that you specify in the schedule Start Window tab.

- **User Archive**

Initiated by the user through the interface on the client and archives all files that the user specifies. An archive is a special type of backup that first backs up the file and then deletes it from the local disk if the backup is successful. This frees local disk space while still keeping a copy for future use (until the retention period expires). Users can start archives only during the times that you specify in the schedule Start Window tab.

- **Application Backup**

A backup type that applies to all database agent clients. For more information on configuring schedules for this type of backup, see the NetBackup guide that came with the product.

- **Automatic Backup**

An automatic backup for all database agent clients, except NetBackup for Informix and Oracle. For more information on configuring schedules for this type of backup, see the NetBackup guide that came with the product.

- **Automatic Incremental Backup**

An automatic incremental backup that applies only to NetBackup for Informix clients. For more information on configuring schedules for this type of backup, see the *NetBackup for Informix System Administrator's Guide*.

- **Automatic Cumulative-Incremental Backup**

An automatic cumulative-incremental backup that applies only to NetBackup for Oracle clients. For more information on configuring schedules for this type of backup, see the *NetBackup for Oracle System Administrator's Guide*.

- **Automatic Differential-Incremental Backup**

An automatic differential-incremental backup that applies only to NetBackup for Oracle clients. For more information on configuring schedules for this type of backup, see the *NetBackup for Oracle System Administrator's Guide*.

- **Automatic Full Backup**

An automatic full backup that applies only to NetBackup for Informix and for Oracle clients. For more information on configuring schedules for this type of backup, see the *NetBackup for Informix System Administrator's Guide* or *NetBackup for Oracle System Administrator's Guide.*

- **Automatic Vault**

An automatic Vault session. Applies only to Vault policies. This does not do a backup, but rather runs the vault command specified in the Vault policy's file list. In this way it starts an automatic, scheduled vault session or vault eject operation.

For more information on configuring a Vault policy, see "Creating a Vault Policy" on page 141.

Calendar Schedule Type

Calendar based scheduling allows you to specify run day options for your task. Choosing the **Calendar** schedule option causes the **Calendar Schedule** tab to appear in the Change Schedule dialog. For details on calendar-based scheduling, see "Calendar Schedule Tab" on page 122.

Frequency Schedule Type

Note **Frequency** does not apply to user schedules because the user can perform a backup or archive whenever the backup window is open.

Specifies how much time must elapse between successful automatic backups for clients on this schedule. For example, assume that you set up a schedule for a full backup with a frequency of one week. If NetBackup successfully completes a full backup for all clients on Monday, it does not attempt another backup for this schedule until the following Monday.

To set the frequency, click in the **Frequency** field and type a number or select a value from the drop-down list. Select a **Frequency** of hours, days, or weeks.

Backup Frequency Determines Schedule Priority

If more than one automatic schedule is due for a client within a policy, the backup frequency determines the schedule that NetBackup uses:

- Jobs from the schedule with the lower frequency (longer period between backups) always get higher priority. For example, a schedule with a backup frequency of one year has priority over a schedule with a backup frequency of one month.
- If full and incremental schedules have the same backup frequency and are both due for the same client, jobs from the full get precedence.

For example, NetBackup prioritizes the following three schedules in the order shown:

1. monthly_full (frequency is one month)
2. weekly_full (frequency is two weeks)
3. daily_incremental (frequency is one week)

If all three schedules are due for a client, NetBackup adds the job for the monthly full to the worklist and skips the other two.

For an explanation of how NetBackup prioritizes each backup job that it adds to its worklist, see "Factors Affecting Backup Time" on page 633.

Multiple Copies (Inline Tape Copy)

Multiple Copies is available if Inline Tape Copy is licensed. With Inline Tape Copy licensed, NetBackup can create up to four copies of a backup simultaneously, provided there are available tape drives for each copy and the drives are on the same media server.

The total number of copies (2 through 10) of a backup that may exist in the NetBackup catalog is determined by the **Maximum Backup Copies** setting on the Host properties Global Attributes tab. (See "Maximum Backup Copies" on page 245.)

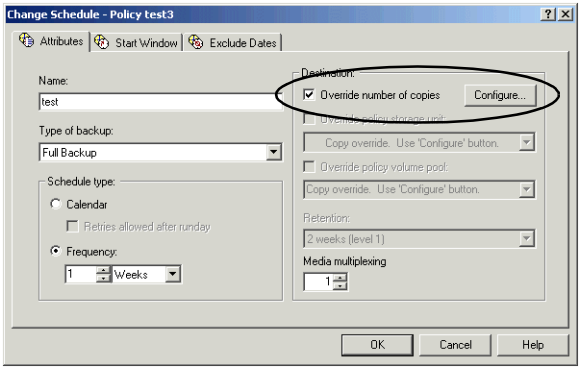
Inline Tape Copy can create up to four copies at backup time, or up to the **Maximum Backup Copies** setting, whichever is smaller. Additional copies may be created at a later time using duplication if the number of copies of the backup is less than the **Maximum Backup Copies** setting.

Note Inline Tape Copy does not support the following storage types: NDMP, third-party copies, EMC Fastrax, disk storage units, or optical devices.
Also, Inline Tape Copy does not support storage units that use a QIC (quarter-inch cartridge) drive type.

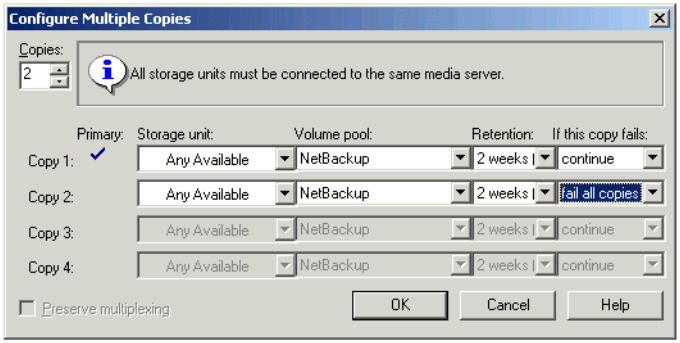
▼ To configure multiple copies during backup

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.
2. Double-click an existing policy or select **Actions** > **New** > **New Policy**to create a new policy.
3. Select the Schedules tab to configure Inline Tape Copy.
4. Double-click an existing schedule or click **New** to create a new schedule.

5. In the Schedule Attributes tab, select **Multiple Copies**, then click **Configure**.



6. Specify the number of copies to be created simultaneously. The maximum is four, or the number of copies specified by the **Maximum Backup Copies** setting, whichever is smaller. (See "Maximum Backup Copies" on page 245.)



Copy 1 is the primary copy. If Copy 1 fails for some reason, the first successful copy is the primary copy.

7. Specify the storage unit where each copy will be stored. (This is not applicable to disk type storage units.) If a storage unit has multiple drives, it can be used for both the source and the destination.

8. Specify the volume pool where each copy will be stored.

9. Select the retention level for each copy. (See "Retention" on page 115.)

10. In the event that the copy should not complete, select whether you'd like the entire job to fail, or whether you'd like the other copy (or copies) to continue.

11. Click **OK**.

Override Policy Storage Unit

Specifies whether to use the policy storage unit or another one for this schedule.

- To override the policy storage unit, select the check box. Choose the storage unit from the drop-down list of previously configured storage units. If the list is empty, no storage units have been configured yet.
- To use the policy storage unit, do not select the check box. NetBackup uses the policy storage unit you specified with the **Policy Storage Unit** general attribute. If you did not specify a policy storage unit, NetBackup uses any available storage unit. (See "Policy Storage Unit" on page 60.)

Override Policy Volume Pool

Specifies whether to use the policy volume pool or another one for this schedule.

- To override the volume pool specified by the **Policy Volume Pool** General Attribute, select the check box. Choose the volume pool from the list of previously configured volume pools.
- To use the policy volume pool, do not select the box. NetBackup uses the volume pool you specified with the **Policy Volume Pool** General Attribute. If you did not specify a policy volume pool, NetBackup uses *NetBackup* as the default.

Retention

Specifies how long NetBackup retains the backups it creates according to this schedule. To set the retention period, select a **Retention** from the drop-down list. When the retention period expires, NetBackup deletes information about the expired backup, making the files in the backups unavailable for restores. For example, if you choose two weeks, you can restore the data from a backup done by this schedule for only two weeks after the backup.

For full backups, always specify a time period that is longer than the frequency setting for the schedule (where the frequency is how often the backup runs). For example, if the frequency for a full backup is one week, specify a retention period of two to four weeks. This leaves enough margin to ensure that the current full backup does not expire before the next successful full backup occurs.

For cumulative incremental backups, always specify a time period that is longer than the frequency setting for the schedule. For example, if the frequency setting is one day, then specify a retention period of one week. This leaves enough margin to ensure that the current cumulative-incremental backup does not expire before the next successful one occurs. A complete restore requires the previous full backup plus the most recent cumulative-incremental backup.

For differential incremental backups, always specify a time period that is longer than the period between full backups. For example, if full backups occur weekly, then save the incrementals for two weeks. A complete restore requires the previous full backup plus all subsequent incrementals.

Default Retention Periods

Set the default retention periods in **Host Properties** > **Master Server** > **Retention Periods**. (See “Retention Periods Tab” on page 246.)The default choices are shown below.

Level	Period	Level	Period	Level	Period
0	1 week	9	infinite	17	expires immediately
1	2 weeks	10	expires immediately	18	expires immediately
2	3 weeks	11	expires immediately	19	expires immediately
3	1 month	12	expires immediately	20	expires immediately
4	2 months	13	expires immediately	21	expires immediately
5	3 months	14	expires immediately	22	expires immediately
6	6 months	15	expires immediately	23	expires immediately
7	9 months	16	expires immediately	24	expires immediately
8	1 year				

Note The levels are index numbers that correspond to the retention period (for example, the default retention period for level 0 is one week). The retention levels are shown here for reference as NetBackup uses them in some reports. NetBackup also uses the level when determining the volume to use for storing a backup.

Precautions For Assigning Retention Periods

- Be certain to assign a retention period that is long enough because NetBackup stops tracking backups when the retention period expires, making it difficult or impossible to recover files.
- Within a policy, always assign a longer retention period to full backups than to incrementals. Otherwise, it may not be possible to restore all your files.
- Archive schedules normally use a retention period of infinite.

Mixing Retention Levels on Backup Volumes

By default, NetBackup stores each backup on a volume that has existing backups at the same retention level (the period is not checked). For example, if a backup has a retention level of 2, NetBackup stores it on a volume with backups at retention level 2. When NetBackup encounters a backup with a different retention level than the previous backup, it switches to an appropriate volume. Because volumes remain assigned to NetBackup until all the backups on them have expired, this approach results in more efficient use of media. Otherwise, for example, one small backup with an infinite retention prevents a volume from being reused, even if all other backups on the volume have expired.

If you want to mix retention levels on volumes, select **Allow multiple retentions per media** in **Host Properties** > **Master Servers** > **Media**.

If you keep only one retention level on each volume, do not use any more retention levels than necessary. This consumes resources and also increases the number of volumes required.

Media Multiplexing

Note Some policy or schedule types do not support media multiplexing and NetBackup does not allow you to select it in those instances.

Specifies the number of jobs from this schedule that NetBackup can multiplex onto any one drive. Multiplexing sends concurrent backup jobs from one or several clients to a single drive and multiplexes the backups onto the media. (See “Multiplexing” on page 402.)

Specify a number from 1 through 8, where 1 specifies no multiplexing.

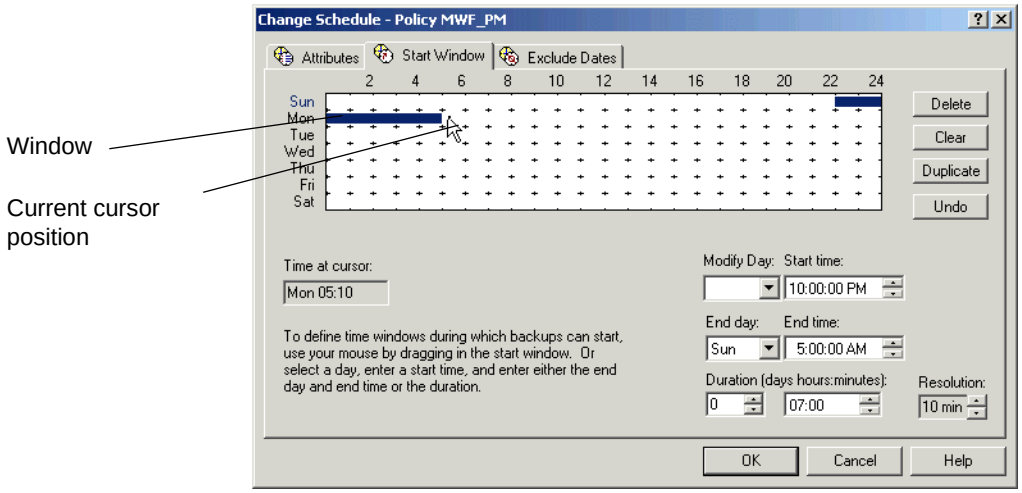
Start Window Tab

Provides controls for setting time periods during which NetBackup can start backups or archives when using this schedule. Time periods are referred to as *backup windows*. Create backup windows as necessary to satisfy backup requirements. For example, create a different window that opens each day or keep the backup window open all week.

▼ To create a backup window

1. Position the cursor over the day and time when you want the backup window to open. The **Time at cursor** field reflects the day and time corresponding to the current position of the cursor.

   Move the cursor and the value changes. The time is displayed based on a 24-hour clock. For example, 1 am is 01:00 and 11 pm is 23:00. 12 pm is 00:00.



   To set the resolution for start or end time settings, change the value in the **Resolution** field. For example, a resolution of 10 minutes allows you to adjust the backup window by 10 minute increments.

2. When the cursor is over the desired start time, press the left mouse button and drag the cursor to the day and time when you want the backup window to close. Release the button.

   - The **Modify Day** and **Start Time** fields display the day and time the backup window will open.
   - The **End Day** and **End Time** fields display the time the backup window will close.

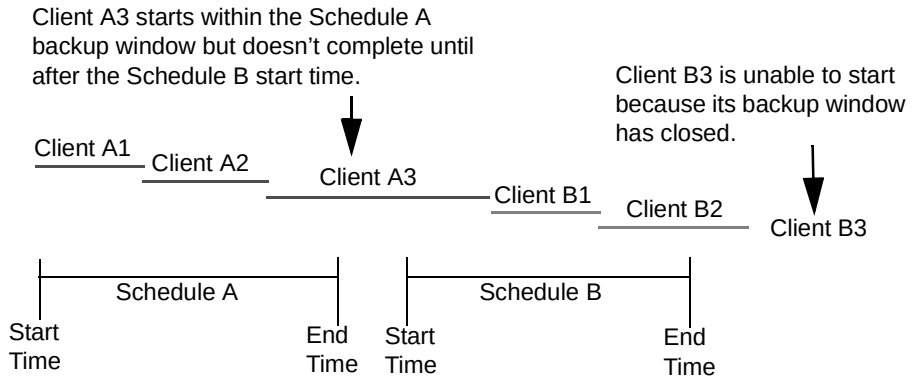
- The **Duration** indicates the length of the backup window based on the start and end date and times.

Specify enough time to allow all clients in the policy to complete a backup.

Also, allow extra time into the schedule in case the schedule starts late due to factors outside of NetBackup (such as unavailable devices). Otherwise, all backups may not be able to start.

Duration Example

The figure below represents the effect of schedule duration on two full-backup schedules, where the start time for the second schedule (B) begins shortly after the end time for the previous schedule (A). Both schedules have three clients with backups due.



The backup for client A3 in Schedule A does not finish until well after the Schedule B window has opened and does not leave enough time for the Schedule B backups. Client B3 must wait until the next time that NetBackup runs Schedule B.

Client A3 illustrates that, once started, a backup runs to completion even if the window closes while the backup is running.

▼ To create backup windows on successive days

1. Move the cursor over the desired start time, then press the Shift key and the left mouse button.
2. Drag the cursor to the time you want the first backup window to close.
3. Keeping the buttons pressed, drag the cursor down to duplicate the window on successive days.

▼ To copy a backup window to another day

1. Click on an existing backup window to select it.
2. Press the Ctrl key and drag to copy the window to another day.

Note If there are blank days immediately following the selected window, clicking **Duplicate** also duplicates the selected backup window on those days. Duplication stops when it reaches a day that already has a schedule defined. For example, you could duplicate the Sunday window on all other days of the week (assuming those days did not yet have a window defined).

▼ To change a backup window

1. Select the backup window.
2. Position the cursor over the end of the window that you want to change. The cursor changes to a two-headed arrow.
3. Press the left mouse button and drag the backup window to the desired length.

▼ To move a backup window

1. Select the backup window.
2. Position the cursor over the center of the selected window so the cursor changes to crossed arrows.
3. Press the left mouse button and drag the backup window to the desired location within the schedule area.

▼ To delete a backup window

1. Select the backup window.
2. Click **Delete**.

▼ To delete all backup windows

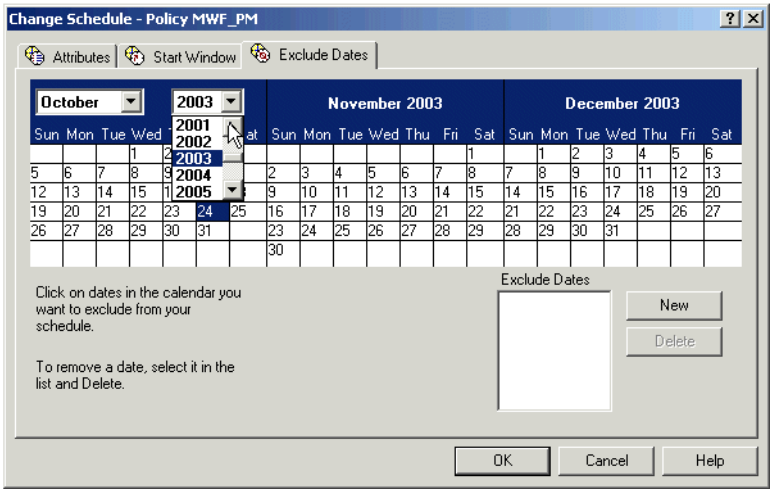
Click **Clear**.

Exclude Dates Tab

If there are particular dates that you would like to exclude from the schedule, select the **Exclude Dates** tab.

▼ To exclude a date from the policy schedule

There are two methods to exclude a date from the schedule:

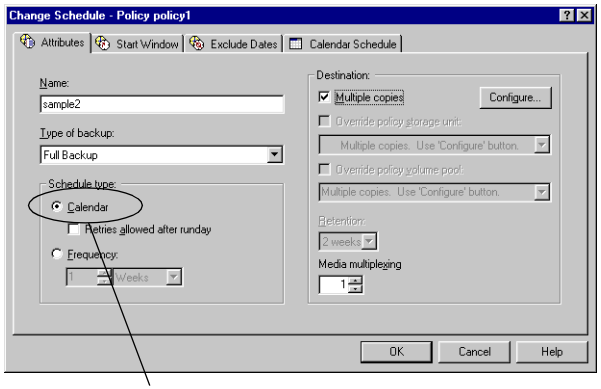


1. Select the **Exclude Dates** tab.
2. Select a 3-month period and year from the scroll-down menus. The calendar updates to display the chosen timeframe.
3. Click the date you wish to exclude. The date appears in the **Exclude Dates** list.

   Another method to exclude dates is to click **New**. Then enter the month, day and year in the Date selection dialog. Click **OK**.

Calendar Schedule Tab

The Calendar Schedule tab appears when **Calendar** is selected as the Schedule type on the **Attributes** tab of the Schedule dialog. Calendar based scheduling provides several run day options for use in scheduling when your task will run.

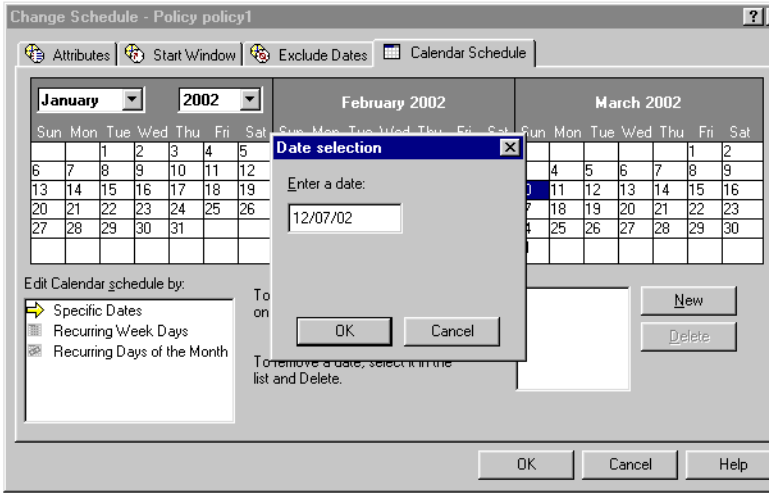


Selecting Calendar on the Attributes tab enables the Calendar Schedule tab

Schedule by Specific Dates

A task can run on specific dates rather than follow a recurring schedule, and specific dates can be added to a recurring schedule. The **Specific Dates** run day option allows you to schedule specific dates on which your task will run. You can schedule specific dates in any month of any year up to and including December 31, 2037.

▼ To schedule a backup on a specific date



1. In the **Calendar Schedule** tab, select **Specific Dates**.
2. Click on the date in the calendar display or click **New**, enter a date, then click **OK**. The date appears in the calendar schedule list.
3. To remove a date, select it in the calendar schedule list and click **Delete**.
4. When you have finished selecting dates for your task, select another tab to make changes or click **OK** to close the dialog.

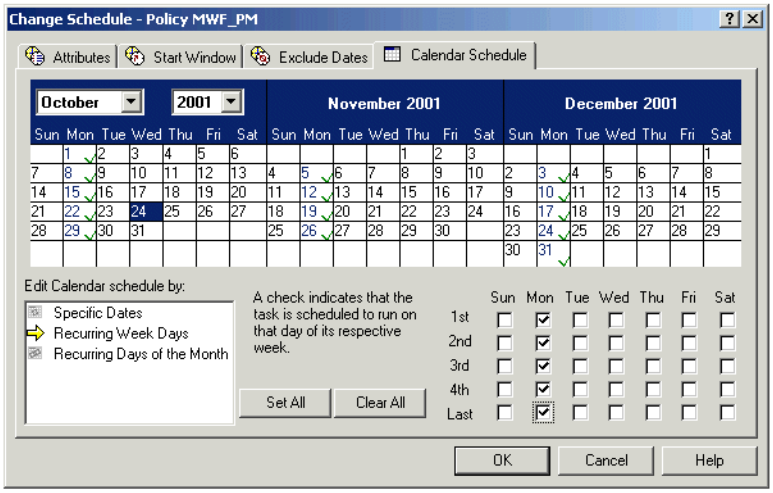
Schedule by Recurring Week Days

The **Recurring Week Days** option provides a matrix that lets you schedule a task for certain days of each week, weeks of each month, or days on particular weeks of the month.

The weekday matrix is not a calendar. It is simply a matrix used to select days and weeks in a month. A check mark entered for a day indicates that the task is scheduled to run on that day of its respective week. By default, no days are selected.

▼ To schedule a recurring weekly backup

1. In the **Calendar Schedule** tab, select **Recurring Week Days**.



2. Select the checkbox for a particular day to check or uncheck the day.

3. Select a column header to check or uncheck the corresponding day for each week of the month.

4. Select a row number to check or uncheck the entire week.

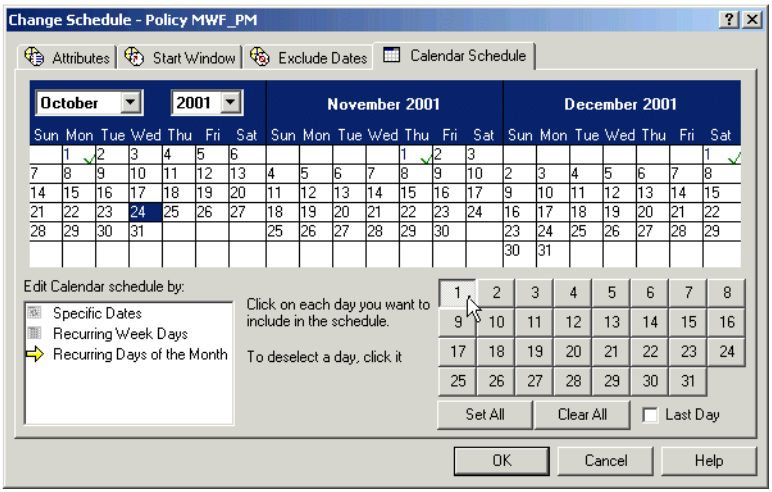
5. Select the checkbox for the appropriate day in the **Last** row to schedule a task for the last week of each month, regardless of the number of weeks in the month.

6. When you have finished selecting dates for your task, select another tab to make changes or click **OK** to close the dialog.

Schedule by Recurring Days of the Month

The **Recurring Days of the Month** option provides a matrix that you can use to schedule a task for certain days of the month. You can also schedule a task to occur on the last day of the month, regardless of the actual date.

▼ To schedule a recurring monthly backup



1. In the **Calendar Schedule** tab, select **Recurring Days of the Month**.

2. Select the button for each day you want included in the run schedule. Clicking the button again will deselect the day.

3. Select the **Last Day** checkbox if you want to run the schedule on the last day of the month, regardless of the date.

4. When you have finished selecting dates for your task, select another tab to make changes or click **OK** to close the dialog.

Examples of Automatic-Backup Schedules

Backups can be scheduled to occur automatically on every day of the week or only on specific days. You can also specify a different backup window for each day.

The days of the week to choose for backups depends on how you want to distribute the backup load. For example, to have all backups occur on Saturday, create a backup window only for Saturday.

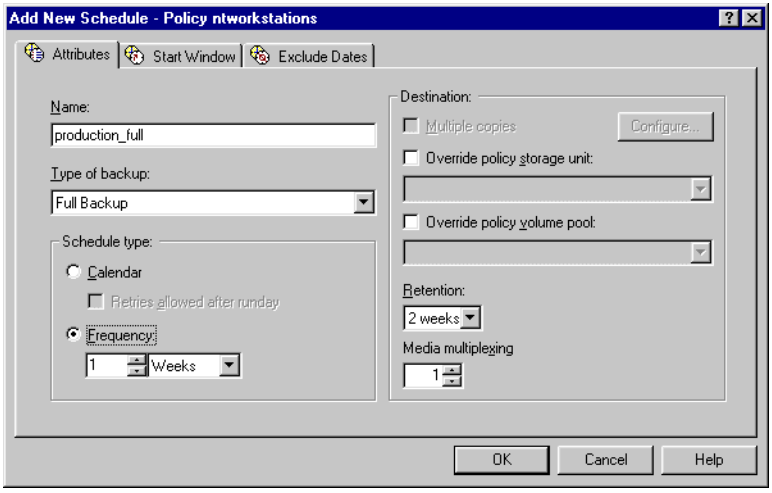
The best times for automatic backups are usually nights and weekends, when client and network activity is lowest. Otherwise, the backups can adversely affect client and network performance and take longer to complete.

Example 1

This example shows two approaches for scheduling automatic backups. The first is the recommended method.

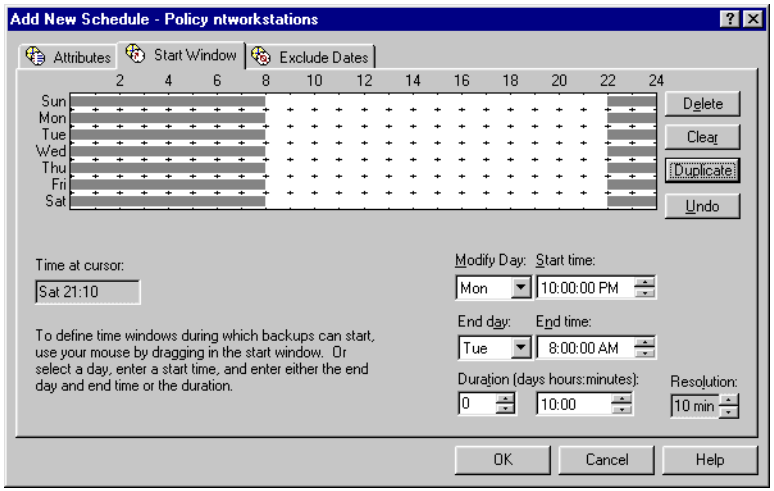
Schedule Runs Every Day (recommended method)

The recommended method is to create schedules that run every day of the week.



If the backup for a client does not complete on one day, NetBackup retries it on the next day. This ensures that a retry occurs promptly in case of a failure or lack of time during the first session.

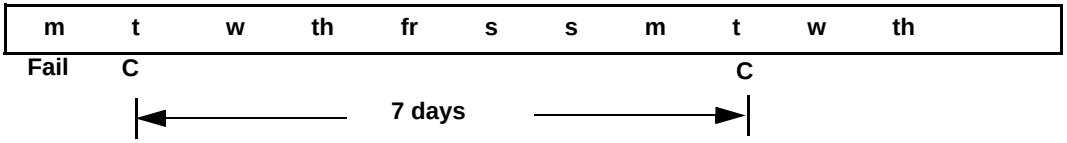
The day of the week when a client is backed up changes if its backup rolls over to the next day.



In this example schedule, full backups can occur on any day of the week but only once every seven days:

If the cycle begins with a full backup on a Monday and completes successfully, the next full backup occurs on the following Monday, seven days later.

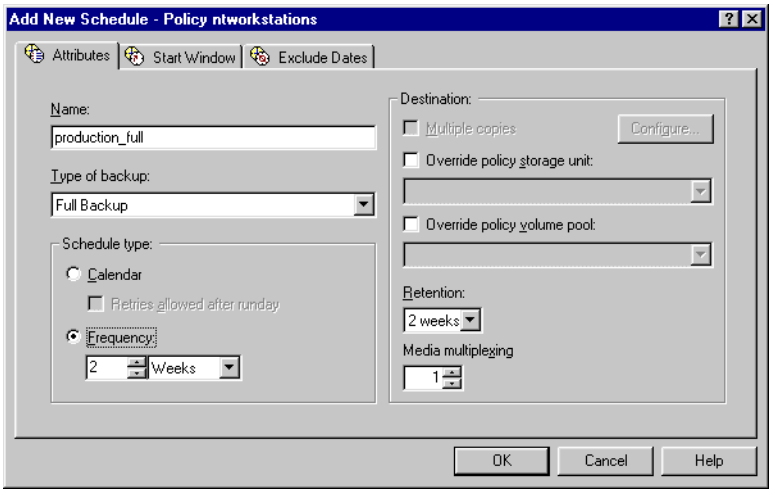
If the backup fails on Monday, NetBackup attempts it at the same time each day until it does successfully complete. NetBackup can attempt the backup on each subsequent day because the schedule allows backups occur on any day, but only once during any seven day period. If the backup completes on Tuesday, NetBackup waits seven days from Tuesday for the next backup.

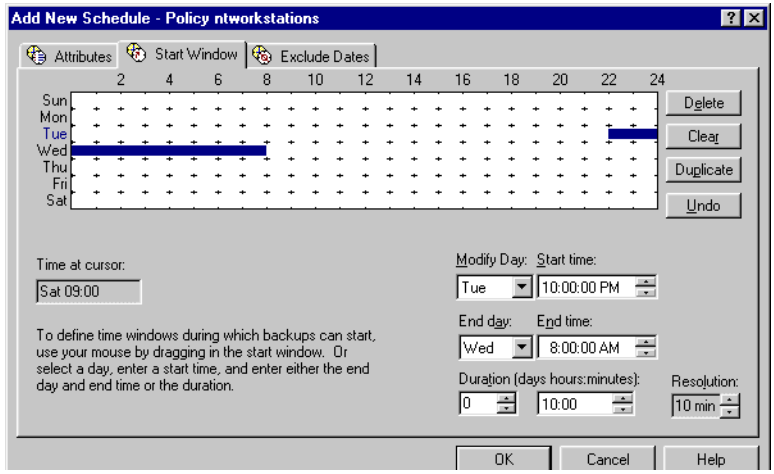


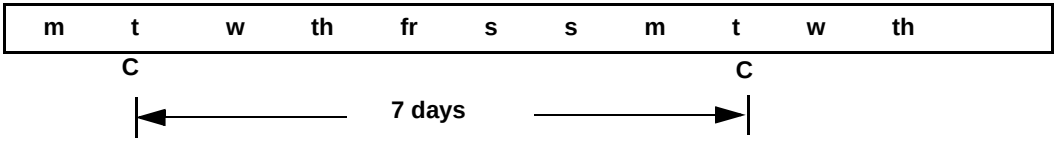
Another Method

This example shows a frequency schedule that allows backups occur only on specific days. Full backups occur only on Tuesdays and every seven days.

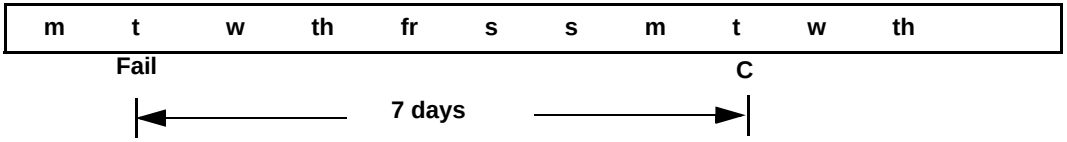
If the cycle begins with a full backup on a Tuesday and completes successfully, the next full backup occurs on the following Tuesday, seven days later.







If the backup fails on Tuesday, NetBackup must wait until the following Tuesday before trying again.

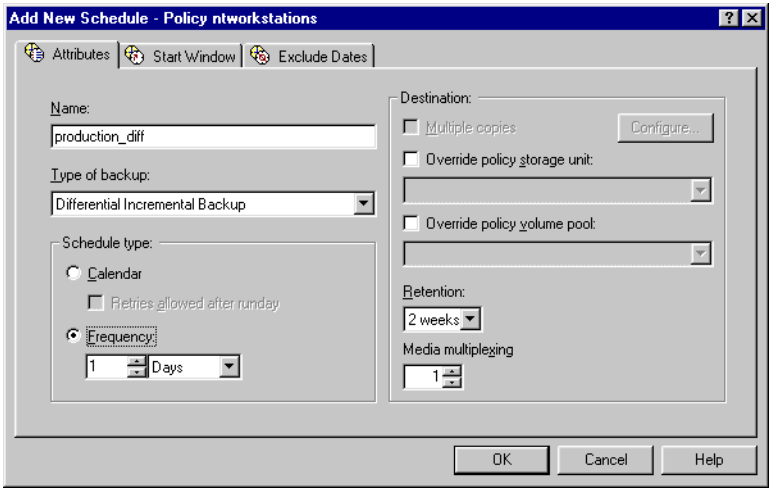


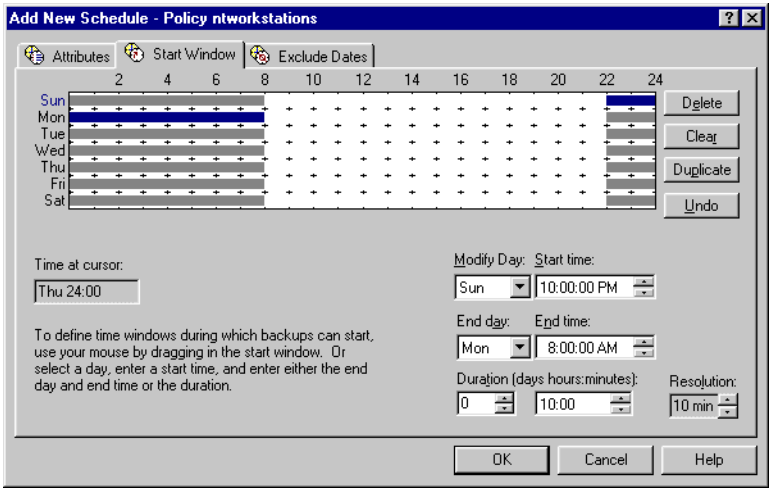
Example 2

The following shows a complete set of frequency schedules that have a backup window every day (recommended method).

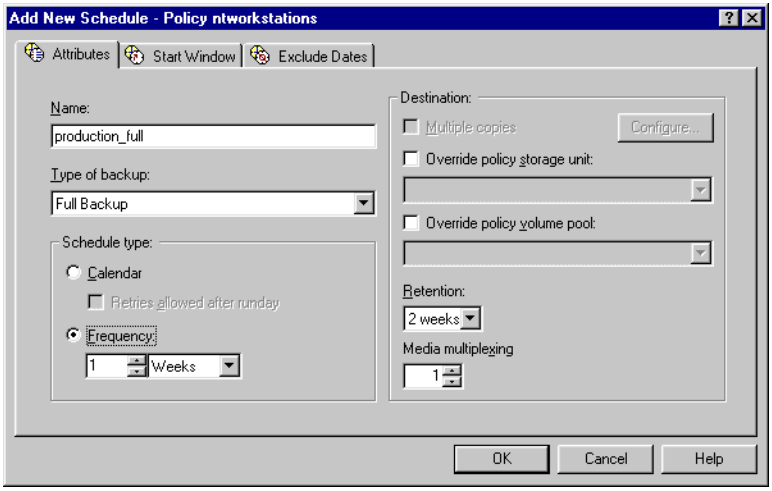
If the backup does not complete on one day, NetBackup tries it again the next day.

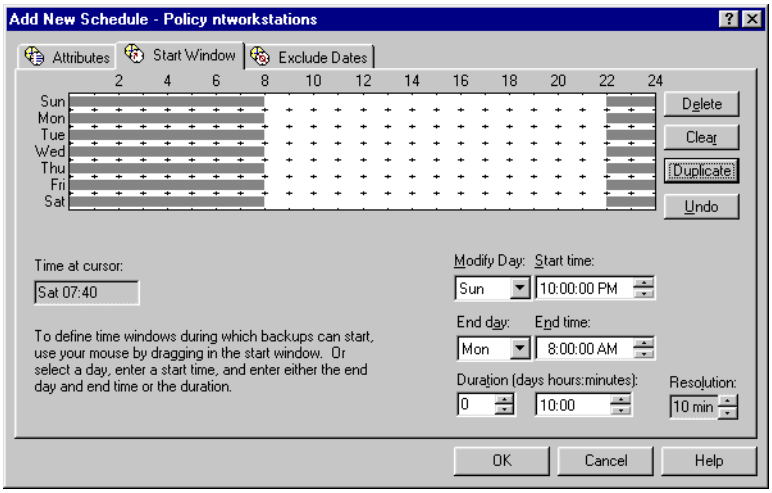
Daily Incremental Backups



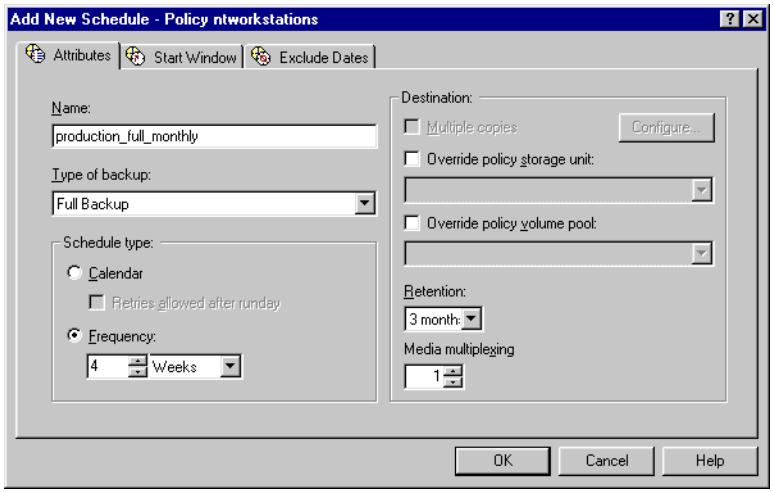


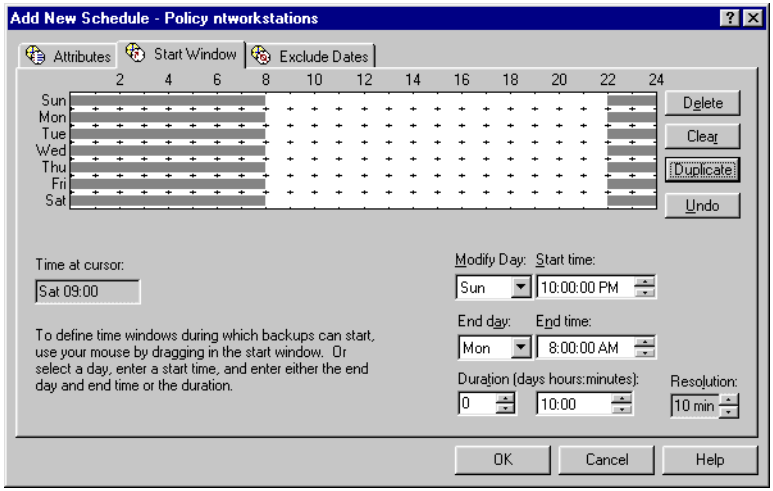
Weekly Full Backups



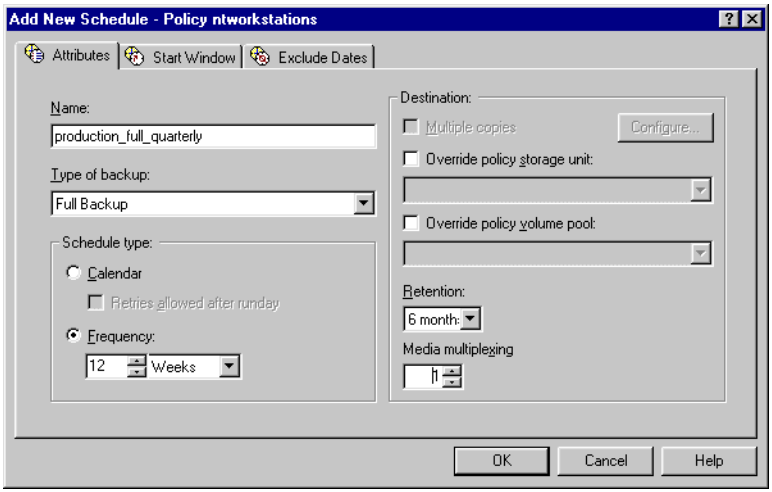


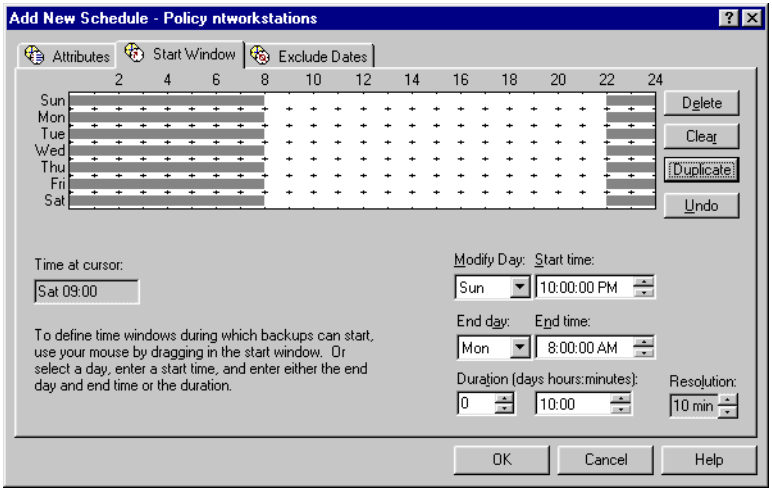
Monthly Full Backups





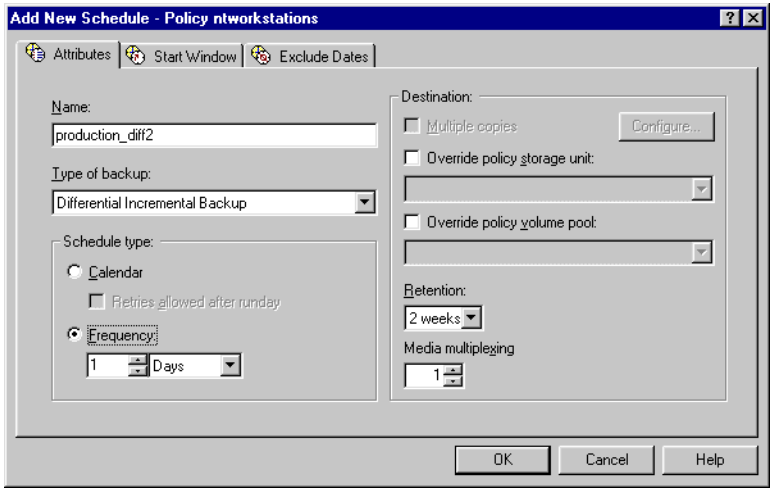
Quarterly Backups

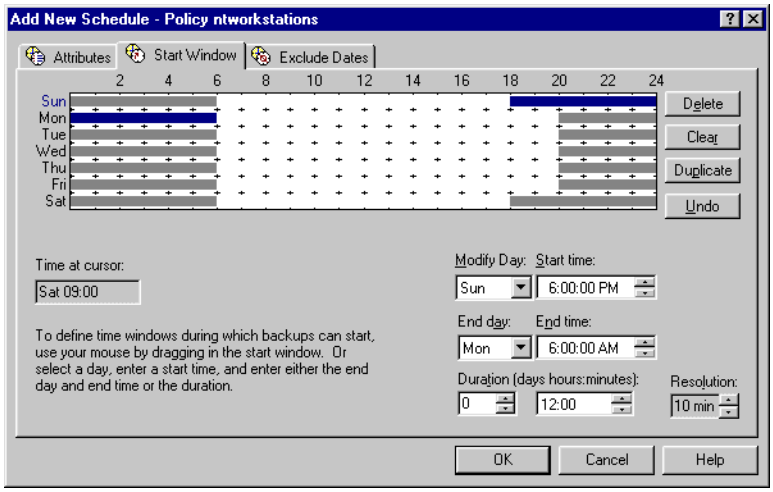




Example 3

The following is an example of using different backup windows, depending on the day.





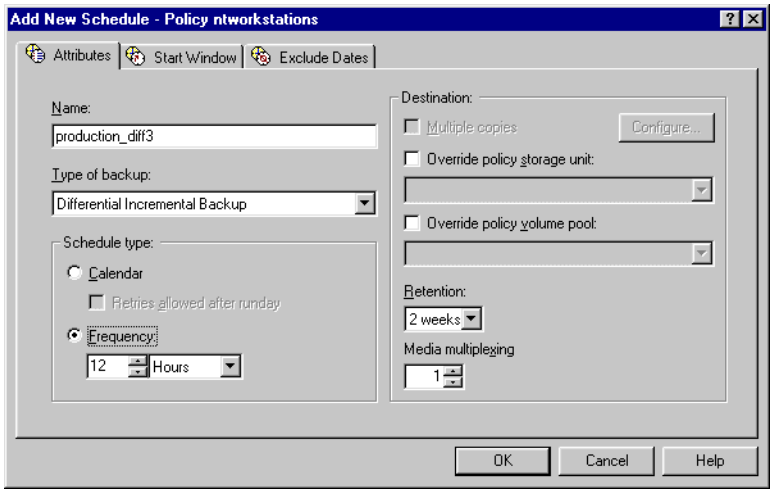
Example 4

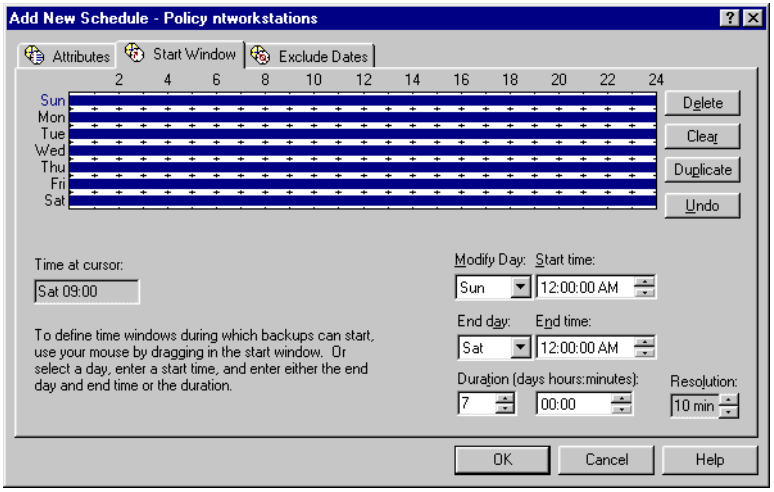
The following is an example where the backup window is longer than the period between backups as determined by frequency.

Backups occur according to time elapsed since the last backup and more than one backup can occur for a client during the backup window.

This mode is useful when you want to perform backups twice (or more) daily.

In the following schedule, the backup window spans 7 days and the frequency is 12 hours. A backup is due every 12 hours.



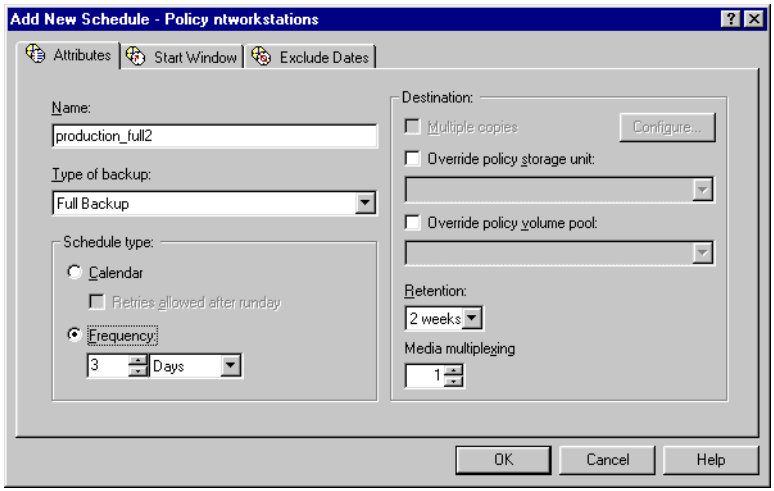


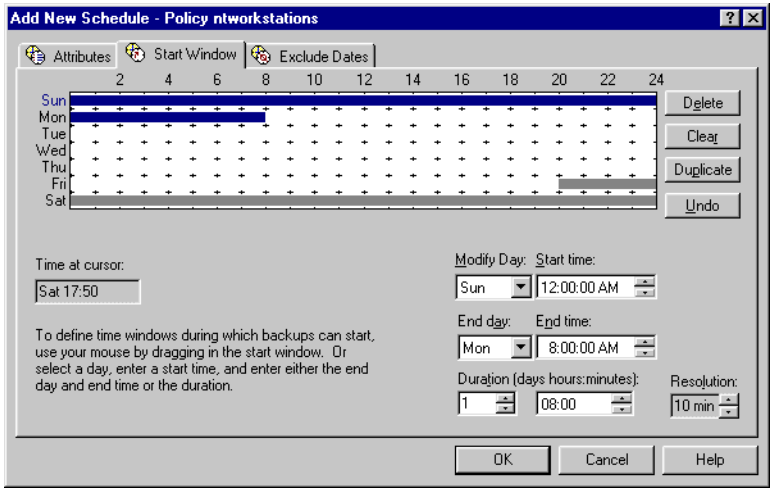
Example 5

The following example allows full backups occur only during weekend hours.

The weekend backups are accomplished by having a start time of 8 pm Friday evening and a duration of 60 hours. This allows NetBackup to continue running backups until 8 am Monday morning.

Because the frequency is three days, backups are due again when the schedule starts on the following Friday. If a failure occurs, the administrator can run a manual backup on Monday and the automatic backup is still due on Friday.

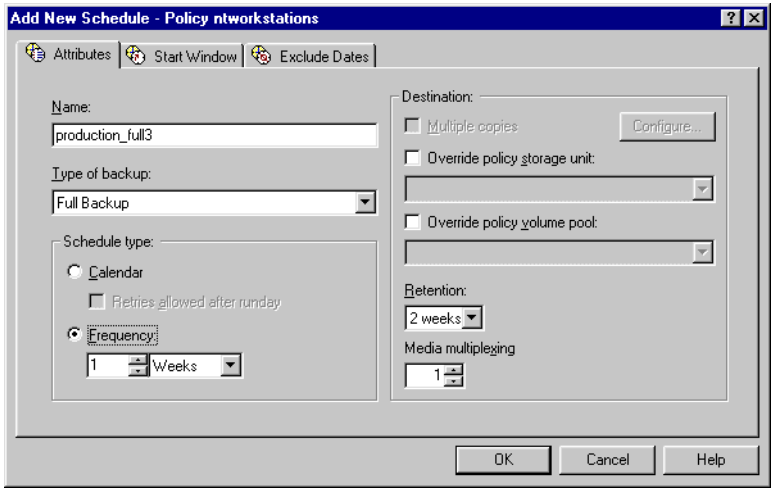


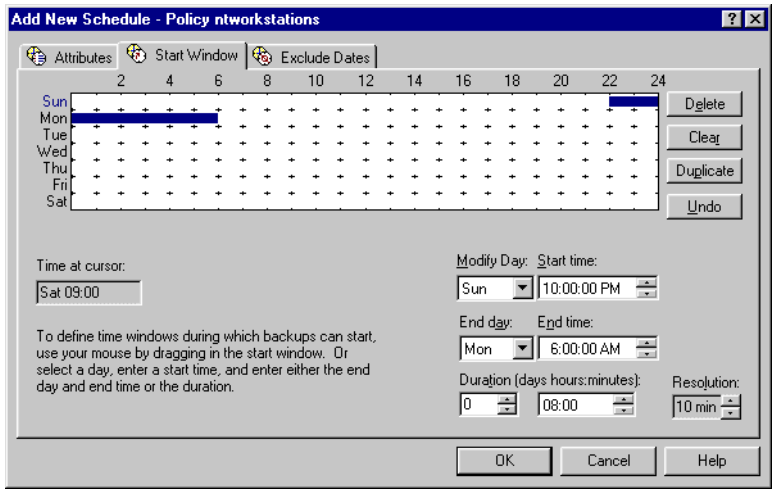


Example 6

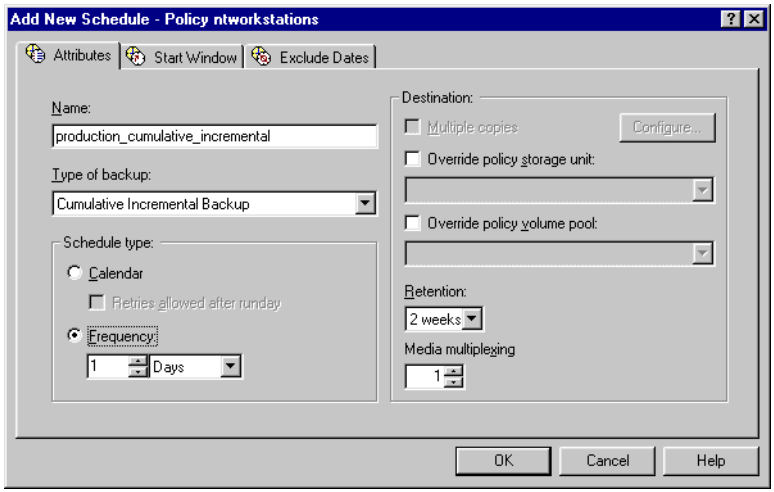
The following is an example where a full backup runs every Sunday and cumulative incrementals run on all other days. Each of the cumulative incremental backups contain all files that have changed since the last full backup. This puts more files in each incremental than are present for a differential but it makes restores easier. If a restore is required on Saturday, the Sunday tape and the Saturday tape are needed to do the restore. If this were a differential incremental, then all tapes Sunday through Saturday would be needed.

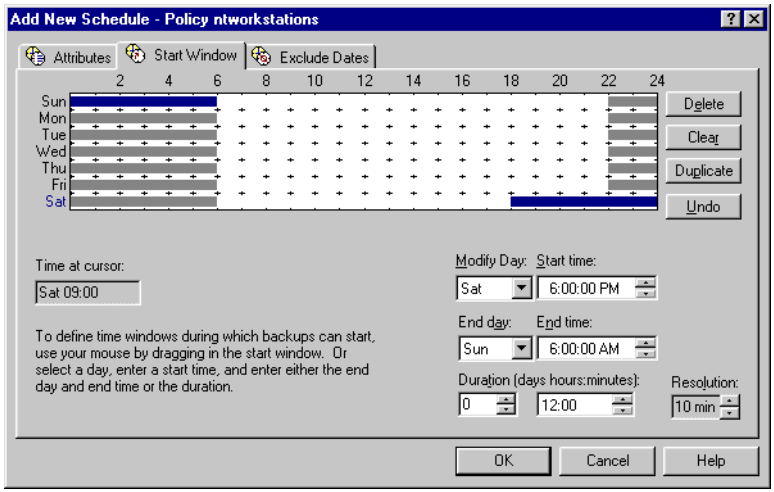
Full Backups





Cumulative Incremental Backups





Considerations for User Schedules

To allow user backups and archives, you must create schedules for them. There is no requirement, however, to create a policy exclusively for user backups.

Restores can occur at any time and do not have schedules.

Note An archive is different from a backup: NetBackup first backs up the selected files, *then deletes them* from the local disk if the backup is successful. In this manual, references to backups also apply to the backup portion of archive operations unless otherwise noted.

Planning User Backup and Archive Schedules

When planning user backup and archive schedules, consider the following:

- Best times to perform backups. For user backups, this is the time most convenient to the users.

  If possible, do not permit user backups and archives when automatic backups are occurring. If an automatic backup is running when a user submits a backup or archive, NetBackup queues the user job. If the automatic backup is long enough, the user job will miss the backup window. Once started, a user job also delays automatic backups and can cause them to miss the backup window.

- Storage unit. Using a different storage unit can eliminate conflicts with automatic backups.

- Volume pool. Use a different volume pool if you want to manage the media separate from the automatic backup media.

Caution If the retention period is not long enough and the retention period expires, it can be difficult or impossible to restore the archives or backups.

- Retention. It is usually best to set the retention period for archives to infinite, since the disk copy of the files is deleted.

Creating Separate Policies for User Schedules

If you create separate policies for user backups or archives, the considerations are similar to those for automatic backups. One difference, however, is that no file list is necessary because users select the files before starting the operation.

The following table shows a set of clients in two user policies.

Policy	Client	Desired Storage	Best Backup Time	Retention
User1	mercury mars jupiter neptune	8 mm tape stacker	08:00 to 16:00	Backups - 6 months Archives - Infinite
User2	pluto	8 mm tape stacker	12:00 to 20:00	Backups - 6 months Archives - Infinite

- All clients in policy User1 have common requirements for user backups and archives.

- The policy named User2 was created for pluto because the user on this client works from 12 pm to 8 pm (12:00 to 20:00) and therefore requires different backup times.

If NetBackup receives a request for a user backup or archive, it uses the first policy and schedule that it finds that has both of the following:

1. The client for which the user is requesting the operation.
2. A user schedule that:
   - Specifies the appropriate operation (backup or archive).
   - Allows the operation to start at the time that the user requests it. If the backup device is busy at the time of the request, NetBackup queues the request and honors it when the device becomes available (providing the backup window is still open).

For example, assume that at 14:00 (2 pm), a user on the client named mars begins a backup of files. NetBackup processes this request as follows:

1. Finds a policy that includes mars in its client list and has a user backup schedule that allows a backup to start at 14:00 (2 pm).
2. Performs the backup.

The following policy and schedule meets the criteria for the above request:

Clients	mercury, mars, jupiter, neptune
Files	Applies only to automatic backups
Type of Backup	User backup
Start Time	08:00
End Time	18:00
Days of Week	All
Retention	6 months
Storage Unit	TS8_1

Using a Specific Policy and User Schedule

To use a specific policy and (or) schedule for user backups or archives, perform the following on the client:

- On Microsoft Windows clients, start the Backup, Archive and Restore client interface. Click **File** > **NetBackup Client Properties** and select the **Backups** tab. Specify the backup policy and backup schedule.
- On NetWare target clients, specify the policy and schedule with `backup_policy` and `backup_sched` entries in the `bp.ini` file (see the NetBackup user's guide for the client).
- On UNIX and Macintosh clients, specify the policy and schedule with `BPARCHIVE_POLICY`, `BPARCHIVE_SCHED`, `BPBACKUP_POLICY`, or `BPBACKUP_SCHED` options in the `bp.conf` file.

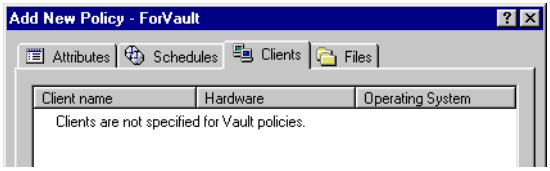
Creating a Vault Policy

Setting up a Vault policy differs from setting up a regular policy.

When configuring a Vault policy, be sure to specify Vault as the policy type. Instead of entering a directive on the File tab, you'll indicate one of two Vault commands. There are no clients specified in Vault policies.

▼ To create a Vault policy

1. In the NetBackup Administration window, expand **Master Server** > **NetBackup Management** > **Policies**.
2. Click the New Policy button .
3. Type a unique name for the new policy in the **Add a New Policy** dialog. Click **OK**.
4. On the Attributes tab, select **Vault** as the policy type.
5. On the Schedules tab, click **New** to create a new schedule. The type of backup defaults to **Automatic**. Complete the schedule.
6. Clients are not specified for Vault jobs, as the Client tab notes.



7. On the Files tab, enter one of two Vault commands. Both commands are found in *install_path*`\netbackup\bin`:

   - `vltrun`: Use this command to initiate a new vault session for a specific vault profile. Enter:

     `vltrun` *profile_name*

     If the profile name is not unique, enter:

     `vltrun` *robot_number* / *vault_name* / *profile_name*

   - `vlteject`: Use this command to eject and / or generate reports for multiple sessions which have not yet ejected media or generated reports. This can operate on all sessions for a vault or on all sessions for a robot or on all sessions for all robots. Use the following syntax:

     `vlteject -eject [-report] [-vault` *vault_name*`]`

     or

     `vlteject [-eject] -report [-vault` *vault_name*`]`

   For more information on Vault names, profile names, and command usage, see the *Vault System Administrator's Guide.*

8. Click **OK**.

Performing Manual Backups

You can perform immediate manual backups of selected automatic backup schedules and clients within a policy. A manual backup is useful for situations such as:

- Testing a configuration.
- When workstations miss their regular backups.
- Before installing new software (to preserve the old configuration).
- Preserving records before a special event such as when companies split or merge.
- Quarterly or yearly financial information.
- In some cases, it may be useful to create a policy and schedule that you use only for manual backups. You can do this by creating it with a single schedule that has no backup window (and therefore never runs automatically).

▼ To perform a manual backup

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Policies**.

2. Select the policy name in the left pane.

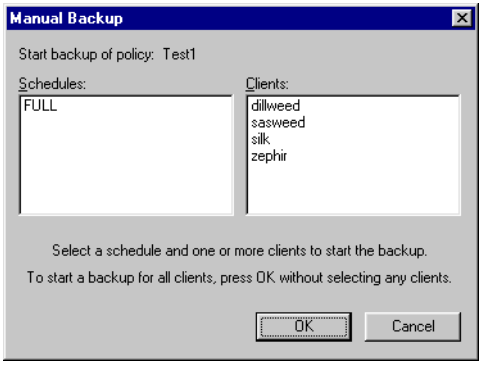
3. Select **Actions** > **Manual Backup**. (The policy must be set to Active for this command to be available.) The Manual Backup dialog appears.

Note Not only does the policy need to be Active, but if **Go into effect** is set on the policy to a future date and time, the backup will not run.

4. In the Manual Backup dialog, select the schedule and the clients that you want to back up.

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

   User schedules do not appear in the schedules list and cannot be manually backed up because they do not have a file list (the user selects the files).



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

Using Catalog for Catalog Backups and Verifying, Duplicating, and Importing Images 4

This chapter explains how to back up and manage the NetBackup catalog files and contains the following sections:

- Introduction to the NetBackup Catalogs
- Configuring Catalog Backups
- Backing Up the Catalogs Manually
- Protecting Large NetBackup Catalogs
- Managing the NetBackup Catalogs
- Converting the Catalog Format
- Searching for Backup Images
- Verifying Backup Images
- Duplicating Backup Images
- Expiring Backup Images
- Importing Backup Images
- Viewing Job Results

Introduction to the NetBackup Catalogs

NetBackup catalogs are internal databases that contain information about the NetBackup configuration and backups. Backup information includes records of the files and the media on which the files were stored. The catalogs also contain information about the media and storage devices that are under the control of Media Manager.

NetBackup requires the catalog information in order to recover any backups that have been performed. Therefore, it is extremely important to configure catalog backups before using NetBackup for regular client backups, and to schedule the catalog backups to occur on a regular basis thereafter. Without regular catalog backups, you risk losing your regular backups if there is a problem with the disk that contains the catalogs.

NetBackup 4.5 now defaults to use a binary format for new catalogs on Windows, Solaris, HP_UX, Compaq Tru64 UNIX, AIX, Linux and SGI platforms. Previous releases created catalogs in ASCII format.

Existing catalogs can be upgraded to binary format using the catalog conversion utility, `cat_convert` as described in “Converting the Catalog Format” on page 173.

Where are the Catalog Files?

The catalogs reside on disk on NetBackup servers. NetBackup chooses default locations for them during installation. If you change the default locations, you must change your catalog backup configuration accordingly.

What Method Do I Use to Back Them Up?

Because the catalogs are essential to restoring files in case of a disk crash, the process for backing them up is separate and different than for standard backups. The two available methods are:

- Automatic backup according to the configuration that you choose in
- Manual backup as explained under

What Types of Media Can I Use?

You can use either removable media (such as a tape) that is configured under Media Manager, or a directory on a hard disk. (See “Media Type” on page 150.)

How Do I Know If a Catalog Backup Succeeded?

The All Log Entries, Problems, and Media Log Entries reports, available from the Reports utility, provide information on NetBackup catalog backups. In addition, you can use:

- `dbbackup_notify` script.
- E-mail, if you configure this capability with the E-mail Address for NetBackup Administrator Global attribute. (See "Administrator E-mail Address" on page 245.)

How Do I Restore The Catalog Backups?

If it is necessary to perform a disaster recovery, restore the catalogs by using the NetBackup `bprecover` command. See the *NetBackup Troubleshooting Guide for Windows* for recovery procedures.

Important Precautions to Observe

- Use only the methods described in this chapter to back up the catalogs. The special backup operations described here are the only ones that can track all relevant NetBackup activities and ensure consistency between the catalog files.
  - Do not use scheduling or backup methods provided by any other vendor.
  - Do not rely on user backups or regular-scheduled backups. If you use these methods and the disk fails, the catalogs as well as the backups are lost and you may not be able to recover any data.
- Back up your catalogs often. If these files are lost, you lose information about backups and configuration changes that were made between the time of the last NetBackup catalog backup and the time that the disk crash occurred.
- Do not use methods other than NTFS compression to compress the catalogs or NetBackup may not be able to read them.
- Keep a hard-copy record of the media IDs where you store the NetBackup catalog backups, or configure the E-mail global attribute. The E-mail global attribute causes NetBackup to send an E-mail that indicates the status of each catalog backup and the media ID that was used. You can then print the E-mail or save it on a disk other than the one that has the catalogs.
- If you back up your catalogs to disk (not recommended), always back up to a different disk than where the catalogs reside. If you back up to the same disk and that disk fails, you will also lose the catalog backups in addition to the catalogs and recovery will be much more difficult. Also, ensure that the disk has enough space for the catalogs or it will fill up and backups will fail.

- NetBackup 4.5 does not support saving catalogs to a remote file system such as NFS or CIFS. The new binary catalog in NetBackup 4.5 is more sensitive to the location of the catalog. In addition, storing your catalog on a remote file system can have critical performance issues for catalog backups.

Configuring Catalog Backups

The easiest way to configure NetBackup catalog backups is to use the Catalog Backup Wizard. This wizard guides you through the configuration process, simplifying it by automatically choosing settings that are good for most configurations. If you are modifying an existing configuration or want access to all available configuration settings, use the manual method. The following sections explain both the wizard and the manual method.

▼ To configure the catalog backup using the Catalog Backup Wizard

1. Launch the **NetBackup Catalog Backup Wizard** by clicking **Configure the Catalog Backup** in the right pane. The wizard is visible when either **Master Server** or **NetBackup Management** is selected in the left pane.

   See the *NetBackup Getting Started Guide* for step-by-step instructions.

2. To change a policy after it is created, see “Backing Up the Catalogs Manually” on page 159.

Note If you are unfamiliar with NetBackup catalog backups, read “Introduction to the NetBackup Catalogs” on page 146 before proceeding. In particular, read the precautions under “Important Precautions to Observe” on page 147.

▼ To configure the catalog backup manually

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

   If your site has more than one master server, use **File** > **Change Server** to select a different server. (See “ Administering a Remote Master Server” on page 320.)

2. Select **Actions** > **Configure NetBackup Catalog Backup**. The NetBackup Catalog Backup dialog appears containing three tabs: Attributes, Schedule, Files.

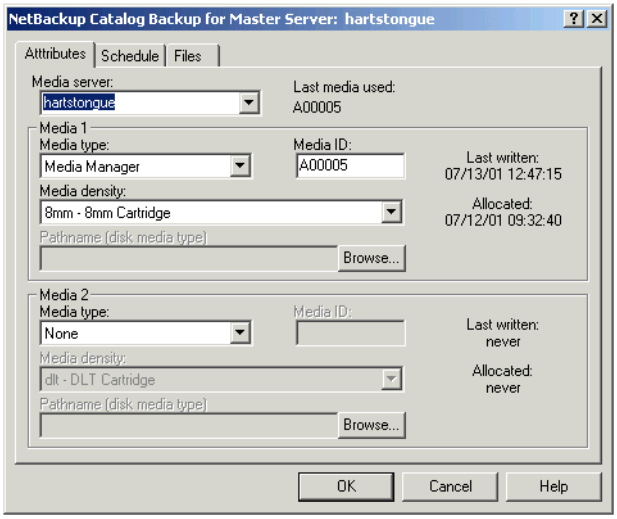
3. Specify the properties on each tab of the dialog as explained in the topics below:

   - “Catalog Attributes Tab” on page 150
   - “Catalog Schedule Tab” on page 154
   - “Catalog Files Tab” on page 156

4. Click **OK**.

Catalog Attributes Tab

The Catalog **Attributes** tab contains general attributes for NetBackup catalog backups.



Media Server

Specifies the name of the NetBackup server to which you are sending the catalog backups. This is always the NetBackup BusinesServer where the catalogs reside and cannot be changed.

Last Media Used

Shows the media ID (for Media Manager media) or absolute pathname (for disk) that contains the last NetBackup catalog backup. The value in this field is the value that you specified for either Media 1 or Media 2. These are the media that NetBackup alternates between for catalog backups.

Media 1 and Media 2 Areas

Specifies the media to use for the catalog backups. You do not have to assign both Media 1 and Media 2. If you do assign both, NetBackup alternates between the media.

Media Type

Specifies the media type. Select one from the drop-down menu:

- **None:** No media is assigned
- **Disk:** A directory on a disk drive
- **Media Manager:** A volume that is in a robot or drive under control of Media Manager

Depending on the storage devices that are available, VERITAS recommends the following choices for **Media Type**:

1. If you have a robot or a tape stacker, choose **Media Manager** and use this automated device to store the catalog backups. This is the easiest way to back up your catalogs because NetBackup automatically finds the volume if it is in a robot or tape stacker when the backup is started.

2. If you do not have a robot or tape stacker, but have an extra standalone storage device that you can devote to catalog backups, choose **Media Manager** and use the extra standalone device.

3. If you have only one standalone drive (no robot or tape stacker), the most convenient method is to choose **Disk** for the media type and send the catalog backups to a hard drive (though this is not as safe as method 4 below). The hard drive that you use for the catalog backup must be different than the hard drive where the catalogs reside. By default, the catalogs are stored in the following locations. If you choose to back up the catalog to disk, the destination of the catalog backup must be on a different drive.

Caution The safest way to protect your data is to save all backups (including your catalog backup) to removable media, then move a full set of that media to offsite storage on a regular basis. A backup written only to disk will share the same risks as the computer(s) being backed up. A natural disaster (for example, lightning, flood or fire) is more likely to destroy both your primary data and its backups if the backups are only on disk.

If the disks holding the catalogs and the catalog backup are both destroyed, it will be much more difficult to recover your business data. Assuming the backups of your business data are on tape, recovering without the catalog backup means manually importing all of the backup tapes to rebuild the catalogs. This process takes time that you may not want to spend when you need to resume your business activities.

4. If you have only one standalone drive (no robot or tape stacker) and there is not enough space available on a different hard drive, choose **Media Manager**. In this situation, you must back up the catalogs to the same tape drive as the backups of your business data. This involves swapping tapes in and out of the drive each time the catalogs are backed up. Swapping tapes is not convenient, but is required because NetBackup will not place catalog backups and the backups of your business data on the same tape.

Media ID

If you've chosen **Media Manager**, specify a valid media ID.

The volume you specify must be configured in Media Manager in the same manner as other NetBackup volumes. This means the media ID must appear under **Master Server** > **Media and Device Management** > **Media**. The volume must also meet the following requirements:

- The volume must be in the NetBackup volume pool. To verify, look under **Media** and ensure that the **Volume Pool** column for the media ID displays NetBackup.
- The volume cannot be currently assigned to NetBackup for backups because NetBackup does not mix catalog backups and regular backups on the same media. To locate an available volume, expand **Master Server** > **Media and Device Management** > **Media** and find a volume where the **Time Assigned** column is empty and the **Status** column is 0. After you specify a volume for catalog backups, a time appears in the **Time Assigned** column and the **Status** column changes to 1. If a column does not appear, right-click in the pane and from the shortcut menu, select **Columns** > **Layout**. In the Set Column Layout dialog, set the specific column to **Show**.

The Last Written information under Media 1 and Media 2 indicate when the volume specified in the Media ID field was last used. The value is *never* if the volume has never been used for NetBackup catalog backups.

Note If you delete and then add back the media ID for a volume that was used for NetBackup catalog backups, NetBackup changes its Last Written date and time. However, the contents of the volume itself is not actually altered until the next time it is used for a backup.

The Allocated information under Media 1 and Media 2 indicate when the media was allocated for NetBackup catalog backups.

Notes on the Media ID

- To delete the media for Media 1 or Media 2, set the **Media Type** value to None. Do not use backspace to leave the Media ID box blank.
- If you delete a volume from the catalog-backup configuration, Media Manager makes it available for reassignment. This can cause problems if, for example, you temporarily change to a different volume.
- You must manually track catalog-backup media separately because NetBackup does not keep a record of catalog-backup media in its catalogs as it does with other backup media. If NetBackup did track catalog-backup media in the catalog, and the disk containing the catalogs crashed, the record would be lost with the catalogs.

  A convenient way to track the media is to configure the E-mail global attribute. When this is done, NetBackup sends an E-mail that indicates the status of each catalog backup and the media ID that was used. You can then print the E-mail or save it on a disk other than the disk containing the catalogs.

If the catalogs are intact, you can also find these media IDs in the Media Manager volume listing. The Status column shows 1 for these volumes. However, these IDs do not appear in the NetBackup media reports.

Media Density

Specifies the media density for Media Manager type media. Click the **Density** box to list the densities that Media Manager supports and select the desired density.

Caution A NetBackup catalog backup *will not* span a tape volume. All the backup data must fit on one tape. Therefore, it is *extremely* important to choose a media density that can hold all the data to be backed up.

Pathname (Disk Media type)

For disk media, this is the path to the directory where you want to store the catalog backup. Type the path in the field. For example:

```
C:\dbbackup
```

The path can be:

- A directory on a disk attached to the master server. NetBackup creates the directory if it does not exist.
- An NFS-mounted file system or a link to an NFS-mounted file system that grants write access to the root user.
- A shared directory on another computer. This shared directory must be available to the service account that the NetBackup Client service logs into at startup. By default, the startup account is set to System. To specify another account, start the **Services** application in the Control Panel. Then select the **NetBackup Client** service, click the **Startup** button, and specify the desired account.

Caution When backing up the catalogs to disk, observe the following precautions:

- Always back up to a physical disk other than the one containing the catalogs. For example, if your computer has two physical disks and the catalogs are on the first disk, back up the catalogs to the second disk. If you back up the catalogs to the same disk and that disk fails, both the catalogs and the backups are lost and it will be difficult or impossible to restore data for your NetBackup clients. By default, the catalogs are stored in the following locations, so the destination of your catalog backup must be on a different disk:

  install_path`\NetBackup\db`
  install_path`\Volmgr\database`
  install_path`\NetBackup\var`

Where the default *install_path* is `C:\Program Files\VERITAS`

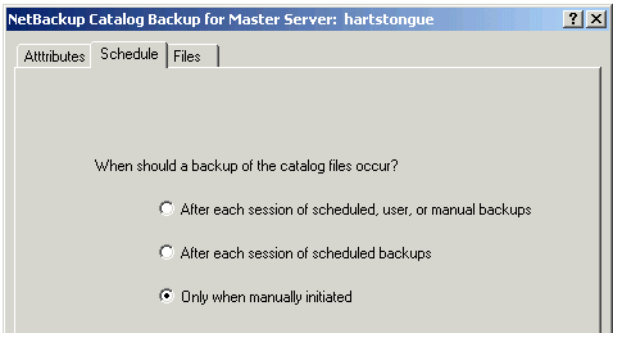
- Ensure that the disk has adequate space for the catalogs. If the disk fills up, the catalog backups will fail.
- Ensure that the path is a directory rather than a file. If the path is a file, an error occurs when the backup is done (*not* when you specify the path).
- The following rule applies to the path you specify:

  In addition to the platform-specific file path separators (/ and \) and colon (:) within a drive specification on Windows, use only alphabetic (ASCII A - X, a - z), numeric (0-9), plus (+), minus (-), underscore (_), or period (.) characters. Do not use a minus as the first character.

Catalog Schedule Tab

The Catalog **Schedule** tab contains selections concerning when you want to back up the catalogs.

Caution It is imperative that you back up your catalogs often. If these files are lost, you lose information about backups and configuration changes that were made between the time of the last catalog backup and the time that the disk crash occurred.



After each session of scheduled, user, or manual backups

Backups up the catalogs after any session that results in the creation of at least one successful backup or archive. This includes automatic, manual, and user backups.

After each session of scheduled backups

Backs up the catalogs after any automatic backup session that results in at least one successful backup of a client. A backup *does not* occur after a manual backup or a user backup or archive.

Only when manually initiated

Does not automatically back up the catalogs. If you elect to back up catalogs manually, select **Master Server** > **Catalog**, right-click **Catalog** and select **Back up NetBackup Catalog**.

Caution If you elect to back up catalogs manually, be certain to do so once a day or after every series of backups.

Recommendations

- If you are sending your catalog backups to a robot or tape stacker, a second standalone tape drive, or to disk, choose either of the two automatic backups.
- If you must use a single standalone tape drive to back up both catalog *and* business data, choose either:
  - If you will be running only one backup session per day or night, choose: **After each session of scheduled backups**
  - If you will be running multiple backup sessions in a single day or night, choose: **Only when manually initiated**

  Because NetBackup will not place catalog and regular backups on the same tape, both methods require you to swap tapes.

The general procedure for catalog backups when you have only one standalone drive is:

1. Insert the tape configured for catalog backups.
2. Manually start the backup. (See “Backing Up the Catalogs Manually” on page 159.)
3. When the backup is complete, remove the tape and store it in a safe place.

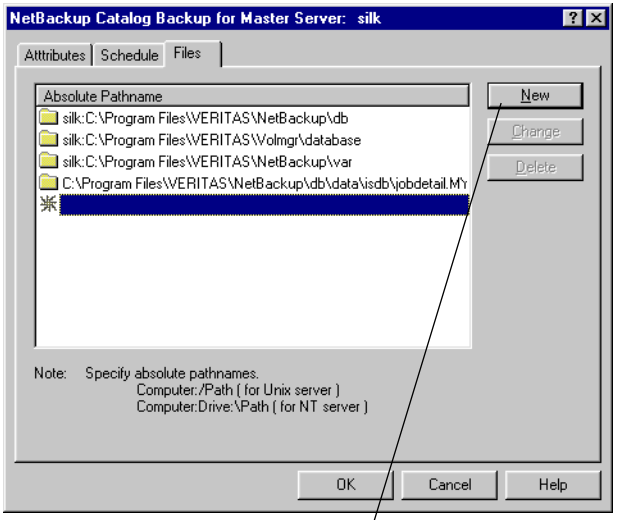
   The catalog-backup tape must be removed when the backup is done or regular backups will not occur. NetBackup does not mix catalog and regular backups on the same tape.

Catalog Files Tab

The Catalog **Files** tab contains the absolute pathnames to the catalog files to be backed up.

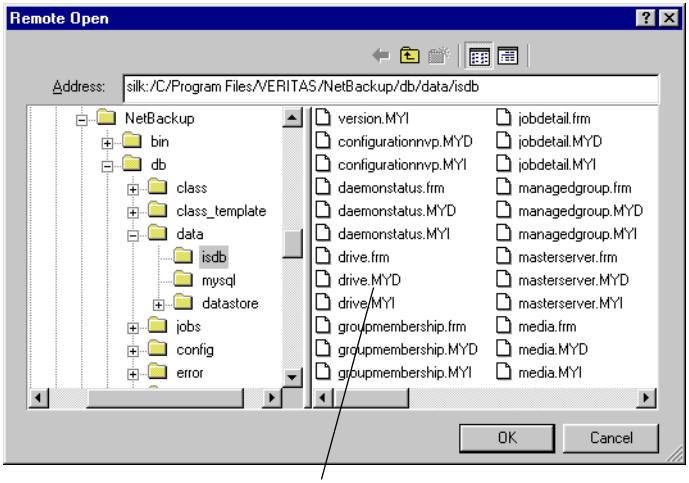
For more information on pathnames, see “Catalog Pathnames” on page 157 and “Pathnames for the NetBackup Database” on page 158.

The pathnames of the catalogs on the master server are automatically added during installation and generally require no action on your part other than to ensure they are listed.



Click to navigate to a database directory or database table

However, the pathnames to the NetBackup database on the media servers are *not* automatically added during installation and require that you add them to the file list.



Select the database directory or an individual table

▼ To add a pathname

1. Click **New**.
2. Type the pathname in the **Absolute Pathname** list. (See “Catalog Pathnames” on page 157.)

3. Click **OK** to complete the addition.

Caution Make sure there are no invalid paths in the list of catalog files to be backed up, especially if you've moved catalog files, deleted old paths, or added new paths to the catalog backup configuration. If NetBackup cannot find or follow a path, the entire catalog backup fails.

▼ To change a pathname

1. Double-click on the path under **Absolute Pathname**.
2. Change the pathname and click **OK**.

▼ To delete a pathname

1. Click on the path under **Absolute Pathname**.
2. Click **Delete**.

Catalog Pathnames

The pathnames of the catalogs on the master server are automatically added during installation and require no action on your part other than to ensure they are listed.

install_path`\NetBackup\db`

The files in this directory have NetBackup scheduling information, error logs, and all information about files backed up from client workstations.

install_path`\volmgr\database`

The files in this directory have the information about the media and devices being used in the configuration.

install_path`\NetBackup\var`

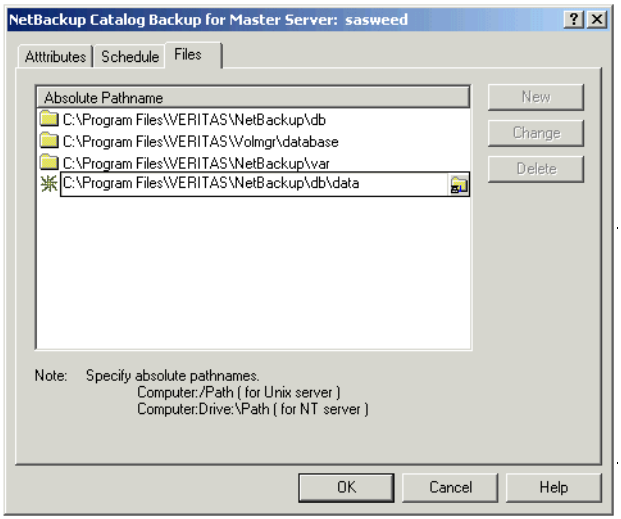
The files in this directory contain license key and authentication information.

Pathnames for the NetBackup Database

The pathnames to the NetBackup database on the master server are *not* automatically added during installation and require that you add them to the list. For example:

install_path`\NetBackup\db\data`

Note The table names and database names in the database pathname are case-sensitive. The database catalog backups will fail if typed without regard to case.



Backing Up the Catalogs Manually

A manual backup starts a backup of the catalogs immediately. Starting a manual backup is useful in the following situations:

- To perform an emergency backup. For instance, if you anticipate a problem or are moving the system and do not want to wait for the next scheduled catalog backup.
- You have only one standalone drive and no robots or tape stacker and are using the standalone drive for catalog backups. In this situation, automatic backups are not convenient because the catalog-backup tape must be inserted before each catalog backup and removed when the backup is done. The tape swapping is necessary because NetBackup does not mix catalog and regular backups on the same tape.

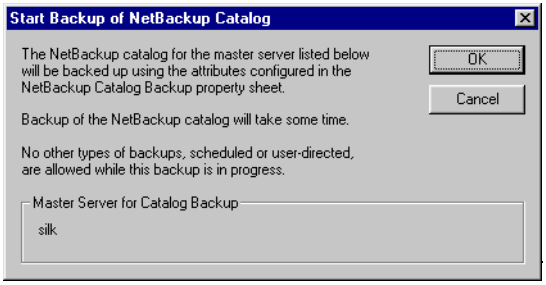
▼ To perform the catalog backup manually

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

   If your site has more than one master server, use **File** > **Change Server** to select a different server. (“ Administering a Remote Master Server” on page 320.)

2. Select **Actions** > **Backup NetBackup Catalog** to start the backup. The Start Backup of NetBackupdialog appears.

   The backup is saved to the least recently used of Media 1 and Media 2.



3. Click **OK** to continue the backup.

Note If the volume for the catalog backup is not in a drive, a mount request occurs and all catalog backups must wait for the mount before they can proceed. For a scheduled catalog backup, all other backups started by the scheduler must wait until the catalog backup is complete.

Protecting Large NetBackup Catalogs

It is very important to ensure that the NetBackup catalogs are backed up regularly. NetBackup provides a built-in mechanism for achieving this. However, this mechanism imposes a limit on the size of the data that can be backed up; namely, the data must all fit on a single piece of media.

This section describes a method that can be used to back up and recover the NetBackup catalog files if they become too large to fit onto a single tape.

Layout of the NetBackup Catalogs

Before implementing a solution for backing up large NetBackup catalogs across multiple tapes, it is important to understand the structure of the catalogs.

The NetBackup and Media Manager catalogs are held within subdirectories on the master server The NetBackup catalogs reside in the directory *install_path*`\NetBackup\db` and the Media Manager catalogs reside in *install_path*`\Volmgr\database`.

The directories under `db` contain further subdirectories or files, which together make up the NetBackup catalogs. The images directory contains a directory sub-tree, with one subdirectory for each NetBackup client that has been backed up (including the master server). Beneath these subdirectories are further directories and files, which hold the information about all the backup images held by NetBackup.

While most of the subdirectories in the NetBackup catalogs are relatively small, the images directory can grow to several tens, or even hundreds of gigabytes. (See “Determining Catalog Space Requirements” on page 166 for more information on estimating the size of the NetBackup catalogs.)

Due to its potentially large size, it is the images subdirectory that can become too large to fit onto a single tape and it is therefore this subdirectory that is addressed in the following sections.

Catalog Backup and Restore Concepts

The following sections present the concepts underlying multiple-tape catalog backups and restores.

Multiple-Tape Catalog Backups

The basic concept behind the protection of large NetBackup catalogs is to split the catalog-backup process into two steps:

1. Back up the majority of the data from the images subdirectory on the master server.
2. Back up a small sub-set of the images subdirectory, together with the remainder of the NetBackup and Media Manager catalog files and directories from the master server.

Since the first backup contains the majority of the data, it must be able to span tapes. This is achieved by using a normal NetBackup job to back up the data. As a result of this normal backup, an entry is placed in the images subdirectory tree for the master server. This catalog entry allows the user to browse the catalog for files during a restore operation.

The second backup must back up the portion of the images subdirectory that contains the catalog entries for the master server, together with the other parts of the NetBackup and Media Manager catalogs. Since this is a relatively small amount of data, it fits onto a single tape. It must also be possible to recover this backup without the NetBackup catalogs being available. This is achieved by using the normal NetBackup catalog-backup mechanism to perform the backups.

Multiple-Tape Catalog Restores

A restore of the NetBackup catalogs is also achieved in two steps. The first step is to use the most recent NetBackup catalog backup to recover the portion of the image catalog containing information about the backups taken from the master server, together with the other parts of the NetBackup and Media Manager catalogs on the master server.

Once this information has been recovered, NetBackup can be started and one of the user interfaces can be used to browse the files backed up from the master. These include the files and directories that constitute the NetBackup images catalog, which were backed up using the first step of the catalog backup described above. Using the normal restore process, these files and directories are restored, completing the operation. You must ensure the option **Overwrite Existing Files** is not selected, since this replaces the files previously recovered in stage 1.

Setting up Multiple-Tape NetBackup Catalog Backups

In order to configure NetBackup to perform multiple-tape backups of its catalogs, define a normal NetBackup policy and make changes to the NetBackup catalog-backup configuration. In addition, you must create a batch file to initiate the multiple-tape catalog backups. These steps are detailed below.

▼ To define a NetBackup policy for catalog backups

1. Use the NetBackup Administration Console to create a new policy with the following policy attributes:
   - Set the **Policy Type** to Standard if the master server is a UNIX machine or MS-Windows-NT if the master server is a Windows machine.
   - Do not choose **Cross Mount Points** if the master server is a UNIX or Windows 2000 machine.
   - Pick a suitable storage unit and volume pool.
   - Set **Limit Jobs per Policy** to 1.
   - Do not choose **Compression**.
   - Set **Job Priority** to 0.

2. Add the master server to the client list

3. Enter the following path in the file list:

   install_path`\NetBackup\db\images`

Note On UNIX, if `/usr/openv/netbackup/db/images` is a symbolic link to another filesystem, you MUST specify the true location of the images directory here. Symbolic links do not apply to Windows.

4. Set up schedules to meet your requirements. VERITAS recommends that the policy contains only a full backup schedule, since this will minimize tape mounting and positioning during restores.

   Do not set any backup windows for the schedules that you define. This ensures that the backup policy is never initiated automatically by the NetBackup scheduler. Instead, you must initiate the backup job manually.

5. Save your changes.

▼ To configure the NetBackup catalog backups

1. In the NetBackup Administration Console, ensure that the **Media Server** setting specifies the required backup server.

2. Specify the following for **Absolute Pathname**:

   masterserver : *install_path*`\NetBackup\db\c*`
   masterserver : *install_path*`\NetBackup\db\error`
   masterserver : *install_path*`\NetBackup\db\media`
   masterserver : *install_path*`\NetBackup\db\images\`*masterserver*
   masterserver : *install_path*`\var`

3. Change the schedule to **Only When Manually Initiated**. This stops the NetBackup catalog backups from running automatically and allows you to control when they run manually.

4. Select appropriate media types, densities, and IDs for the two catalog-backup media.

5. Save your changes.

Create a Batch File to Initiate the Backups

It is also important that the second-stage backup of the NetBackup catalogs occurs directly after the first-stage backup. A good way to ensure this is to write a batch file that initiates both backups, one after the other. The following is an example batch file for backing up the catalogs:

```
REM ------------------------------------------------------------------
REM -     Catalog backup batch file -
REM -     Performs a two-stage backup of the NetBackup catalogs -
REM ------------------------------------------------------------------
@ECHO OFF

REM Change to the name of the correct policy
SET POLICY=nbu_db_backup
REM Change to the name of the correct schedule
SET SCHED=full_backup
ECHO Running first stage catalog backup
C:\Install_path\VERITAS\NetBackup\bin\bpbackup.exe -w -i -c POLICY -s SCHED
IF NOT ERRORLEVEL O GOTO FATL_ERR_1

ECHO Running second stage catalog backup
C:\Install_path\VERITAS\NetBackup|bin\admincmd\bpbackupdb.exe
IF ERRORLEVEL > O GOTO FATL_ERR_2
GOTO END

:FATL_ERR_1
ECHO Fatal Error! Catalog backup Phase 1 failed.
GOTO END
:FATL_ERR_2
ECHO Fatal Error! Catalog backup Phase 2 failed.
GOTO END

:END
```

How To Initiate a Multiple-Tape Catalog Backup

Similar to how the automatic-catalog backup works, it is important to ensure that no other NetBackup operations that modify the NetBackup catalogs are in progress while the two catalog backups are performed. Such operations include:

- Backups and archives
- Catalog compression
- TIR record expiration or retrieval (during a restore operation)
- Catalog image record expiration
- Image imports
- Image duplication

Performing the catalog backups when any of these operations are in progress can cause an inconsistent catalog backup.

Since both image import and image duplication operations must be initiated manually by the NetBackup administrator, it is relatively easy to ensure that these are not in progress during the catalog backup. However, it is more difficult to ensure that no backups or restores are running, since both the NetBackup scheduler and other users can initiate these.

More difficult still, are operations that are started automatically by NetBackup, such as catalog compression, TIR record expiration or retrieval, and image record expiration. Due to the way the NetBackup scheduler interlocks processes, do not start the two-step backup batch file with the *install_path*`\NetBackup\bin\session_notify` script. We suggest using another scheduler to start the two-step backup batch file or run it manually when the above operations are not occurring.

Managing the NetBackup Catalogs

This section explains the following aspects of managing the NetBackup catalogs:

- "About the Binary Catalog Format" on page 191
- "Determining Catalog Space Requirements" on page 166
- "Compressing the Image Catalog" on page 170
- "Moving the NetBackup Image Catalog" on page 171
- "Reduce Restore Times by Indexing the Image Catalog" on page 173

About the Binary Catalog Format

Maintaining the catalog in a binary file format has several advantages to maintaining the catalog in a text format.

- The catalog is more compact in binary format. The binary representations of numbers, dates, etc. takes up less disk space than the text representations.
- The catalog in binary format is much faster to browse and search, especially for very large file sizes.
- The catalog in binary format supports alternate backup methods without requiring post-processing, improving catalog performance for alternate backup methods.

Upon installation, NetBackup does *not* convert existing ASCII catalogs to the new binary catalog format. However, any new catalogs created will be binary. You may elect to upgrade any existing NetBackup catalogs to binary format using the catalog conversion utility, `cat_convert`, described below.

Catalog Conversion Utility

In order to allow users to convert from ASCII to binary, or from binary to ASCII, NetBackup offers a catalog format conversion utility called `cat_convert`. The utility converts NetBackup catalog `.f` files between version 3.4, 4.0V or 4.5 ASCII format and 4.5 binary format. `cat_convert` automatically detects the source catalog file format and converts it to the other format.

Binary Catalog File Limitations

There are a few size limitations associated with the binary catalog to keep in mind.

- The maximum number of files that can be backed up per image:

  $(2^{31}) - 1$ files = 2,147,483,647 files = 7FFFFFFF files

- The maximum number of different user IDs and group IDs (combined):

  $(2^{31}) - 1$ IDs = 2,147,483,647 IDs = 7FFFFFFF IDs

Determining Catalog Space Requirements

NetBackup requires disk space to store its error logs and information about the files it backs up. The maximum amount of disk space that NetBackup requires at any given time varies according to the following factors:

- Number of files that you are backing up
- Frequency of full and incremental backups
- Number of user backups and archives
- Retention period of backups
- Average length of full pathname of files
- File information (such as owner permissions)
- Average amount of error log information existing at any given time

▼ To estimate the disk space required for a catalog backup

1. Estimate the maximum number of files that each schedule for each policy backs up during a single backup of all its clients.

   shows that a full backup for policy S1 includes 64,000 files.

2. Determine the frequency and retention period of the full and incremental backups for each policy.

3. Use the information from steps 1 and 2 above to calculate the maximum number of files that exist at any given time.

   For example:

   Assume you schedule full backups every seven days with a retention period of four weeks and differential incremental backups daily with a retention period of one week. The number of file paths you must allow space for is four times the number of files in a full backup plus one week's worth of incrementals.

   The following formula expresses the maximum number of files that can exist at any given time for each type of backup (daily, weekly, etc.):

   Files per Backup x *Backups per Retention Period* = *Max Files*

   For example:

If a daily differential incremental schedule backs up 1200 files for all its clients and the retention period is seven days, the maximum number of files resulting from these incrementals that can exist at one time are:

1200 x 7 days = 8400

If a weekly full backup schedule backs up 3000 files for all its clients and the retention period is four weeks, the maximum number of files due to weekly-full backups that can exist at one time are:

3000 x 4 weeks = 12,000

Obtain the total for a server by adding the maximum files for all the schedules together. The maximum number of files that can exist at one time due to the above two schedules is the sum of the two totals, which is 20,400.

Note For policies that collect true-image-restore information, an incremental backup collects catalog information on all files (as if it were a full backup). This changes the above calculation for the incremental from 1200 x 7 = 8400 to 3000 x 7 = 21,000. After adding 12,000 for the fulls, the total for the two schedules is 33,000 rather than 20,400.

4. Obtain the number of bytes by multiplying the number of files by the average length of the file's full pathnames and file information.

Determining the space required for binary catalogs:

If you are unsure of the average length of a file's full pathname, use 100. Using the results from the examples in step 3, yields:

(8400 x 100) + (12,000 x 100) = 1992 kilobytes (1024 bytes in a kilobyte)

Determining the space required for ASCII catalogs:

If you are unsure of the average length of a file's full pathname, use 150. (Averages from 100 to 150 are common.) Using the results from the examples in step 3, yields:

(8400 x 150) + (12,000 x 150) = 2988 kilobytes (1024 bytes in a kilobyte)

Note If you have ASCII catalogs and use catalog indexing, multiply the number in step 4 by 1.5%.

5. Add 10 to 15 megabytes to the total calculated in step 4. This is the average space for the error logs. Increase the value if you anticipate problems.

6. Allocate space so all this data remains in a single partition.

File Size Considerations

File system limitations:

- For a FAT 32 file system, the maximum file size is 4GB.
- Some UNIX systems have a large file support flag. Turn the flag ON to enable large file support. For example, AIX disables large file support by default, so the file size limit is 2GB.
- Linux does not support files larger than 2GB.

One file size and security-related limitation:

For UNIX systems, set the file size limit for the root user account to *unlimited* in order to support large file support.

Example

"Example Reference Table for Catalog Requirements" on page 169 shows backup schedules, retention times, and number of files for a group of example policies. By substituting the information from this table into the formula from step 3 above, we can calculate the maximum number of files for each policy. The following steps demonstrate this for policy S1:

1. Apply the following formula to policy S1:

   Max Files equals:

   (*Files per Incremental* x *Backups per Retention Period*)
   +
   (*Files per Monthly Full Backups* x *Backups per Retention Period*)

2. Substitute values from "Example Reference Table for Catalog Requirements" on page 169:

   1000 files x 30 + 64,000 files x 12 = 798,000 files

   Perform steps 1 and 2 for each policy. Adding the results together shows that the total files for all policies is:

   4,829,600 files

   Multiply the total number of files by the bytes in the average path length and statistics (100 for this example). The total amount of disk space required for file paths is:

   460.59 megabytes (1,048,576 bytes in a megabyte)

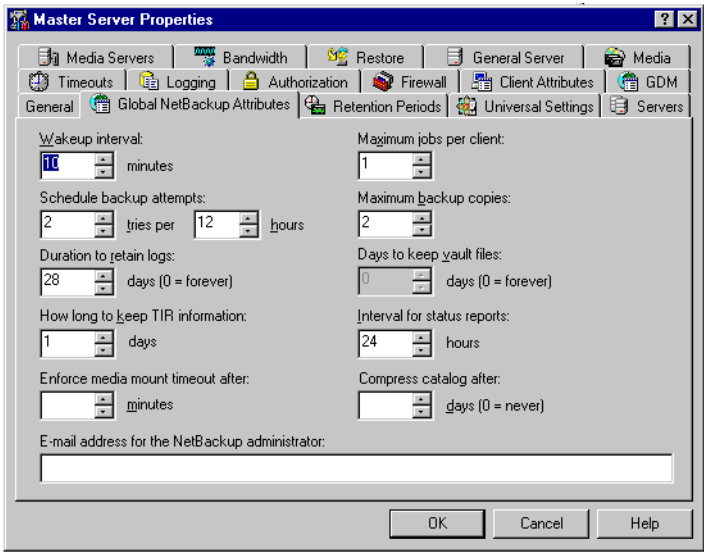
Add 15 megabytes for error logs results in a final uncompressed catalog space requirement of:

475.59 megabytes

Example Reference Table for Catalog Requirements

Policy	Schedule	Backup Type	Retention	Number of Files
S1	Daily	Incremental	1 month	1000
	Monthly	Full	1 year	64,000
S2	Daily	Incremental	1 month	1000
	Monthly	Full	1 year	70,000
S3	Daily	Incremental	1 week	10,000
	Weekly	Full	1 month	114,000
	Monthly	Full	1 year	114,000
S4	Daily	Incremental	1 week	200
	Weekly	Full	1 month	2000
	Monthly	Full	3 months	2000
	Quarterly	Full	Infinite	2000
WS1	Daily	Incremental	1 month	200
	Monthly	Full	1 year	5600
WS2	Daily	Incremental	1 week	7000
	Weekly	Full	1 month	70,000
	Monthly	Full	1 year	70,000

Compressing the Image Catalog



The image catalog has information about all client backups and is accessed when a user lists or restores files. NetBackup offers you the option of compressing all or older portions of this catalog. There is no method to selectively compress image-catalog files other than by age.

Control image-catalog compression by setting the the Global NetBackup attribute, **Compress Catalog After**. This attribute specifies how old the backup information must be before it is compressed, thereby letting you defer compression of newer information and not affect users who are listing or restoring files from recent backups. By default, **Compress Catalog After** is set to 0 and image compression is not enabled.

For more information, see “Global NetBackup Attributes Tab” on page 242.

Caution Do not use other methods to compress or uncompress the image-catalog files. This practice causes inconsistent image-catalog entries and can produce incorrect results when users list and restore files.

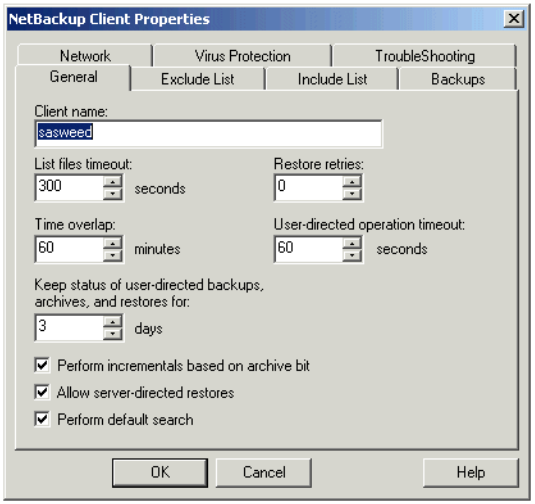
The catalog must be in an NTFS partition for compression to occur. If you choose to compress the image catalog, NetBackup uses NTFS compression on the server to perform compression after each backup session, regardless of whether successful backups were performed. The operation occurs while the scheduler is expiring backups and before running the `session_notify` script and the backup of the NetBackup catalogs.

When numerous compressed image-catalog files must be processed, the backup session is extended until compression is complete. The additional backup time is especially noticeable the first time you perform compression. To minimize the impact of the initial sessions, consider compressing the files in stages. For example, you can start by compressing records for backups older than 120 days and then reduce this value over a period of time until you reach a comfortable setting.

Compressing the image catalog can greatly reduce the disk space used as well as the amount of media required to back up the catalog. The amount of space you reclaim varies with the types of backups you perform. Full backups result in a larger percentage of

catalog compression than incremental backups because there is normally more duplication of data in a catalog file for a full backup. A reduction of 80 percent is sometimes possible.

This reduction in disk space and media requirements is achieved at the expense of performance when a user lists or restores files. Since the information is uncompressed at each reference, performance degradation is in direct proportion to the number and size of compressed files that are referenced. If the restore requires numerous catalog files to be uncompressed, you may have to increase the time-out value associated with list requests by changing the **List Files Timeout** General property setting on the client.



1. Select the images. The images are located under the following directory:

   install_path`\NetBackup\Images\Clients`

2. On the **Properties** tab, clear the **Compress** box.
3. Click **OK**.

Moving the NetBackup Image Catalog

If the NetBackup catalog is too large for its current disk partition you can move image information for individual clients to another partition.

▼ To move the NetBackup image catalog

1. Back up the NetBackup catalogs. (See “Backing Up the Catalogs Manually” on page 159.)

   This ensures that you can recover image information in case something is accidentally lost during the move.

2. Check the **Jobs** tab in the Activity Monitor and ensure that no backups or restores are running for the client.

   If jobs are running, either wait for them to end or stop them by using the **Jobs** tab in the Activity Monitor.

3. Use the **Services** tab in Activity Monitor to stop the Request Manager and Database Manager services.

   This prevents jobs from starting and the database from being modified while you are performing this procedure.

4. Create a file named `ALTPATH` in the image catalog directory.

   For example, if NetBackup is installed in its default location and the client name is mars, the path to the image catalog is:

   `C:\Program Files\VERITAS\NetBackup\db\images\mars\ALTPATH`

5. Create the directory to which you intend to move the image information. For example:

   `E:\NetBackup\alternate_db\images\`*client_name*

6. On the first line of the `ALTPATH` file, specify the path to the directory where you intend to move the client's image information. For example:

   `E:\NetBackup\alternate_db\images\`*client_name*

   This will be the only entry in the `ALTPATH` file.

7. Move all files and directories (except the `ALTPATH` file) that are in the current client directory to the new directory.

   For example, if the images are currently in

   `C:\Program Files\VERITAS\NetBackup\db\images\mars`

   and the `ALTPATH` file specifies

   `E:\NetBackup\alternate_db\images\mars`

   then move all files and directories (except the `ALTPATH` file) to

   `E:\NetBackup\alternate_db\images\mars`

8. Add the new image directory to the NetBackup catalog backup configuration. (See "Catalog Files Tab" on page 156.)

   In the above example, you would add

   `E:\NetBackup\alternate_db\images\mars`

Caution Failure to add the alternate image directory to the catalog-backup configuration can result in loss of backup data if there is a disk failure.

9. Start the NetBackup Request Manager and NetBackup Database Manager services by using the Services tab in the Activity Monitor.

   Backups and restores can now resume for the client.

Converting the Catalog Format

Upon installation, NetBackup does *not* convert existing ASCII catalogs to the new binary catalog format. However, any new catalogs created will be binary. You may elect to upgrade any existing NetBackup catalogs to binary format using the catalog conversion utility, `cat_convert`, described below.

Maintaining the catalog in a binary file format has several advantages to maintaining the catalog in a text format.

- The catalog is more compact in binary format. The binary representations of numbers, dates, etc. takes up less disk space than the text representations.
- The catalog in binary format is much faster to browse and search, especially for very large file sizes.
- The catalog in binary format supports alternate backup methods without requiring post-processing, improving catalog performance for alternate backup methods.

In order to allow users to convert from ASCII to binary, and binary to ASCII, NetBackup offers a catalog format conversion utility called `cat_convert`. The utility converts NetBackup catalog `.f` files between version 3.4, 4.0V or 4.5 ASCII format and 4.5 binary format. `cat_convert` automatically detects the source catalog file format and converts it to the other format.

Reduce Restore Times by Indexing the Image Catalog

If you have large numbers of backups, reduce the total time required to restore files by creating indexes of the backed up files that are recorded in the NetBackup image catalog. NetBackup can then use the indexes to go directly to the catalog entry for a file rather than starting the search at the beginning of the catalog entries.

Note This section applies to ASCII catalogs only. Binary catalogs do not need catalog indexing.

Use the following command to generate indexes for one or all clients, and for up to nine levels of directories:

install_path`\NetBackup\bin\index_clients.cmd` *level client_name*

Where:

- *level* is the number of directory levels (1 to 9) to be indexed. The levels refer to the directories from where files were backed up on the client.

  For example, if you're searching for `C:\payroll\smith\taxes\01` and *level* is 2, NetBackup starts the search at `C:\payroll\smith`. The default is 9.

- *client_name* is the name of the client of the backups you want to index. The default is all clients.

Run this command once, to activate indexing for a client. Once activated, indexing is done automatically each night when NetBackup does its cleanup for the previous day's activities.

Catalog Index Examples

- To index client mars to index level 5 (five levels of directories), run:

  install_path`\NetBackup\bin\index_clients.cmd 5 mars`

- To index selected clients, run a command for each of them (you cannot use wildcards). The following indexes clients named mars, jupiter and neptune to index level 5:

  install_path`\NetBackup\bin\index_clients.cmd 5 mars`

  install_path`\NetBackup\bin\index_clients.cmd 5 jupiter`

  install_path`\NetBackup\bin\index_clients.cmd 5 neptune`

- To index all NetBackup clients to index level 3, run:

  install_path`\NetBackup\bin\index_clients.cmd 3`

- To index all NetBackup clients to index level 9, run:

  install_path`\NetBackup\bin\index_clients.cmd`

Note Changing the index level affects only future index creation and does not immediately create index files.

Catalog Index Space Requirements

The index files do not require much space. Regardless of how many clients you have, indexing all clients to level 9 requires about 1.5 percent more space in the NetBackup catalog than if you do not use indexing for any clients. NetBackup does not produce index files for backups that contain less than 200 files.

The index files reside in a directory named:

install_path`\NetBackup\db\images\`*clientname*`\INDEX`

The indexing level resides in a file named:

install_path`\NetBackup\db\images\`*clientname*`\INDEXLEVEL`

Note If you are collecting true-image restore information, the `INDEX` files take much more space for incrementals.

Disabling Catalog Indexing

Note When using a binary catalog, disable catalog indexing.

- To stop NetBackup from generating new `INDEX` files for a client, delete the `INDEXLEVEL` file. NetBackup continues to use existing `INDEX` files.
- To temporarily stop using the `INDEX` files during searches but retain existing index files, change the `INDEX` directory to `INDEX.ignore`. When you are done, change `INDEX.ignore` back to `INDEX` to resume indexing.
- To permanently eliminate `INDEX` files for a client, delete the `INDEX` directory and the `INDEXLEVEL` file.

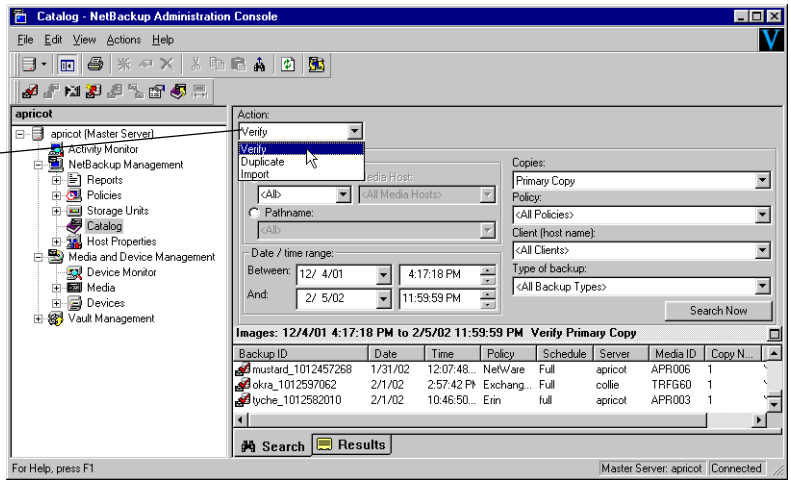
Searching for Backup Images

Use **Catalog** to search for a backup image. You may want to search for a backup image in order to:

- Verify the backup contents with what is recorded in the NetBackup catalog.
- Duplicate the backup image to create up to 10 copies.
- Promote a copy of a backup to be the primary backup copy.
- Expire backup images.

- Import expired backup images or images from another NetBackup server.

Specify Verify, Duplicate, or Import, depending on the desired operation



NetBackup uses the following criteria to build a list of backups from which you can make your selections.

Search Criteria for Backup Images

Search Criteria	Description
Action	Select the action that was used to create the image for which you're looking: **Verify**, **Duplicate**, **Import**.
Media ID	The media ID for the volume that contains the desired backups. Type a media ID in the box or select one from the scroll-down list. To search on all media, select **<All>**.
Media Host	The host name of the media server that produced the originals. Type a host name in the box or select one from the scroll-down list. To search through all hosts, select **All Media Hosts**.
Pathname	To search for an image on a disk storage unit, select **Pathname** and specify the file path that includes the originals.
Date/time range	The range of dates and times that includes all the backups for which you want to search. The default range is determined by the Global attribute setting, **Interval for status reports**.
Copies	The source you want to search. From the scroll-down list, select either **Primary** or the copy number.

Search Criteria for Backup Images (continued)

Search Criteria	Description
Policy	The policy under which the selected backups were performed. Type a policy name in the box or select one from the scroll-down list. To search through all policies, select **All Policies**.
Client (host name)	The host name of the client that produced the originals. Type a client name in the box or select one from the scroll-down list. To search through all hosts, select **All Clients**.
Type of backup	The type of schedule that created the backups for which you are searching. Type a schedule type in the box or select one from the scroll-down list. To search through all schedule types, select **All Backup Types**.

Notes on Searching for an Image

When searching for a:

- Duplication image: If the original is fragmented, NetBackup duplicates only the fragments that exist on the specified volume.
- Verification image: Backups that have fragments on another volume are included, as they exist in part on the specified volume.
- Import image: If a backup begins on a media ID that has not been processed by Step 1, it is not imported. If a backup ends on a media ID that has not been processed by Step 1, the imported backup is incomplete

Verifying Backup Images

NetBackup can verify the contents of a backup by reading the volume and comparing its contents to what is recorded in the NetBackup catalog.

Although this operation does not compare the data on the volume with the contents of the client disk, it does read each block in the image to verify that the volume is readable. (However, data corruption within a block could be possible.) NetBackup verifies only one backup at a time and tries to minimize media mounts and positioning time.

▼ To verify backup images

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

2. Set up the search criteria for the image you wish to verify as explained in the "Search Criteria for Backup Images" table. Click **Search Now**.

3. Select the image you wish to verify and select **Actions > Verify**. The Confirm Verify dialog appears.

   To display information on each file that NetBackup verifies, select **Enable full logging**.

4. Click the **Results** tab, then select the verification job just created to view the job results. See "Viewing Job Results" on page 189.

Duplicating Backup Images

NetBackup can create up to 10 copies of unexpired backups. Indicate the number of backup copies in **Host Properties** > **Master Servers** > **Global Attributes** > **Maximum backup copies**. See "Global NetBackup Attributes Tab" on page 242.

If is licensed, NetBackup can create up to four of the copies simultaneously. (See the note below.)

NetBackup does not verify in advance whether the storage units and drives required for the duplicate operation are available for use, only that the destination storage unit exists.

The following lists describe scenarios which present candidates for duplication and scenarios where duplication is not possible:

Possible to duplicate backups:	Not possible to duplicate backups:
- from one storage unit to another. - from one media density to another. - from one server to another. - from multiplex to nonmultiplex format. - from multiplex format and retain the multiplex format on the duplicate. The duplicate can contain all or any subset of the backups that were included in the original multiplexed group. This is done with a single pass of the tape. (A multiplexed group is a set of backups that were multiplexed together during a single session.)	- while the backup is being created. - when the backup has expired. - using the NetBackup scheduler to automatically schedule duplications. - of the NetBackup catalogs. - when it is a multiplexed duplicate of the following: – NDMP backup – Backups from disk type storage units – Backups to disk type storage units – Nonmultiplexed backups

Note Do not duplicate images while a NetBackup catalog backup is running. This results in the catalog backup not having information about the duplication.

Notes on Multiplexed Duplication

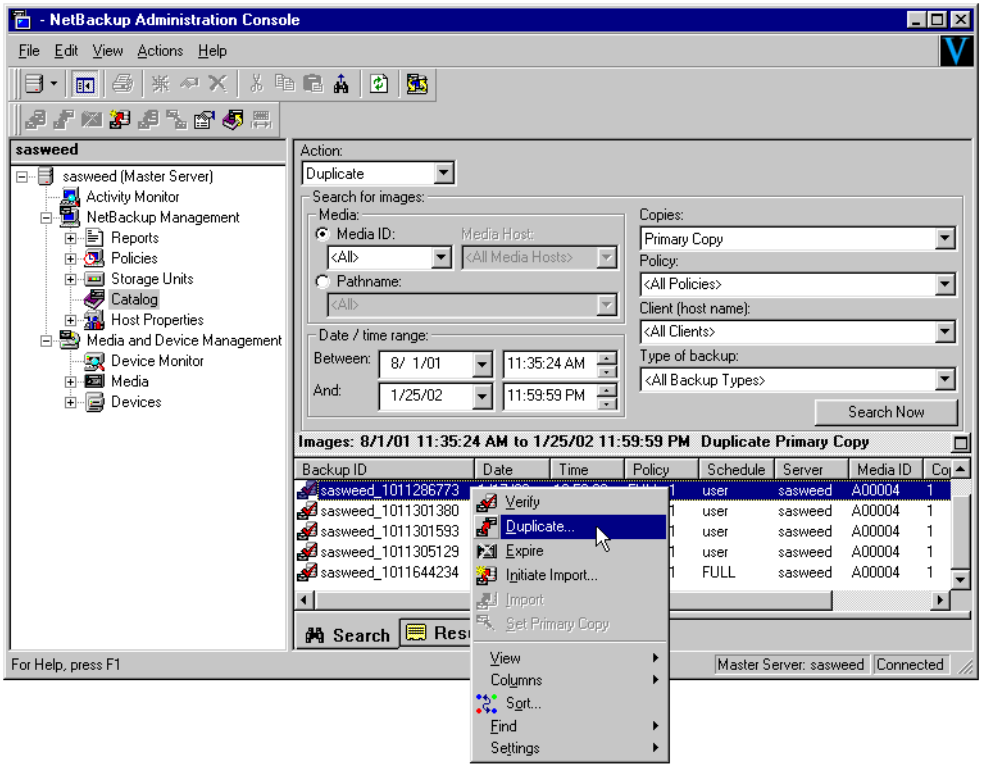
- When duplicating multiplexed backups, the multiplex settings of the destination storage unit and the original schedule are ignored. However, if multiple multiplexed groups are duplicated, the grouping within each multiplexed group is maintained. This means that the duplicated groups will have a multiplexing factor that is no greater than that used during the original backup.
- If all backups in a multiplexed group are duplicated to a storage unit that has the same characteristics as the one where the backup was originally performed, the duplicated group will be identical, with the following exceptions:
  - If EOM (end of media) is encountered on either the source or destination media.
  - If any of the fragments in the source backups are zero length (occurs if many multiplexed backups start at the same time), then during duplication these zero length fragments are removed.

▼ To duplicate backup images

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

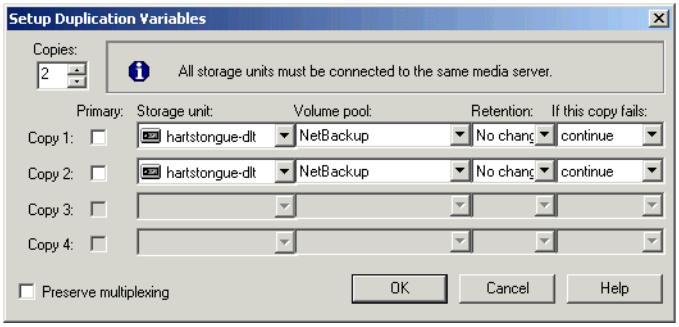
2. Set up the search criteria for the image you wish to duplicate. Click **Search Now**.

3. Right-click the image you wish to duplicate and select **Duplicate** from the shortcut menu. The **Setup Duplication Variables** dialog appears.



4. Specify that one copy is to be created. If Vault is installed, you may create more than one copy.

   If Vault is installed and there are enough drives available, the copies will be created simultaneously. Otherwise, the system may require operator intervention if, for instance, four copies are to be created and there are only two drives.



5. The primary copy is the copy from which restores will be done. Normally, the original backup will be the primary copy.

   If you want one of the duplicated copies to become the primary copy, check the appropriate box, otherwise leave the fields blank.

6. Specify the storage unit where each copy will be stored. If a storage unit has multiple drives, it can be used for both the source and destination. Disk-type storage units may be used if only one copy is to be made.

Note Inline Tape Copy does not support the following storage types: NDMP, third-party copies, EMC Fastrax, disk storage units, or optical devices.
Also, Inline Tape Copy does not support storage units that use a QIC (quarter-inch cartridge) drive type.

7. Specify the volume pool where each copy will be stored.

   NetBackup does not verify in advance that the media ID selected for the duplicate copy is not the same as the media ID of the volume that contains the original backup. Because of this potential deadlock, specify a different volume pool to ensure a different volume is used.

8. Select the retention level for the copy, or select *No change*.

   The duplicate copy shares many attributes of the primary copy, including backup ID. Other attributes, such as elapsed time, apply only to the primary. It is the primary copy that NetBackup uses to satisfy restore requests.

   - If *No Change* is selected for the retention period, the expiration date is the same for the duplicate and source copies. You can use the `bpexpdate` command to change the expiration date of the duplicate.

- If a retention period is indicated, the expiration date for the copy is the backup date plus the retention period. For example, if a backup was created on November 14, 2001 and its retention period is one week, the new copy's expiration date is November 21, 2001.

9. Specify whether the remaining copies should continue or fail if the specified copy fails.

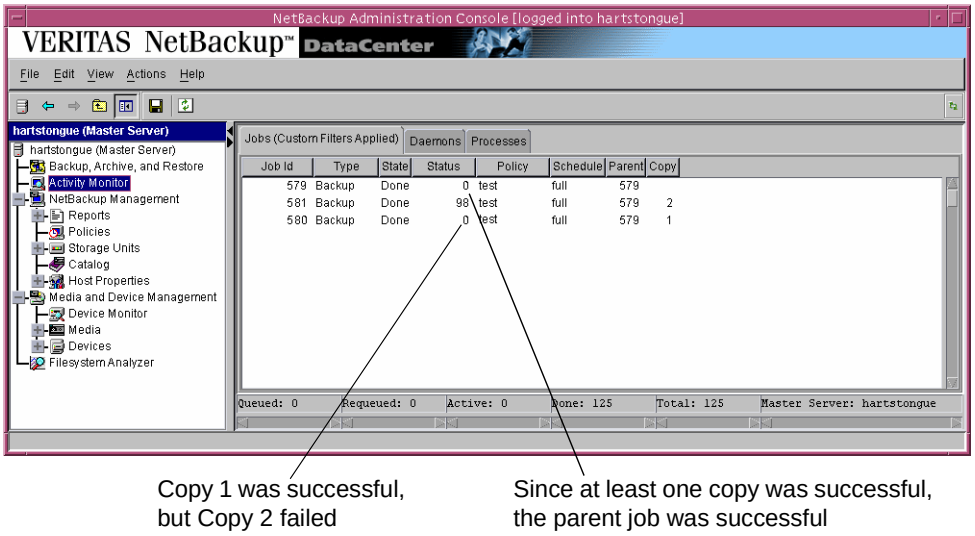
10. If the selection includes multiplexed backups and the backups are to remain multiplexed in the duplicate, check **Preserve Multiplexing**. If you do not duplicate all the backups in a multiplexed group, the duplicate will have a different layout of fragments. (A multiplexed group is a set of backups that were multiplexed together during a single session.)

    By default, duplication is done serially and attempts to minimize media mounts and positioning time. Only one backup is processed at a time. If **Preserved Multiplexing** is enabled, NetBackup first duplicates all backups that cannot be multiplex duplicated before the multiplexed backups are duplicated.

11. Click **OK** to start duplicating.

12. Click the **Results** tab, then select the duplication job just created to view the job results. See "Viewing Job Results" on page 189.

The following example shows a backup with two copies. The parent job is 579, copy 1 is job 580, and copy 2 is job 581. Copy 1 finished successfully, but copy 2 failed with a 98 status (error requesting media). Since at least one copy finished successfully, the parent job shows a successful (0) status.



Promoting a Copy to a Primary Copy

Each backup is assigned a *primary copy*. NetBackup uses the primary copy to satisfy restore requests. If the primary copy is unavailable and you have created a duplicate, select a copy of the backup and set it to be the primary copy.

▼ To promote a backup copy to a primary copy

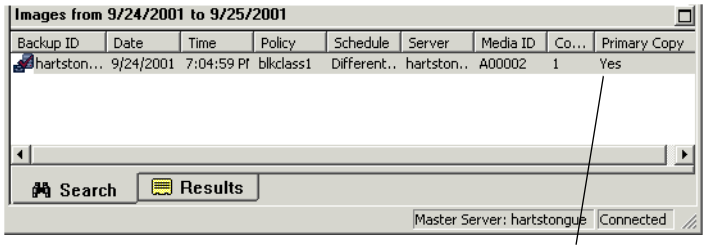
1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

2. Set up the search criteria for the image you wish to promote to a primary copy. (See "Searching for Backup Images" on page 175.) Be sure that you've indicated a copy in the **Copies** field and not **Primary Copy**. Click **Search Now**.

3. Select the image you wish to promote.

4. Click **Actions > Set Primary Copy**.

After promoting to the primary copy, the Primary Status column immediately reads **Yes**.



Primary Copy status indicates that the image is now the primary copy

You can also promote a backup copy to a primary copy using the command line.

▼ To promote a backup copy to a primary copy using bpduplicate

1. Enter the following command:

install_path`\NetBackup\bin\admincmd\bpduplicate -npc` *pcopy* `-backupid` *bid*

Where:

install_path is the directory were NetBackup is installed.

pcopy is the copy number that will become the new primary copy.

bid is the backup identifier as shown in the Images on Media report.

To find the volume that has the duplicate backup, use the Images on Media report. Specify the backup ID which is known (and also the client name if possible to reduce the search time). The report shows information about both copies. See “Images on Media Report” on page 206.

The `bpduplicate` command writes all output to the NetBackup logs so nothing appears in the command window.

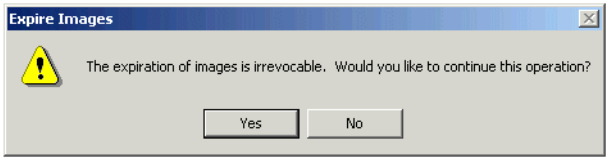
After promoting the duplicate to the primary copy, use the Backup, Archive and Restore interface on a client to list and restore files from the backup. See the *NetBackup User’s Guide* for instructions.

Expiring Backup Images

To expire a backup image means to force the retention period to expire. When the retention period expires, NetBackup deletes information about the backup, making the files in the backups unavailable for restores without first reimporting.

▼ To expire a backup image

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.
2. Set up the search criteria for the image you wish to expire as explained in the table, “Search Criteria for Backup Images” on page 176. Click **Search Now**.
3. Select the image you wish to expire and select **Actions** > **Expire**.
4. A message appears telling you that once the backups have been expired, they cannot be used for restores.



5. Select **Yes** to proceed with expiring the image or **No**.

Importing Backup Images

NetBackup can import backups that have expired, or are from another NetBackup server. During an import operation, NetBackup recreates NetBackup catalog entries for the backups that are on the imported volume. This option is useful for moving volumes from one site to another and for recreating NetBackup catalog entries for expired backups.

The expiration date for the imported items is the current date plus the retention period. For example, if a backup is imported November 14, 2001 and its retention period is one week, the new expiration date is November 21, 2001.

Notes About Importing Backup Images

- NetBackup does not direct backups to imported volumes.
- To import from a volume that has the same media ID as an existing volume (for example A00001) on this server, first duplicate the existing volume to another media ID (for example, B00001). Then, remove information about the existing media ID that is causing the problem (in this example, A00001) from the NetBackup catalog by running the following command:

install_path`\NetBackup\admincmd\bin\bpexpdate -d 0 -ev` *media ID*

  Next, delete the existing media ID that is causing the problem (in this example, A00001) from Media Manager on this server. Finally, add the volume you are importing (the other A00001) to Media Manager on this server. The *Media Manager System Administrator's Guide* contains instructions for deleting and adding volumes.

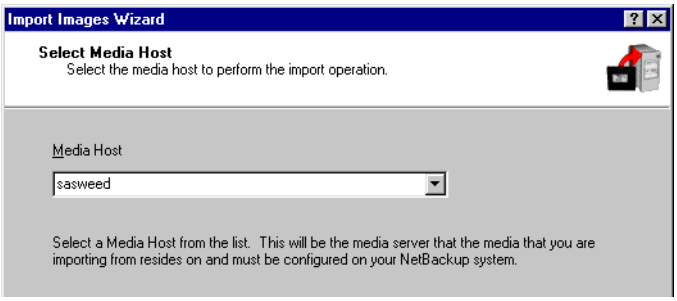
  To avoid this problem in the future, use unique prefix characters for media IDs on all servers.

- You cannot import a backup if an unexpired copy of it already exists on the server where you are trying to import it.
- You cannot import data from disk-image.

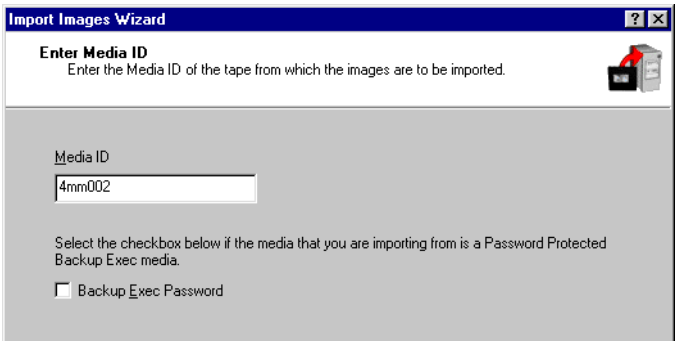
▼ To import backup images using the Import Images Wizard

1. Add the media IDs that have the backups to Media Manager on the server where you are going to import the backups.
2. Select **Import Images** in the right pane to launch the wizard. **Import Images** is available when **Master Server** or **NetBackup Management** is selected.
3. The wizard explains the 2-step import process. This wizard takes you through Phase I. Click **Next**.

4. Type the name of the host that contains the volume you are going to import. Click **Next**.

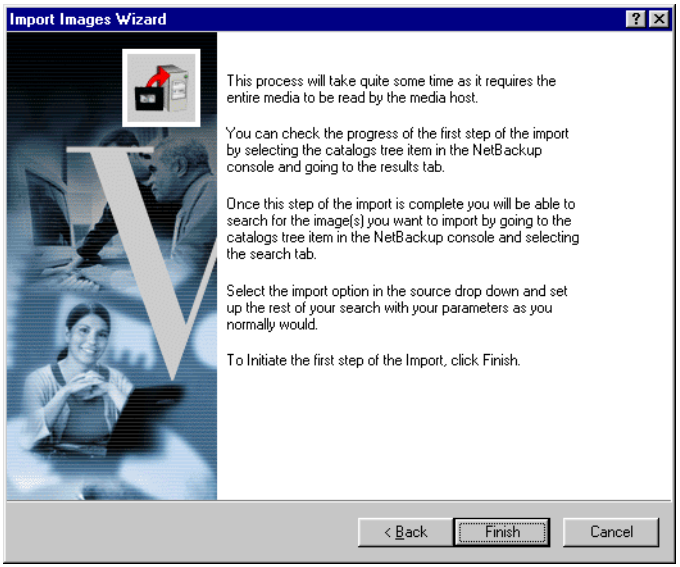


5. Type the Media ID of the volume that contains the backups you are importing. Click **Next**.



6. Click **Finish**. The wizard explains how to check the progress as the media host reads the media. (See "Viewing Job Results" on page 189.)

7. To complete the import, see "To import backup images – Phase II" on page 188.



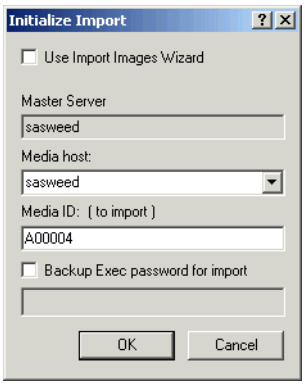
▼ To initiate an import without the Import Wizard – Phase I

The result of initiating an import is to create a list of expired images from which you can select images to import. However, no importing occurs at this stage.

1. Add the media IDs that have the backups to Media Manager on the server where you are going to import the backups.

2. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

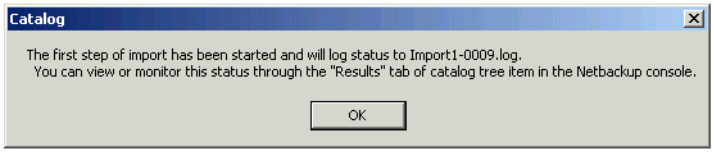
3. Select **Actions > Initiate Import**. The Initialize Import dialog appears.



   - The **Master Server** field indicates the master server to which you are importing the images.
   - In the **Media Host** field, specify the name of the host that contains the volume you are going to import.
   - In the **Media ID (to import)** field, type the Media ID of the volume that contains the backups you are importing.
   - If you're importing Backup Exec images, check **Backup Exec Password for Import**, then enter the password.

   Click **OK**. The Catalog dialog appears.

4. Click **OK** to start the process of reading the catalog information from the source volume.



5. Click on the Catalog Results tab to see NetBackup look at each image on the tape and determine whether or not it has expired and can be imported. The job also displays in Activity Monitor as an Import type. Select the import job log just created to view the job results.

Note Since it is necessary to mount and read the tape at this phase, reading the catalog and building the list can take some time to complete.

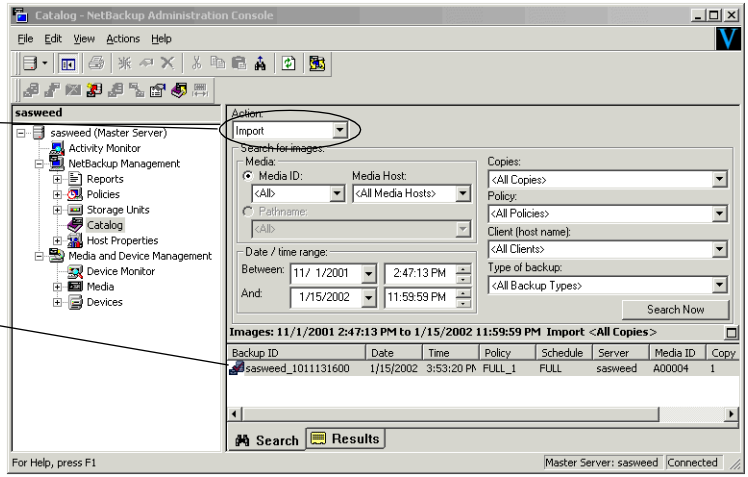
▼ To import backup images – Phase II

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

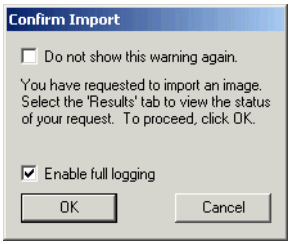
2. Set up the search criteria to find imported images by setting the search action to **Import**.

Select **Import** to search for imported images

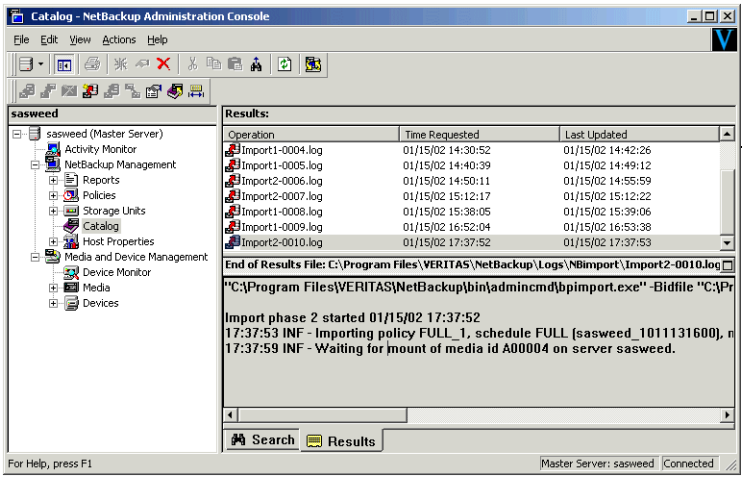
Images eligible for importing appear as a result



3. Select the image(s) you wish to import and Select **Actions** > **Import**. The Confirm Import dialog appears.



4. To view the log, click the **Results** tab, then select the import job log just created.



Note When importing backups that have fragments on more than one tape, do not start the import until you have read the catalog for all the tapes containing fragments. Otherwise, the import will fail with a message similar to: `Import of backupid failed, fragments are not consecutive`.

Viewing Job Results

The results of verify, duplicate, or import jobs appear in the **Results** tab. The top portion of the dialog displays all existing log files.

To view a log file, select the name of the log from the list. The log file currently displayed appears in the bottom portion of the **Results** dialog. If an operation is in progress, the log file display is refreshed as the operation proceeds.

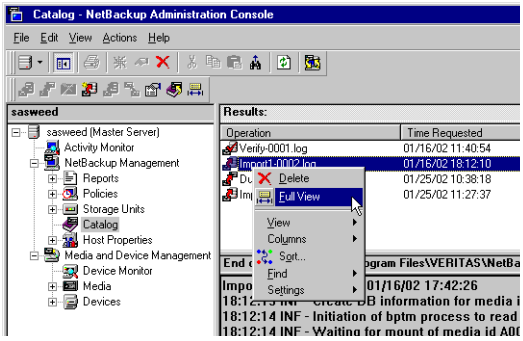
▼ To view or delete a log file

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Catalog**.

2. Click the **Results** tab.

3. Select a log file.

4. Select **Edit** > **Full View** or **Edit** > **Delete**. You can also right-click the log file and select an action from the scroll-down menu.



Viewing NetBackup Reports 5

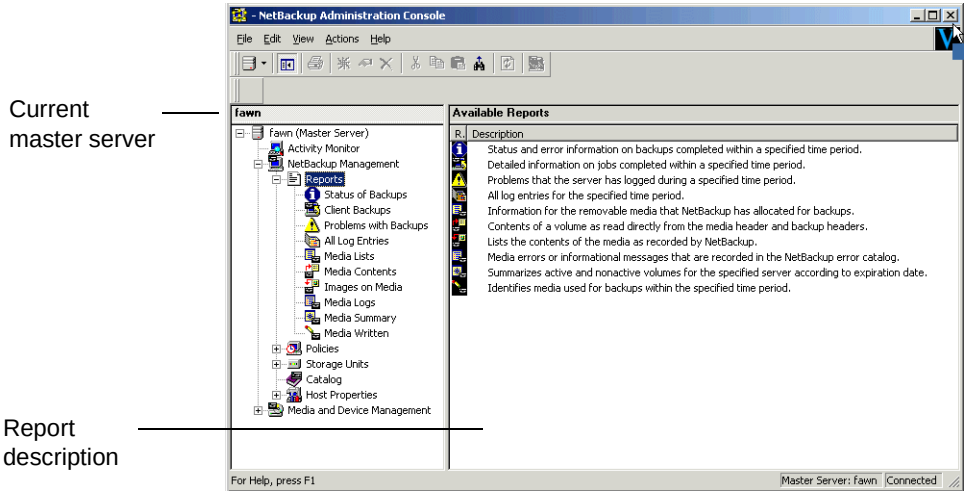
NetBackup provides reports for verifying, managing, and troubleshooting NetBackup operations. NetBackup reports show status or problem information for NetBackup servers or clients. A Troubleshooting Wizard is available to help analyze the cause of errors that can appear in a NetBackup report.

The following topics are discussed in this chapter:

- NetBackup Management Reports Application
- Reports Window
- Report Descriptions
- Using the Troubleshooting Wizard With Reports

NetBackup Management Reports Application

Once **Reports** is expanded in the NetBackup Administration Console, the right pane displays a description of all possible reports. Each report type is discussed in “Report Descriptions” on page 197.



▼ To run a report

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Reports**. A list of possible reports appears.

   The report information is for the master server that is currently selected. To run a report on a different master server, click **File** > **Change Server**. (See “ Administering a Remote Master Server” on page 320.)

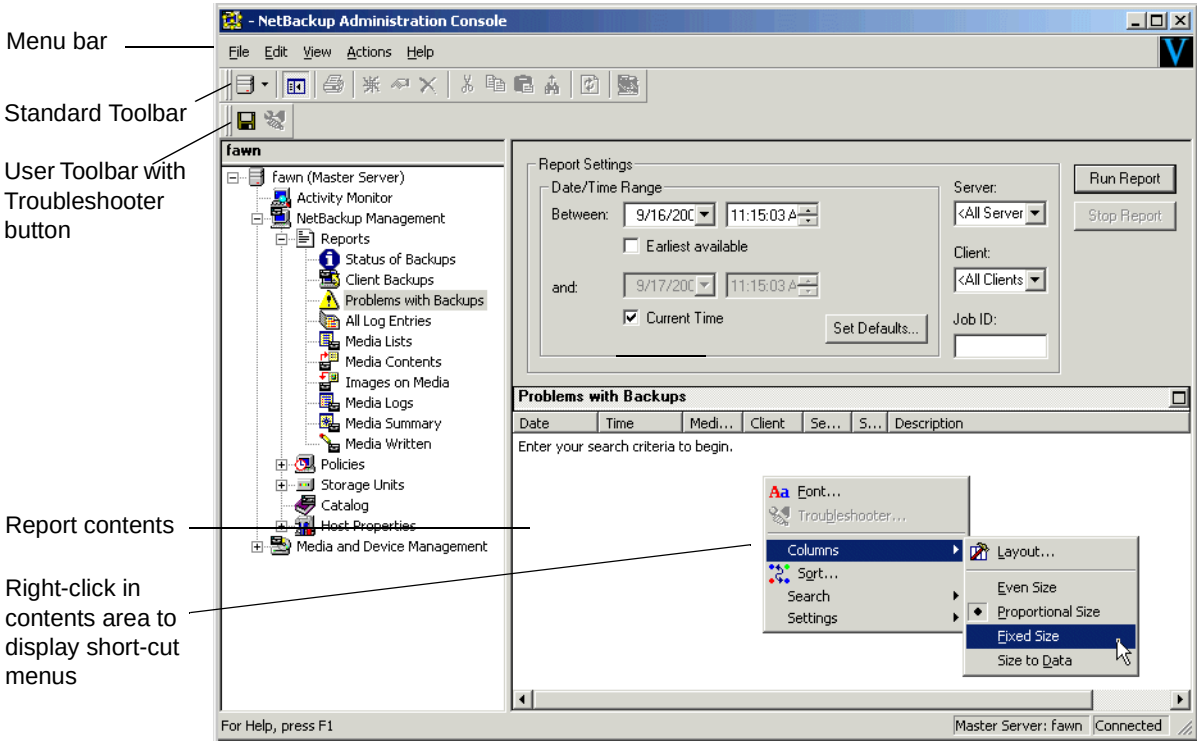
2. Double-click the name of the report you would like to run.

3. Select the media server(s) and / or clients on which to run the report and / or select the time period for which the report will run.

4. Click **Run Report**. For a description of the report fields, see “Report Descriptions” on page 197.

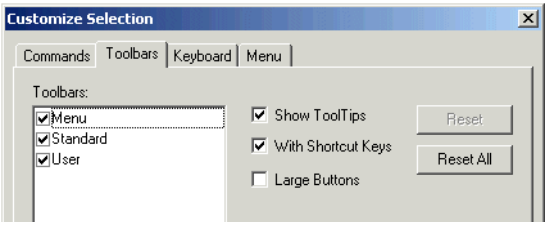
Reports Window

The Reports window contains a number of methods to make it easier for you to view report listings and manage report data.



Customizing the Window

Many of the items you see in the Toolbar window can be customized using the selections on the **View** menu, or by changing the tab selections on **View** > **Customize**.



Standard and User Toolbars

The buttons on the toolbars provide shortcuts for menu commands. To display or hide the standard NetBackup toolbar, click **View** > **Toolbar**.

Select **View** > **Customize** > **Toolbars** > **User** to display or hide the user toolbar.

For information on the standard toolbar buttons, see "Using the NetBackup Administration Console" on page 3.

The Reports user toolbar contains shortcuts for the following actions:

- Save
- Troubleshooter

Report Contents Pane

The right pane in the Reports window displays the contents of the report that you've run or that you will run.

Status Bar

The status bar appears at the bottom of the window and displays various report settings when a report is running. To display or hide the status bar by click **View** > **Status Bar**.

Shortcut Menus

To display a list of commands that apply to a list, right-click on a report. Depending on which report you're viewing, the shortcut list may include:

- **Font:** Use to change the typeface and point size of the display text in the report pane.
- **Troubleshooter Wizard:** Launches the Troubleshooter Wizard. The wizard is available only when a line in a report is selected that shows a NetBackup status code. (See "Using the Troubleshooting Wizard With Reports" on page 209.)
- **Columns:** Opens a submenu that contains commands for changing the order and size of columns. Includes: **Layout** options, **Even Size**, **Proportional Size**, **Fixed Size**, and **Size to Data**.
- **Sort:** Use to specify sort criteria for the columns.
- **Search:** Use to find text within the report.

- **Settings:** Options to reload settings from default, save the current settings as the default settings, or save settings on exit.

Reports Settings

You can specify the following criteria for building your report. Not all of these settings are available for every report type.

Date/Time

Specify the time period that you want the report to cover.

- Default start time is one day before the report was run.
- Default end time is the time the report is run.

The main factor that determines the time period for which information is available is the **Duration to Retain Logs** setting on the Global host properties.

Client

Click the **Client** box and select **All** or the client to which the report will apply.

Media Server

Click the **Media Server** box and select **All** or the name of the media server to which the report will apply.

Job ID

Specifies the Job ID for which you want the report.

Media ID

For media types of reports, specify the media ID or **All**. The Media Contents report requires a specific ID.

Volume Pool

For a media summary report, specify the volume pool name or **All**.

Verbose Listing

For the media summary report, select **Verbose Listing** to have NetBackup provide more details.

▼ To print a report

1. After running a report, click **File** > **Print**. The Print dialog appears.
2. In the Print dialog, specify the settings.

   You can also specify font and column settings for the report.
3. Click **OK**.

▼ To save a report

1. After running a report, click **File** > **Save**. The Save dialog appears.
2. In the **Save In** box, select the drive and directory where you want to save the report.
3. Specify the file name and file type.
4. Click **OK**.

▼ To copy report text to another document

1. Select the report text that you want to copy.
2. Click **Edit** > **Copy** or press Ctrl-c.
3. Paste the selected text into a document (for example, an Excel document).

Report Descriptions

The following topics describe the contents of each NetBackup report.

Status of Backups Report

The Status of Backups report shows status and error information on jobs completed within the specified time period. If an error has occurred, a short explanation of the error is included. The following table explains the columns in the Status of Backups report:

Status of Backups Report

Column	Meaning
Date	Date that the backup occurred.
Time	Time of day that the backup occurred.
Policy	Name of the policy that was used to back up the client.
Schedule	Name of the schedule that was used to back up the client.
Server	NetBackup server that is controlling the media used for the backup.
Severity	Severity level of the status. info: informational only. error: an error occurred.
Type	Type of status.
Client	Name of the client that was backed up.
Status	Completion status code. If the status code is 0, the operation succeeded. If status is not 0, the backup was not entirely successful. Use the Troubleshooting Wizard to find an explanation of specific status codes.
Process	Process that returned the status.
Description	Message describing the status.

Client Backups Report

The Client Backups report shows detailed information on backups completed within the specified time period. The following table explains each field in the Client Backups report.

Client Backups Report

Field	Meaning
Master Server	Master server that controlled the backup.
Client	Name of the client that was backed up.
Policy	Name of the policy that was used to back up the client.
Schedule Type	Type of schedule used for the backup: - Full - Incr (differential incremental) - Cinc (cumulative incremental) - UBackup (user backup) - UArchive (user archive)
Backup Date	Date that the backup began.
Backup Time	Time of day that the backup began.
Backup ID	Identifier that NetBackup assigns when it performs the backup.
Compressed	*Yes* indicates that the backup was compressed.
Policy Type	Type of policy (for example, Standard, MS-Windows-NT, and so on).
Schedule	Name of the schedule that was used for the backup.
Retention Level	Retention level indicates how long NetBackup will keep a record of this backup. (See “Retention” on page 115.)
Elapsed Time	How much time the backup required to complete.
Expiration Date	Date when NetBackup will expire the record of this backup.
Expiration Time	Time when NetBackup will expire the record of this backup.
Encrypted	*Yes*, if the backup is encrypted. Encryption and decryption is possible only with the NetBackup Encryption option.

Client Backups Report (continued)

Field	Meaning
Kilobytes	Number of kilobytes in the backup.
Number of Files	Number of files in the backup.
Primary Copy	Primary copy shows which copy (1 or 2) NetBackup uses to satisfy restore requests.
Image Type	Regular: Image from a scheduled or user-directed backup. Pre-imported: Image for which phase 1 of the import process has been completed. Imported: Image that has been imported into the NetBackup database on this server.
Keyword	Keyword that the user associates with this image at the time of the backup.
Extended Security Info	This field is reserved for future use and always displays *No*.
File Restore Raw	Individual file restore from raw. This is set by the corresponding policy attribute, if it applies.
Image Dump Level	Applies to NDMP backups. *0* indicates a full backup and greater than 0 indicates an incremental backup.
File System Only	This field is reserved for future use and always displays *No*.
Object Descriptor	This field is reserved for future use and is always empty.
Multiplexed	*Yes* indicates that the backup was multiplexed.
TIR Available	*Yes* indicates that NetBackup is collecting true image restore information for this policy and it is possible to perform a true image restore of the directories in the backup.

Problems Report

The Problems report lists the problems that the server has logged during the specified time period. The information in this report is a subset of the information obtained from the All Log Entries report. (See “All Log Entries Report” on page 200.)

All Log Entries Report

The All Log Entries report lists all log entries for the specified time period. This report includes the information from the Problems report and Media Log Entries report. This report also shows the transfer rate, which is useful in determining and predicting rates and backup times for future backups (the transfer rate does not appear for multiplexed backups). The following table explains the columns in the All Log Entries report:

All Log Entries Report

Column	Meaning
Master Server	Master server that controlled the backup.
Date	Date that the backup occurred.
Time	Time of day that the backup occurred.
Policy	Name of the policy that was used to back up the client.
Schedule	Name of the schedule that was used to back up the client.
Server	NetBackup server that is controlling the media used for the backup.
Severity	Severity level of the status: info = informational only. error = an error occurred.
Type	Type of status.
Client	Name of the client that was backed up.
Status	Completion status code. If the status code is 0, the operation succeeded. If status is not 0, the backup was not entirely successful. Use the Troubleshooting Wizard to find an explanation of specific status codes.
Process	Process that returned the status.
Description	Message describing the status.

Media Lists Report

The Media Lists report shows information for volumes that have been allocated for backups. This report does not show media for disk type storage units or for backups of the NetBackup catalogs.

- For information about backups saved to disk storage units, use the Images on Media report.
- To track media used for catalog backups, keep a hard copy record or configure the E-mail global attribute. The E-mail global attribute causes NetBackup to send an E-mail that indicates the status of each catalog backup and the media ID that was used. You can then print the E-mail or save it on a disk other than the one that has the catalogs.

The following table explains the columns in the Media Lists report:

Media Lists Report

Column	Meaning
Master Server	Master server that controlled the backup.
Media ID	Media ID that is assigned when the volume is added to Media Manager.
Retention Level	Retention level for the backups on this volume. An asterisk after the retention level number means that the volume can have multiple retention levels. When there are multiple retention levels, the number shown was the first level assigned.
# of Images	Total number of backups on the volume.
Valid images	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.
Allocated Date	Date that Media Manager allocated the volume.
Allocated Time	Time that Media Manager allocated the volume.
Expiration Date	Date when the backups on the volume expire.
Expiration Time	Time when the backups on the volume expire.
Last Written Date	Date when the volume was last used for backups.
Last Written Time	Time when the volume was last used for backups.

Media Lists Report (continued)

Column	Meaning
Last Restore Date	Date when the last restore was done from this volume.
Last Restore Time	Time of day when the last restore was done from this volume.
Density	Density of the device that produced the backups on this volume.
KBytes	Total number of kilobytes on this volume.
Number of Restores	Number of times this volume has been used for restores.
Status	The messages that commonly appear here are: Suspended: The volume will not be used for further backups until retention periods for all backups on it have expired. You can still restore from the media. **Frozen**: The volume is no longer used for backups. However, the information about it is frozen permanently and you can still restore from the volume (expired backups must be imported first). **Full**: The volume is full and no more backups are written to it. **Imported**: The backup was imported. **MultiRetlev**: The volume contains backups of more than one retention level. **MPX**: The volume allows multiplexed backups.
Partner ID	For an optical disk, this is the media ID of the volume on the other side of the platter (BusinesServer does not support optical disks).
VM Pool	A number that corresponds to the volume pool for the media. 0 = None 1 = NetBackup For other numbers, find the media ID in the volume list on the volume database host for the media ID. This list shows the volume pool for each volume.
Header Size	Optical header size in bytes. (BusinesServer does not support optical disk.)
Sector Size	Optical sector size in bytes. (BusinesServer does not support optical disk.)
Last Offset	Optical offset of the last header. (BusinesServer does not support optical disk.)
Media Server	Server where the volumes reside.

Media Contents Report

The Media Contents report shows the contents of a volume as read directly from the media header and backup headers. This report lists the backup IDs (not each individual file) that are on a single volume. If a tape has to mounted, there will be a longer delay before the report appears.

Note The Media Contents report does not apply to disk type storage units or NetBackup catalog backups.

The following table explains the columns in the report.

Media Contents Report

Column	Meaning
Master Server	Master server that controlled the backup.
Media ID	Media ID that contains this backup. The media ID is the same for all backups since the Media Contents can be run on only a single Media ID.
File Number	Position of the file, where file 1 is the first. If the volume contains multiplexed backups, it can have multiple files with the same number.
Backup ID	Identifier that NetBackup assigns when it performs the backup.
Creation Date	Date when NetBackup created the backup.
Creation Time	Time of day when NetBackup created the backup.
Expiration Date	Date when the backup expires.
Expiration Time	Time of day when the backup expires.
Retention level	Period of time that NetBackup retains the backup. An asterisk after the retention level number means that the volume can have backups with different retention levels and that the number shown was the first level assigned.
Copy Number	Shows the copy number (1 or 2).
Fragment	Greater than 1 only if the backup is split across multiple volumes or if the storage unit maximum fragment size is exceeded.
Size	Shows the number of bytes in the fragment and applies only to optical disk (BusinesServer does not support optical disk).

Media Contents Report (continued)

Column	Meaning
Media's Media ID	Media ID as recorded for the entire volume (matches Media ID above).
Media Partner ID	For an optical disk, this is the media ID of the volume on the other side of the platter (BusinesServer does not support optical disk).
Media Density	Density of the device that produced the backups on this volume.
Media Allocated Date	Date when Media Manager allocated the volume.
Media Allocated Time	Time of day when Media Manager allocated the volume.
Media Last Written Date	Date when the volume was last used for backups.
Media Last Written Time	Time of day when the volume was last used for backups.
Media Expiration Date	Date when the volume expires.
Media Expiration Time	Time of day when the volume expires.
Media Last Restore Date	Date when the last restore was done from this volume.
Media Last Restore Time	Time of day when the last restore was done from this volume.
Media KBytes	Total number of kilobytes on this volume.
Media Images	Number of images on the volume.
Media Valid Images	Number of valid (unexpired) 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.
Media Retention Level	Retention level for the backups on this volume. An asterisk after the retention level number means that the volume can have multiple retention levels. When there are multiple retention levels, the number shown was the first level assigned.

Media Contents Report (continued)

Column	Meaning
Media Volume Pool	A number that corresponds to the volume pool for the media. 0 = None 1 = NetBackup For other numbers, find the media ID in the volume list on the volume database host for the media ID. This list shows the volume pool for each volume.
Media Number of Restores	Number of times this volume has been used for restores.
Media Status	The messages that commonly appear here are: **Suspended**: The volume is not used for further backups until retention periods for all backups on it have expired. You can still restore from the media. **Frozen**: The volume is no longer used for backups. However, the information about it is frozen permanently and you can still restore from the volume (expired backups must be imported first). **Full**: The volume is full and no more backups are written to it. **Imported**: The backup was imported. **MultiRetlev**: The volume contains backups of more than one retention level. **MPX**: The volume allows multiplexed backups.
Media Header Size	Optical header size in bytes. (BusinesServer does not support optical disks.)
Media Sector Size	Optical sector size in bytes. (BusinesServer does not support optical disks.)
Media Last Offset	Optical offset of the last header. (BusinesServer does not support optical disks.)
Block size	Size of the data blocks used to write the backup. When multiplexing is used, the block size can vary between backups on the same volume.
Header Type	A bit field as follows: Empty header Last header HP800 WORM special TIR header BMAP header

Media Contents Report (continued)

Column	Meaning
Policy Type	Type of client that was backed up.
Sched Type	Type of schedule that produced the backup: full, differential incremental, cumulative incremental, or user-directed.
Flags	This column can contain one or more of the following: Compression Encryption TIR (true-image recovery) IFR (individual file restore from raw). (Not supported on BusinesServer.)
Mpx Headers	Reserved
Policy	Policy for this backup.
Sched	Schedule for this backup.

Images on Media Report

The Images on Media report lists the contents of the media as recorded in the NetBackup image catalog. You can generate this report for any type of media (including disk) and filter it according to client, media ID, or path.

Note The Images on Media report does not show information for media used for NetBackup catalog backups.

The following table explains the columns in the Images on Media report:

Images on Media Report

Column	Meaning
Master Server	Name of the master server that controlled the backup.
Backup ID	Identifier that NetBackup assigns when it performs the backup.
Policy	NetBackup policy for which the backup was created.

Images on Media Report (continued)

Column	Meaning
Schedule Type	Type of schedule that produced the backup: Full (full backup) Incr (differential incremental) Cinc (cumulative incremental) Ubackup (user backup) Uarchive (user archive)
Retention Level	Retention level for the schedule.
Number of Files	Number of files in the backup.
Compressed	*Yes* if the backup is compressed.
Encrypted	*Yes* if the backup is encrypted. Encryption and decryption is possible only with the NetBackup Encryption option.
Expiration Date	Date that the retention period for the backup ends.
Expiration Time	Time that the retention period for the backup ends.
Fragment Number	Number of the fragment. TIR if the fragment is part of a true-image backup.
Client Type	A number that corresponds to the type of client that was backed up. (See the `bpbackup` command description for a list of the numbers for each client type.)
Client	Name of the client that was backed up.
Schedule	Name of the schedule that produced the backup.
Copy Number	Greater than 1 only if there are multiple copies.
KBytes	Size of the fragment in kilobytes. This value does not include the space for tape headers between backups. A fragment size of 0 is possible in a multiplexed backup.
Remainder	Bytes written beyond kilobytes filed. Size of fragment is exactly: Kilobytes*1024 + Remainder.
Media Type	Type of media and can be removable (Rmed) or disk (Disk).
Density	Density of the device that produced the backup.

Images on Media Report (continued)

Column	Meaning
File Number	File number on the media.
ID	Media ID of the volume that has the backup image. For disk, it is a pathname.
Host	Server with the catalog that has this information.
Block Size	Size of the data blocks used to write the backup. When multiplexing is used, the block size can vary between backups on the same volume.
Offset	Applies only to optical disk (not supported on BusinesServer) and is the byte offset on the media where the backup image begins. Ignore this value for tapes and magnetic disk.
Media Date	Date that the media was allocated for use by NetBackup.
Media Time	Time that the media was allocated for use by NetBackup.
Device Written On	Device where the backup was written. This is the drive index configured in Media Manager.
Blockmap	Indicates whether this fragment is a blockmap (Yes or No).
Multiplexed	Indicates whether this image is multiplexed (Yes or No)

Media Logs Report

The Media Logs report shows media errors or informational messages that are recorded in the NetBackup error catalog. This information also appears in the All Log Entries report. (See “All Log Entries Report” on page 200.)

Media Summary Report

The Media Summary report summarizes active and nonactive volumes for the specified server according to expiration date. It also shows how many volumes are at each retention level. In verbose mode, the report shows each media ID and its expiration date.

Nonactive media are those with a status of FULL, FROZEN, SUSPENDED, or IMPORTED. Other volumes are considered active. (See “Media Lists Report” on page 201.)

The only expired volumes that appear in this report are those that are FROZEN. NetBackup deletes other expired volumes from its media catalog when it runs backups. An expired volume with other status can show up only if you run the report between the time the volume expires and the next backup is done.

Media Written Report

The Media Written report identifies volumes that were used for backups within the specified time period. This report does not display volumes used for NetBackup catalog backups or volumes used for duplication if the original was created prior to the specified time period.

The following table explains the columns in the Media Written report:

Media Written Report

Column	Meaning
Master Server	Master server that controlled the backup.
Media ID	Media ID that is assigned when the volume is added to Media Manager.
Last Written Date	Date when the media was last written.
Last Written Time	Time when the media was last written.
Host	NetBackup server that has the volume database with the records for this volume.
Times Written	Number of times this media was written.
KBytes	Total number of kilobytes on this volume.
Retention Level	Retention level for the backups on this volume.

Using the Troubleshooting Wizard With Reports

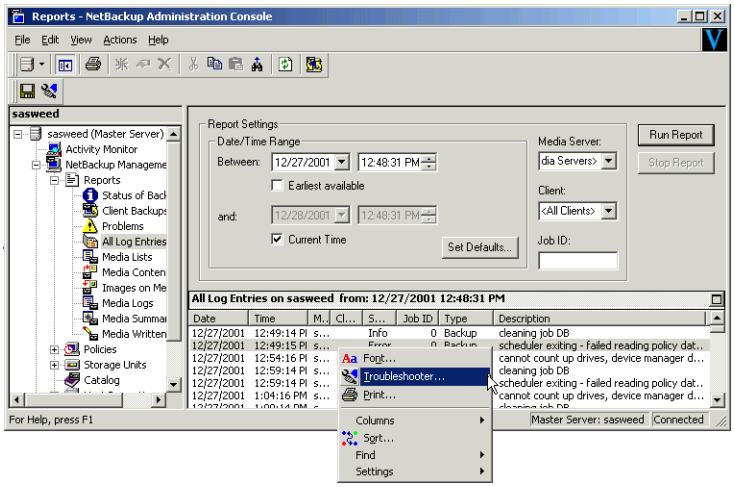
You can use the Reports Troubleshooting Wizard to find explanations and corrective actions when a job returns a NetBackup status code.

▼ To run the Reports Troubleshooting Wizard

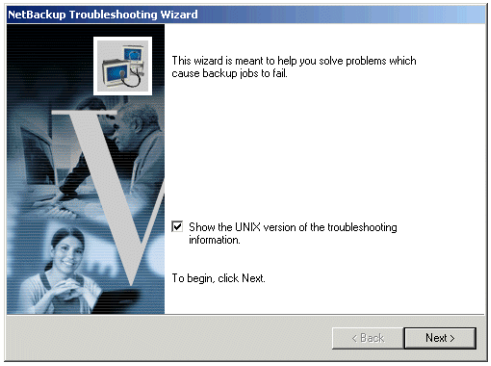
1. Run a report.

2. Right-click the line in the report containing the error status code.

3. Select **Troubleshooter** on the shortcut menu. (Or select the line and click **Actions** > **Troubleshooter**.)



The Troubleshooting wizard appears.



4. Click **Next** to see an explanation of the error code. If you'd like to see the description in UNIX terms, click the checkbox on the first wizard screen.

5. Click **Next** again to see a list of corrective actions.

Monitoring NetBackup Activity 6

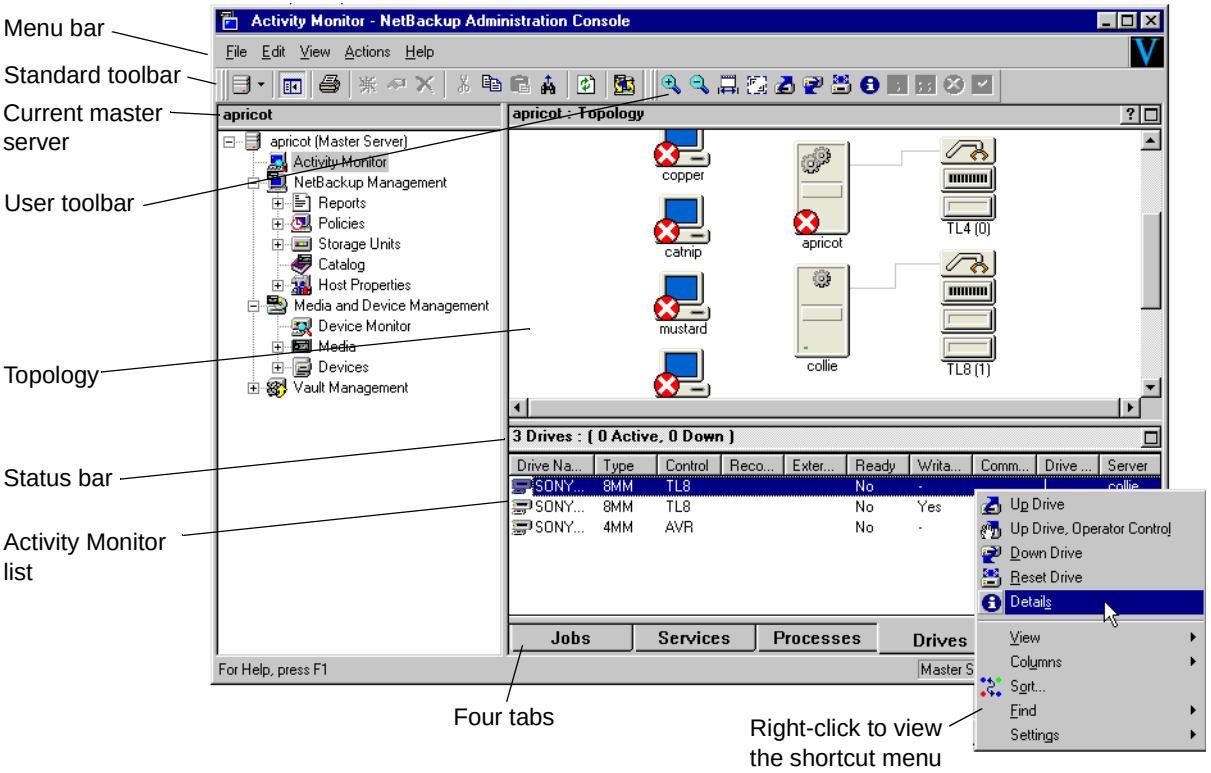
This chapter explains how to use the NetBackup Activity Monitor to perform the following functions:

- Monitor the progress of NetBackup jobs.
- Delete completed (Done) jobs and cancel uncompleted jobs.
- Save job information.
- Start and stop NetBackup services.
- Monitor NetBackup processes.
- Use the troubleshooting wizard to troubleshoot failed jobs.

Introduction to the Activity Monitor

Use the Activity Monitor in the NetBackup Administration Console to monitor and control NetBackup jobs, services, processes, and drives.

The Activity Monitor contains the following information:



Menu Bar

The Menu bar consists of File, Edit, View, Actions, and Help. See Chapter 1 for a description of the items found on File, Edit, View, and Help.

In the Activity Monitor, the **Find** options on the **Edit** menu are especially useful when managing many hosts and storage units. Use the **View** menu for sorting the jobs and changing the layout and appearance of the lists.

Shortcut Menus

Right-clicking in the Activity Monitor list area produces different shortcut menus depending on which tab is displayed. The following table is a list of possible menu items:

Shortcut Menu Items

Menu Item	Description
Delete	Deletes completed (Done) jobs that you have selected in the Jobs tab. If you have selected only uncompleted jobs (Queued, Re-Queued, or Active), the Delete command is not available. If both completed and uncompleted jobs are selected, the uncompleted jobs will be ignored.
Cancel Job	Cancels uncompleted jobs that you have selected in the Jobs list.
Details	Displays detailed information about the job, service, process or drive you select in the list.
Troubleshooter	Starts the Troubleshooting Wizard for a job.
Stop Service	Stops services that you have selected in the Services list.
Start Service	Starts services that you have selected in the Services list.
Up Drive	Sets the drive to up in automatic volume recognition (AVR) mode. This is the normal and default mode for drives. In AVR mode, a robot automatically retrieves, mounts, unmounts, and stores volumes. Manual intervention is necessary only when a request causes an error.
Up Drive, Operator Control	Sets the drive to up in operator control mode (OPR). This mode is normally used only for security reasons.
Down Drive	Sets the selected 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.
Reset Drive	Resets the specified drive, terminating the drive assignment and taking control away from the assigned user.

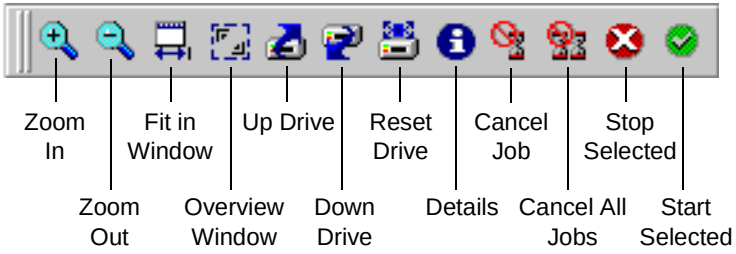
Standard and User Toolbars

The buttons on the toolbars provide shortcuts for menu commands. To display or hide the standard NetBackup toolbar, click **View** > **Toolbar**.

Select **View** > **Customize** > **Toolbars** > **User** to display or hide the user toolbar.

For information on the standard toolbar, see “Using the NetBackup Administration Console” on page 3.

The Activity Monitor user toolbar contains shortcuts for the following actions:



Status Bar

The status bar appears at the top of the Activity Monitor list and displays the following information, depending on which tab is currently selected:

- The master server on which the jobs reside.
- The number of jobs in each of the job states: Queued, Active, Requeued, Done.
- Number of services running.
- Number of drives and the state of each (Active, Down).

Activity Monitor Topology

The Activity Monitor topology view displays the state and configuration of the entire NetBackup system being administered.

The topology view shows master servers, media servers, clients, and NetBackup storage unit devices. The view displays backup and restore activity, job failures, services that are down, and drive state status.

Master server

Media server

The following figures represent some of the icons you may see in the Activity Monitor. Others are possible.

Client being backed up

Client running a NetBackup restore

Client with a failed job

Client backup and restore failure

Master server backup

Host backup and restore

Media server with services down

Master server backup and restore failure with services down

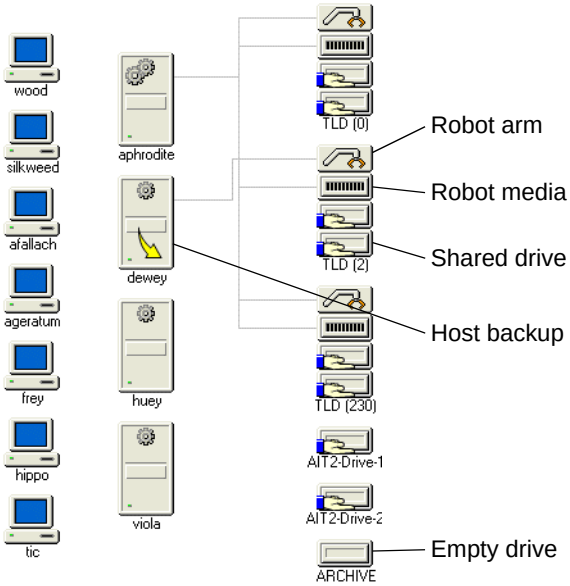
Topology Connections

The topology view also displays the physical and logical connections between devices.

Connecting lines appear between a drive in use and the server using it. For example, connecting lines appear between a media server and a device running a job.

Robots and drives are represented as connected to a media server. Drives that are physically located in a robot are shown directly below the robot. Standalone drives are represented as individual drive objects.

The *NetBackup Media Management System Administrator's Guide* contains additional information on media devices.



Selecting an Activity Monitor tab allows you to select different views of your configuration.

Selecting Topology Objects

Selecting objects in the topology pane is one method to filter the contents of the Activity Monitor list. Multiple objects of the same type can be selected by pressing the Ctrl key and selecting another object.

Multiple objects of the same type can be selected by pressing the Ctrl key and selecting another object. Selection of unlike objects is not allowed.

Selecting an object highlights the connecting lines from the object to all other objects to which it is connected.

Click a server to highlight all attached robots, media, and drives configured to the server.

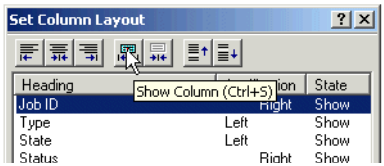
Jobs Tab

The **Jobs** tab displays all jobs that are in process or have been completed for the master server currently selected. The Activity Monitor contains detailed information for the following types of jobs:

- Backup
- Archive
- DB Backup (backup of the catalog database)
- Duplicate
- Import
- Restore
- Verify
- Vault

Using Filters to Customize the Jobs List Output

▼ To set job detail selections



1. Open the Activity Monitor.
2. Click **View** > **Columns** > **Layout**. The **Set Column Layout** dialog appears, showing the current settings.
3. Select the heading you wish to display or hide.
4. Select the **Show Column** button to display the heading.
5. Select the **Hide Column** button if you do not want to see the column heading.
6. Click **OK** to apply the changes.

To determine what each heading indicates, see the following table:

Job List

Column	Description
Job ID	Identifier that NetBackup assigns to each job. The identifier is unique on the server where the job was run.

Job List (continued)

Column	Description
Type	Type of job.
State	Queued - Jobs in the NetBackup scheduler queue. A queued restore job is one for which NetBackup is still determining which files are needed. Active - Currently active jobs. Re-Queued - Jobs that are placed back in the scheduler queue as retries because the previous attempt was unsuccessful. Done - Completed jobs.
Status	NetBackup status code that indicates the completion status. There is no value until the job is done. A status of zero (0) means that the job completed successfully. Any other completion value for status indicates a problem.
Policy	Name of the policy that NetBackup is using to back up the client.
Schedule	Name of the schedule that NetBackup is using to back up the client.
Client	Name of the client associated with the job.
Media Server	NetBackup server controlling the media.
Start Time	Date and time that the first attempt was initially queued.
Elapsed Time	Amount of time that has elapsed since the job was initially queued.
End Time	Date and time that the job completed.
Storage Unit	Name of the storage unit that the job is using.
Attempt	For Active jobs, this indicates the number of the current attempt. For Done jobs it indicates the total number of attempts.
Operation	For Active jobs, this indicates the operation that is currently being performed.
Kilobytes	Number of kilobytes that have been written.
Files	Number of files that have been written.

Job List (continued)

Column	Description
Tapes to Eject	The number of tapes to be ejected for the selected Vault job. *The number may not represent the number of tapes actually ejected.* For example, if the Vault profile was configured for manual eject, the tapes may not have yet been ejected. Or, if something went wrong with the device, fewer tapes may actually have been ejected than the number here indicates.
Master	Master server where the job was run.
Current File	For Active jobs, this is the path of a file that was recently written to the image. If the job is backing up many files, not all of them necessarily appear in this column over the course of the backup.
% Complete (Estimated)	Percentage of the job that is complete. For backups, it is based on the size of the previous backup for the same policy, client, schedule, and retention level. If there is no previous backup that matches this criteria then NetBackup does not provide an estimate. If the current backup is larger, this indication is 100%. For other types of jobs, the estimate is based on other factors.
Job PID	Process ID. If the backup is multiplexed, all jobs associated with the same multiplexed storage unit have the same PID.
Owner	Owner of the job.
KB Per second	Average kilobytes per second over the length of the current attempt.
Active Start	Time when the most recent attempt became active.
Active Elapsed	Time since the most recent attempt became active.
Copy	The copy number when the Inline Tape Copy option is used.
Robot	The name of the robot with which Vault is associated.
Vault	The name of the logical Vault for a robot configured through Vault management.
Profile	The profile defines the processing to be done by a Vault job. Multiple profiles can be configured for the Vault.
Session ID	The session ID, a unique numeric value, for a Vault session. Session ID assignment starts at 1 the first time a Vault session is run after Vault has been installed. The value increments by one every time a new Vault session runs. If a Vault job is restarted, the restarted session uses the session ID of the original job.

Job List (continued)

Column	Description
Parent Job ID	When Vault is used, each child job refers to the parent job by this number. The Parent Job ID for a parent job is 0.

▼ To monitor the detailed status of selected jobs

1. Open the Activity Monitor. The Activity Monitor opens to the **Jobs** tab.
2. Select the **Jobs** tab.
3. Select the job(s) for which you want to view details.
4. Select **Actions > Details**. A Jobs Details dialog appears for each job you selected.

▼ To delete completed jobs

1. Select the job(s) you want to delete in the Jobs list.
2. Select **Actions > Delete**. All jobs you selected will be deleted.

▼ To cancel uncompleted jobs

1. Select the uncompleted jobs you want to cancel. An uncompleted job is one that is in the Queued, Re-Queued, or Active state.
2. Select **Actions > Cancel Job**. All jobs you selected will be cancelled.

   To cancel all uncompleted jobs in the jobs list, click **Actions** > **Cancel All Jobs**.

▼ To print job detail information from a list of jobs

1. Select a job to print. Hold down the Control or Shift key to select multiple jobs. If no job is selected, all jobs will be printed.
2. Select **File** > **Print**.

▼ To print job detail information from a single job

1. Double-click on a job to open it.
2. In the **Job Details** dialog, click **Print**, then select a printer and set the printer options.

Job Detail Printout

```
                                                    Job Details:296
                    Job State Done
                    Job type: Backup                                                    Started: 2/13/02 3:47:54 PM
                 Backup type: Scheduled                                                 Elapsed: 00:00:11
                 Policy type: MS-Windows-NT                                               Ended: 2/13/02 3:48:05 PM
                      Client: silk
              Master Server: sasweed
                   Priority: 0
                      Owner: root
                      Group:
                  Retention: 3 weeks
                Compression: No
                                                    Attempt 1
                     Job PID: 4260                                                      Started: 2/13/02 3:47:56 PM
   Current kilobytes written: 0                                                         Elapsed: 00:00:09
       Current files written: 0                                                           Ended: 2/13/02 3:48:05 PM
                Storage unit: sasweed-4mm-robot-tl4-0
                Media server: sasweed
                      Status: none of the files in the file list exist(71)
File list:

C:\SWAP\ToPrinter
```

▼ To copy Activity Monitor text to another document

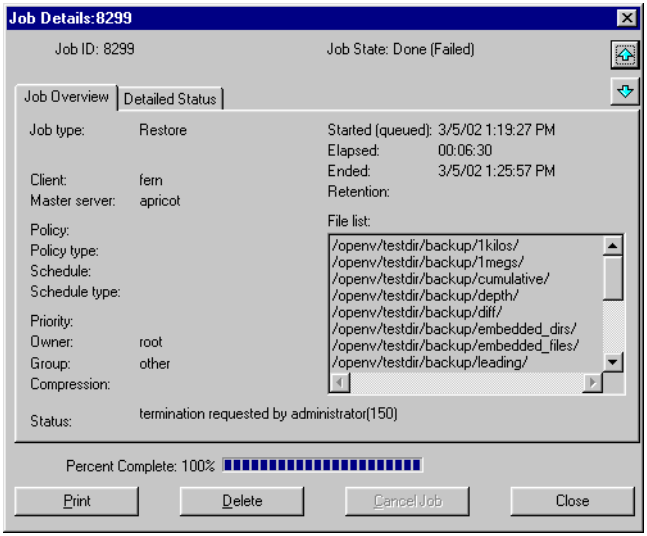
1. Select a job.
2. Select **Edit** > **Copy**.
3. Paste the selected text into the file (for example, an Excel document).

Viewing Job Details

The Job Details dialog contains detailed job information about the selected job.

- The Job ID and state appear at the top of the dialog. When the job is complete, the state changes to *Done*.
- The arrows allow you to show details for either the next or previous job in the job list (based on the order in which the list is sorted).
- **Percent Complete** at the bottom of the dialog shows how much of a running job is completed and the time remaining to completion.
- The **Overview** tab provides general information about the entire job. (See “Job Details: Overview Tab” on page 222.)

- The **Detailed Status** tab provides specific information about job attempts. (See “Job Details: Detailed Status Tab” on page 224.

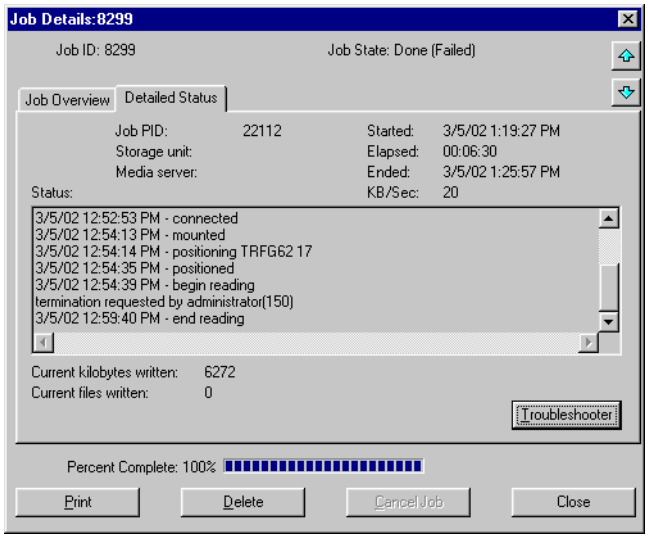


Job Details: Overview Tab

Field	Meaning
Job Type	Type of job.
Backup type	Scheduled, user-directed, immediate (manual backup), or archive.
Client	Name of the client associated with the job.
Master server	Master server on which the job is run.
Policy	Name of the policy that NetBackup is using to back up the client.
Policy type	Type of policy to which the client belongs. For example, MS-Windows-NT or Standard.
Schedule	Name of the schedule that NetBackup is using to back up the client.
Schedule type	Type of schedule controlling the backup. For example, Full or Cumulative-Incremental.
Priority	Priority for the policy as specified by the priority policy attribute.

Job Details: Overview Tab (continued)

Field	Meaning
Owner	Owner of the job.
Group	Group to which the job owner belongs.
Compression	Yes if NetBackup is using software compression. Otherwise, No.
Status	Status code and text describing the completion status of each job attempt.
Started	Date and time that the first attempt was initially queued.
Elapsed	Amount of time that has elapsed since the job was initially queued.
Ended	Date and time that the operation was completed.
Retention	Retention level assigned to the backup. This is specified on the schedule.
Device	The name of the robot with which the Vault is associated. (Appears for Vault jobs only.)
Vault	The name of the logical Vault for a robot configured through the Vault Management node. (Appears for Vault jobs only.)
Profile	Name of the profile that defines the processing to be done by a Vault job. Multiple profiles can be configured for the Vault.
File List	List of files that are being backed up for the policy.



Job Details: Detailed Status Tab

Field	Meaning
State	Queued: Jobs in the NetBackup scheduler queue. A queued restore job is one for which NetBackup is still determining which files are needed. Active: Currently active jobs. Re-Queued: Jobs that are back in the scheduler queue as retries because the previous attempt was unsuccessful. Done: Completed jobs.
Job PID	Process ID. If the backup is multiplexed, all jobs associated with the same multiplexed storage unit have the same PID.
Storage unit	Name of the storage unit that NetBackup is using.
Media Server	NetBackup server controlling the media.
Started	Time when this attempt began.
Elapsed	Elapsed time for this attempt.
Ended	Time when this attempt ended.
KB/sec	Data transfer rate in kilobytes per second.

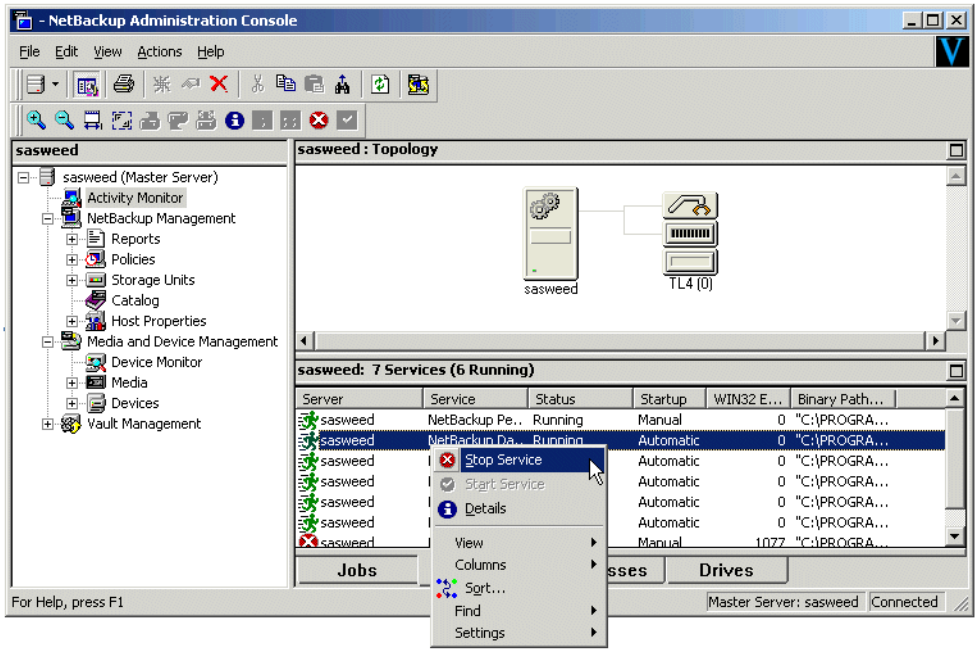
Job Details: Detailed Status Tab (continued)

Field	Meaning
Status	Events that have occurred up to this point. For example, this box contains entries for when the client connects to the server and when the server begins writing data. When the job is complete, the last line shows the completion status.
Current kilobytes written	Number of kilobytes that have been written to the media up to this time.
Current files written	(Present for active jobs.) Files that have been written to the media up to this time.

Services Tab

The **Services** tab displays the status of NetBackup services on the master server and all media servers used by the master server that you are monitoring.

Note In order to see any services or processes on another machine, the other machine must be running on a Microsoft platform and the user must be authenticated on the Microsoft platform.



▼ To monitor NetBackup services

1. Open the Activity Monitor. The Activity Monitor opens to the **Jobs** tab.
2. Select the **Services** tab.
3. Double-click a service from the service list to view a detailed status.

   A Service Details dialog appears for the service you selected. To view the status of the previous service or the next service, click the up or down arrow.

▼ To start or stop a service

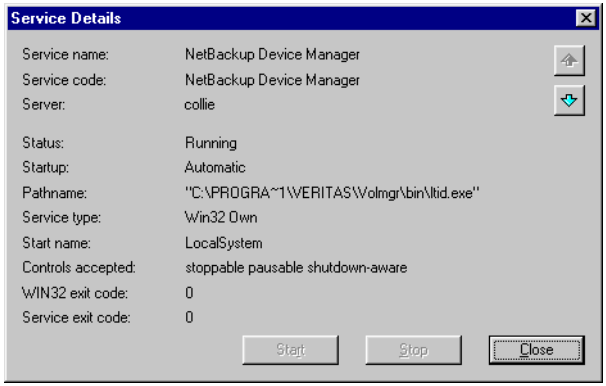
1. Open the Activity Monitor.
2. Select the **Services** tab.

Note Starting or stopping services requires the necessary permissions on the system where the service is running.

3. Select the service(s) you want to start or stop.

4. Select **Actions** > **Stop Selected** or **Actions** > **Start Selected**.

   Or, right-click the service and select **Start Service** or **Stop Service** from the shortcut menu.



Services Details List

Column	Description
Service Code	Short name for the service.
Service	Long name of the service (more descriptive).
Status	Starting, Running, Stopped, Stopping, Paused, Pausing.
Service Type	As defined by Microsoft.
Startup	As defined by Microsoft.
Start Name	As defined by Microsoft.
Binary Pathname	Pathname of the program that performs this service.
Controls Accepted	What this process allows (can it be stopped, started and so on).
Win32 Exit Code	As defined by Microsoft.
Service Specific Exit Code	Exit code as defined by the service.

Processes Tab

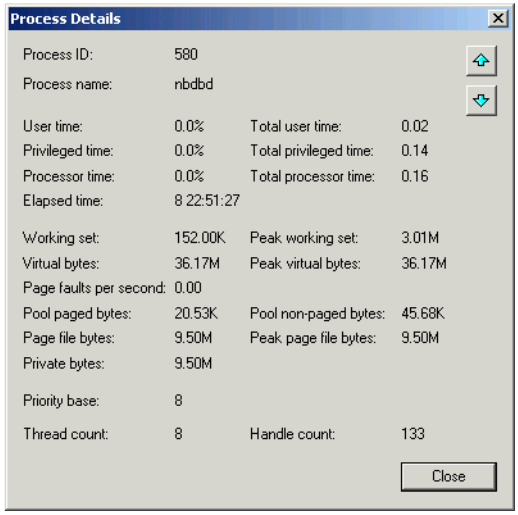
The **Processes** tab displays the NetBackup processes running on the selected master server.

Note In order to see any services or processes on another machine, the other machine must be running on a Microsoft platform and the user must be authenticated on the Microsoft platform.

▼ To monitor NetBackup processes

1. Open the Activity Monitor.
2. Select the **Processes** tab. Double-click a process from the process list to view detailed status.

   For a description of the process details, see “Processes Details List” on page 228.



Processes Details List

Column	Meaning
Process ID	Unique identifier of this process. Process ID numbers are reused, so they only identify a process for the lifetime of that process.
Process Name	Name of the process.

Processes Details List (continued)

Column	Meaning
User Time	Percentage of processor time that this process's threads have spent in user mode.
Total User Time	Amount of processor time (in seconds) that this process has spent in user mode.
Privileged Time	Percent of processor time that this process has spent in privileged mode.
Total Privileged Time	Amount of processor time (in seconds) that this process has spent in privileged mode.
Processor Time	Percentage of processor time (since the last refresh) that all of the threads of this process have used.
Total Processor Time	Amount of process time (in seconds) that this process has spent.
Elapsed Time	Total time (in seconds) since the process was created.
Working Set	Current number of bytes in the set of memory pages used by this process.
Peak Working Set	Maximum number of bytes in the set of memory pages used by this process at any point in time.
Virtual Bytes	Current size in bytes of the virtual address space the process is using.
Peak Virtual Bytes	Maximum number of bytes of virtual address space the process has used at any one time.
Page Faults Per Second	Rate of virtual memory Page Faults by the threads running in this process.
Pool Paged Bytes	Number of bytes in the Paged Pool, a system memory area where space is acquired by operating system components as they accomplish their tasks.
Pool Non-paged Bytes	Number of bytes in the Non-paged Pool, a system memory area where space is acquired by operating system components as they accomplish their tasks.
Page File Bytes	Current number of bytes this process has used in the paging file(s).

Processes Details List (continued)

Column	Meaning
Peak Page File Bytes	Maximum number of bytes that this process has used in the paging file(s).
Private Bytes	Current number of bytes this process has allocated that cannot be shared with other processes.
Priority Base	Current base priority of this process.
Thread Count	Number of threads currently active in this process.
Handle Count	Total number of handles currently open by this process.

▼ To start or stop a process

1. Open the Activity Monitor.
2. Select the **Processes** tab.

Note Starting or stopping processes requires the necessary permissions on the system where the service is running.

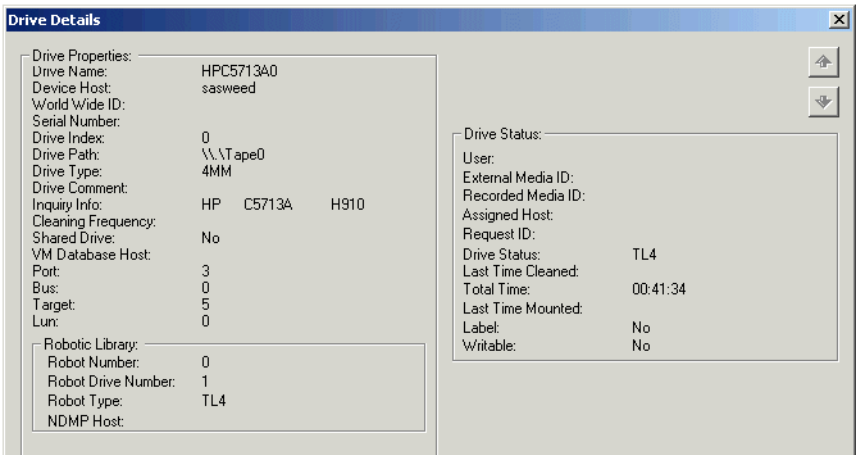
3. Select the process(es).
4. Select **Actions** > **Start Selected** or **Actions** > **Stop Selected**.

   Or, right-click the process and select **Start Selected** or **Stop Selected** from the shortcut menu.

Drives Tab

The **Drives** tab displays the status of NetBackup drives on the master server that you are monitoring.

To view drive details, double-click a drive.



▼ To monitor NetBackup drives

1. Open the Activity Monitor. The Activity Monitor opens to the **Jobs** tab.
2. Select the **Drives** tab. Double-click a drive from the drive list to view a detailed status.
3. A **Drives Details** dialog appears for the process you selected. To view the status of the previous drive or the next drive, click the up or down arrow.

   For a description of the properties, see Chapter 5 of the *Media Manager System Administrator's Guide.*

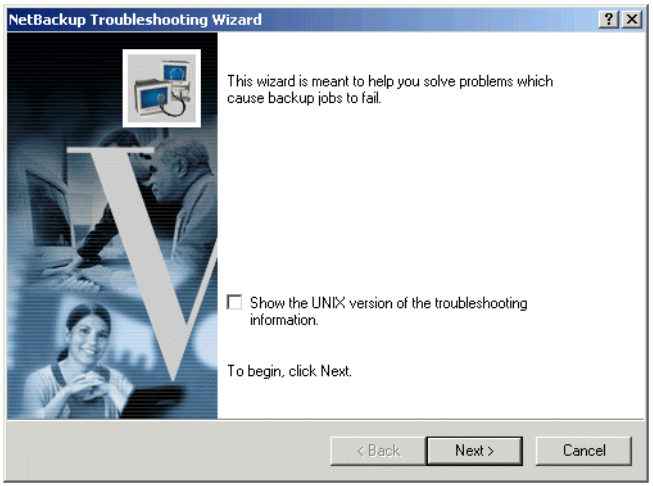
Using the Troubleshooting Wizard

When a job returns a NetBackup status code, use the Troubleshooting Wizard to find out the reason for the failure and what to do to correct the problem.

▼ To use the Troubleshooting Wizard

1. Right-click a failed job in the Activity Monitor Jobs tab.

2. Select **Troubleshooter** from the shortcut menu. The Troubleshooting Wizard appears.



3. The explanation and corrective actions can be different depending on whether the server is UNIX or Windows.

   If the problem involves a UNIX NetBackup server, check **Show the UNIX version of the Troubleshooting Guide** to see UNIX troubleshooting information.

4. Click **Next** to see an explanation, then again to see a list of corrective actions.

Note The wizard is also available from the **Details** tab in the Job Details dialog. If NetBackup attempted the operation more than once, you can troubleshoot a specific attempt by selecting that attempt before clicking the **Troubleshooter** button.

Media Mount Errors

When media is mounted for NetBackup jobs, errors can occur. Depending on the kind of error encountered, a mount request becomes either queued or is cancelled.

Queued Media Mount Errors

When queued, an operator-pending action is created and is displayed in the Device Monitor. This leads to one of the following actions:

- The mount request is suspended until the condition is resolved.
- The request is denied by the operator.
- The media mount timeout is reached.

Cancelled Media Mount Errors

When automatically cancelled, NetBackup tries to select other media to use for backups. (This applies only in the case of backup requests.)

Many conditions lead to the automatic cancelling of the mount request instead of queuing a mount request. This leads to reselection of different media and a stronger likelihood that the backup is not held up.

The following conditions can lead to automatic media reselection:

- When the requested media is in a DOWN drive.
- When the requested media is misplaced.
- When the requested media is write-protected.
- When the requested media is in a drive not accessible to the media server.
- When the requested media is in an offline ACS LSM (Automated Cartridge System Library Storage Module). (ACS robot type only.)
- When the requested media has an unreadable barcode. (ACS robot type only.)
- When the requested media is in an ACS that is not accessible. (ACS robot type only.)
- When the requested media has been otherwise determined to be unmountable.

Managing the Jobs Database

NetBackup uses the *install_path*`\NetBackup\bin\admincmd\bpdbjobs -clean` command to periodically delete done jobs. By default, `bpdbjobs` deletes all done jobs that are more than three days old and retains more recent done jobs until the three-day retention period expires.

If `bprd`, the NetBackup request daemon, is active, `bprd` starts `bpdbjobs` automatically when performing other cleanup tasks. This occurs the first time `bprd` wakes up after midnight. The automatic startups occur regardless of whether you choose to run `bpdbjobs` at other times by using `cron` or alternate methods.

`bpdbjobs` determines how long to retain a job by checking the following locations in the order indicated:

1. The `bp.conf` file for job retention period options.
2. The `BPDBJOBS_OPTIONS` environment variable.
3. `bpdbjobs` command line options.

Jobs Retention Period Options

Use the options listed in the table below in the `bp.conf` file to determine the length of time NetBackup retains jobs.

The options can be entered as upper or lower case in the `bp.conf` file, in the `BPDBJOBS_OPTIONS` environment variable, or as a command line parameter. For example:

```
keep_days 7

KEEP_SUCCESSFUL_HOURS 5
```

Assuming the options in the `bp.conf` file are not overridden by `BPDBJOBS_OPTIONS` or `bpdbjobs` command line options, the Activity Monitor keeps unsuccessful jobs for seven days and successful jobs for five hours.

Jobs Retention Period Options

Option	Description
`keep_days` *days* (see note 1)	Specifies how many days `bpdbjobs` keeps done jobs. Can range from 1 and 30, while values outside this range are ignored. Default: three days.
`keep_hours` *hours* (see note 1)	Specifies how many hours `bpdbjobs` keeps done jobs. Can range from 3 to 720, while values outside this range are ignored. Default: 72 hours.
`keep_successful_days` *days* (see note 2)	Specifies how many days `bpdbjobs` keeps successful done jobs. Can range from 1 to 30 but must be less than `keep_days`. Values outside the range are ignored. Default: three days.
`keep_successful_hours` *hours* (see note 2)	Specifies how many hours `bpdbjobs` keeps successful done jobs. Can range from 3 to 720 but must be less than `keep_hours`. Values outside the range are ignored. Default: 72 hours.

Jobs Retention Period Options (continued)

Option	Description
verbose	Causes bpdbjobs to log additional information in the debug log in the /usr/openv/netbackup/logs/bpdbjobs directory if this directory exists.

Notes:

1. keep_days and keep_hours are mutually exclusive. If both values are specified, bpdbjobs uses only the last one found.
2. keep_successful_days and keep_successful_hours are mutually exclusive. If both values are specified, bpdbjobs uses only the last one found. A successful done job shows a status of 0 in the status column of the Jobs List. The status message reads: *The requested operation was successfully completed*.
3. The retention period values are measured against the time the job ended.

BPDBJOBS_OPTIONS Environment Variable

BPDBJOBS_OPTIONS settings override corresponding options in the bp.conf file. Both can be overridden by bpdbjobs command line options.

BPDBJOBS_OPTIONS offers the same options as described in "Jobs Retention Period Options" on page 234, and provides a convenient way to set the options in a script.

Example Batch File: cleanjobs.bat

```
set BPDBJOBS_OPTIONS= -keep_days 5 -keep_successful_hours 3
C:\VERITAS\NetBackup\bin\admincmd\bpdbjobs -clean %1 %2 %3 %4 %5 %6 %7
```

bpdbjobs Command Line Options

bpdbjobs interacts with the jobs database and is useful as a command line administration tool to delete or move done job files. The command line options are the last location bpdbjobs checks for instructions on retaining jobs, overriding corresponding options in either the bp.conf file or BPDBJOBS_OPTIONS.

See Appendix A in this manual for the bpdbjobs syntax.

The -clean option causes bpdbjobs to delete done jobs older than a specified time period. Done jobs that are not as old as the specified time period are moved to the jobs/done directory.

For example:

```
bpdbjobs -clean -keep_jobs 30
```

bpdbjobs Debug Log

If you need detailed information on `bpdbjobs` activities, enable the `bpdbjobs` debug log by creating the following directory:

install_path`\NetBackup\logs\bpdbjobs`

Note Before using this or other debug logs, read the guidelines in the Debug Logs section of the *NetBackup Troubleshooting Guide for Windows*.

Configuring Host Properties 7

This chapter explains the NetBackup property settings and contains the following topics:

- Viewing Host Properties
- Changing Settings in the Properties Tabs
- Master Server Properties
- Media Server Properties
- Client Properties

Viewing Host Properties

The NetBackup Administration Console displays properties for the Master Server, Media Servers, and Clients under **Host Properties**.

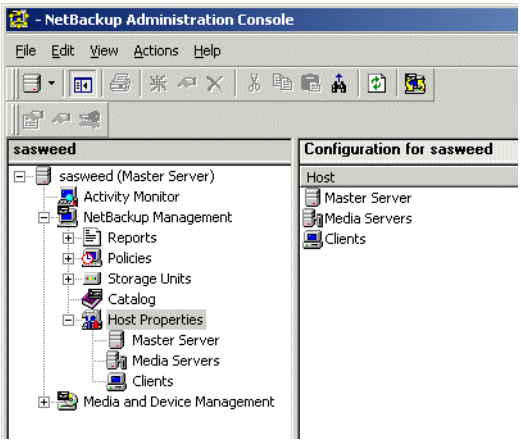
▼ To view master server, media server, or client properties

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Host Properties**.

2. Select **Master Server**, **Media Servers**, or **Clients**.

3. In the right pane, double-click the server or client to view the properties.

   To see the properties of a different master server, click **File** > **Change Server**.



Changing Settings in the Properties Tabs

The NetBackup properties can be changed in order to customize NetBackup to meet specific site preferences and requirements. In most instances, the internal software defaults provide satisfactory results.

Interpreting the Initial Settings

The check boxes are in one of the following states:

- Selected (checked) if the attribute is selected for all selected machines.
- Clear if the property is clear on all selected machines.
- Gray check if the property is set differently on the selected machines.

If the property contains a text field for specifying a value, the text field:

- Contains a value if the property has the same value for all selected machines.
- Clear if the property does not have the same value for all selected machines. When the cursor is moved to such a text field, a small notice appears at the bottom of the dialog noting that the value is different on the selected hosts.

Changing Property Settings

If the property contains a text field for specifying a value:

- To set the property to the same value for all selected clients, select the associated check box and type the value in the field.
- To leave the property unchanged, clear the associated check box. The field changes to gray.

If the property contains only a check box:

- To set the property on all selected machines, select the check box.
- To clear the property on all selected machines, clear the check box.
- To leave the property unchanged, set the box to a gray check.

At any time you can:

- Click **Cancel** to cancel changes made since the last time changes were applied.
- Click **Apply** to save changes to all of the properties for the selected machines. The changes are applied after clicking **OK**.
- Click **OK** to apply all changes since the last apply and close the dialog.

Note After making a change to the NetBackup configuration through any of the Host Properties dialogs, restart all daemons and utilities (including the NetBackup Administration Console) to ensure that the new configuration values are used.

Selecting Multiple Hosts

You may select one or more hosts under Host Properties in order to change settings on multiple hosts at the same time.

The Host Properties tabs use specific conventions regarding multiple host selection:

If a tab contains a **Selected Host** (or similarly named) combo box, all controls on the tab reflect the values for the host currently selected in the **Selected Host** box.

If a tab does *not* contain a **Selected Host** (or similarly named) combo box, settings of all the selected hosts are combined to arrive at a value that is displayed to the user. For example, assume that hosts apricot and jackfruit are selected. If the respective settings have the same value on both the hosts, the dialog controls display that value. If the values of respective settings are different between the selected hosts, the following will hold true for various controls settings:

- Check boxes when multiple hosts are selected:

  The check box turns into a tri-state check box. The user has three choices for this setting: check it, uncheck it or leave it tri-state, where it appears with a grayed tick mark. Keeping it tri-state will not alter this setting on any of the selected hosts. Checking or un-checking it will have an effect on all the selected hosts.

- Radio buttons when multiple hosts are selected:

  None of the buttons in the button group appear selected. Leaving it in that state keeps the hosts untouched. Selecting any one from the group updates the setting on all selected hosts.

- Number spinner when multiple hosts are selected:

  The spinner appears blank. Leaving it blank keeps the setting untouched on the selected hosts. Changing the value updates the setting on all selected hosts.

- Text field when multiple hosts are selected:

  The text field appears blank. Changing the value updates the setting on all selected hosts.

- If the selected hosts are of various operating systems, none of the operating system-specific information appears.

  For example, two clients are selected: Linux client apricot and Windows 2000 client grapefruit. Neither the Windows Client node nor the UNIX Client node will appear in the Host Properties tree, or any of the sub-nodes. If all the selected hosts are running the same operating systems, the corresponding node and sub-node will appear.

Getting Help on Property Settings

While on a properties tab, click **Help**. Or, for help on a specific field, click in the field, then press **`F1`**.

Required Permissions

To change the properties on other machines, the NetBackup server where you logged on using the NetBackup Administration Console must be in the Servers list on the other system.

For example, if you logged on to server shark using the NetBackup Administration Console and want to change a setting on a client tiger, tiger must include shark in its Servers List. (See “Adding a NetBackup Server to a Server List” on page 320.)

Note All updates to a destination machine (unless it is the same as the machine you logged on to using the NetBackup Administration Console) will fail if the target machine has placed a checkbox in **Disallow Server File Writes** on the Universal Settings tab. (See "Universal Settings Tab" on page 249.)

Master Server Properties

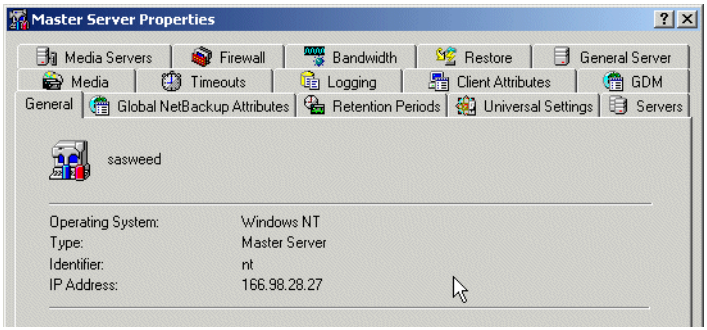
Property settings that pertain to master servers are found in the NetBackup Administration Console under **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**.

Note The following sections describe the **Master Server** property tab settings.After making a change to the NetBackup configuration through any of the Host Properties dialogs, restart all daemons and utilities (including the NetBackup Administration Console) to ensure that the new configuration values are used.

General Tab

The **General** tab provides general information about the selected master server, media server, or client:

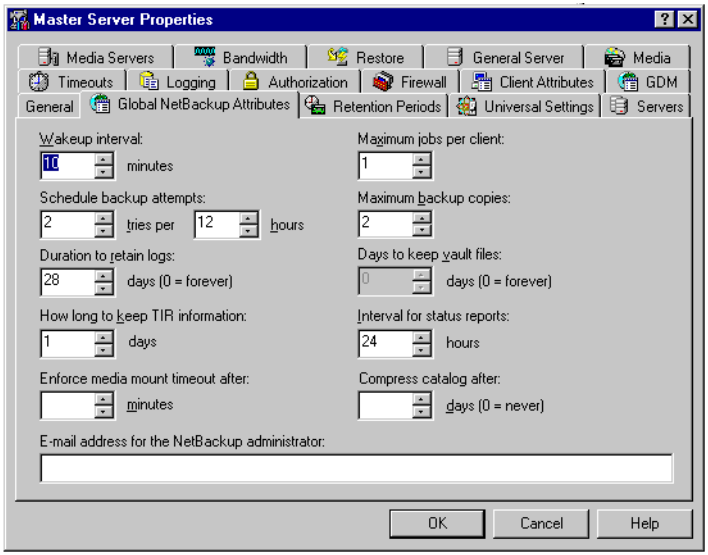
- Server or client name
- Operating system
- Type of machine in the configuration
- Identifier
- IP address



Global NetBackup Attributes Tab

The **Global NetBackup Attributes** properties tab appears under **Master Server**.

The properties, as set here, affect all operations for all policies and clients. The default values are adequate for most installations but can be changed.



Wakeup Interval

Specifies how often the scheduler checks schedules for backups that are due. Long wakeup intervals can cause the scheduler to start too late in a backup window to complete all the backups for a schedule. Minimum setting: 1 minute. Default: 10 minutes.

Schedule Backup Attempts

Note This attribute does not apply to user backups and archives.

Specifies the number of times that NetBackup will try to complete a scheduled backup job during the specified time period. **Schedule Backup Attempts** allows you to limit the number of tries if, for example, a client or drive is down or media is unavailable.

Retries do not occur until all backups on the worklist have been tried at least once within the backup window. If the backup window closes before the retry starts, the job fails with a status code 196.

The number of tries must be greater than 0 in order for scheduled backups to occur. Specifying 0 for number of tries is legal but stops all scheduled backups.

The time period must *always* be greater than 0. Default: 2 tries in 12 hours.

Duration to Retain Logs

Specifies the length of time, in days, that the master server keeps its error catalog, job catalog, and debug log information. NetBackup derives the Backup Status, Problems, All Log Entries, and Media Log Entries reports from its error catalog, so this attribute limits the time period that these reports can cover.

Keep the logs as long as you need them to evaluate failures. For example, if you check the backups every day you can delete the logs sooner than if you check them once a month. However, the logs can consume a lot of disk space so do not keep them any longer than necessary.

A setting of 0 means that NetBackup will keep the logs forever. Minimum duration: 1 day. Default: 28 days. Maximum: forever.

How Long to Keep TIR Information

Specifies the number of days to keep true image restore information on disk. This applies to all policies for which NetBackup is collecting true image restore information.

A setting of 0 means that NetBackup will keep the logs forever. Default: 1 day.

When NetBackup performs a true image backup, it stores two images on the backup media:

- Backed up files
- True image restore information

NetBackup also stores the true image restore information on disk in the *install_path*`\NetBackup\db\images` directory and keeps it for the number of days specified by this global attribute. Keeping the information on disk speeds up restores. If a user requests a true image restore after the information has been deleted from disk, NetBackup retrieves the required information from the media. The only noticeable difference to the user is a slight increase in total restore time. NetBackup deletes the additional information from disk again after one day.

Enforce Media Mount Timeout After

Specifies the number of minutes that NetBackup waits for the requested media to be mounted, positioned, and ready on backups and restores. Default: 0 (no timeout). If you do not specify 0, the value must be 5 minutes or greater.

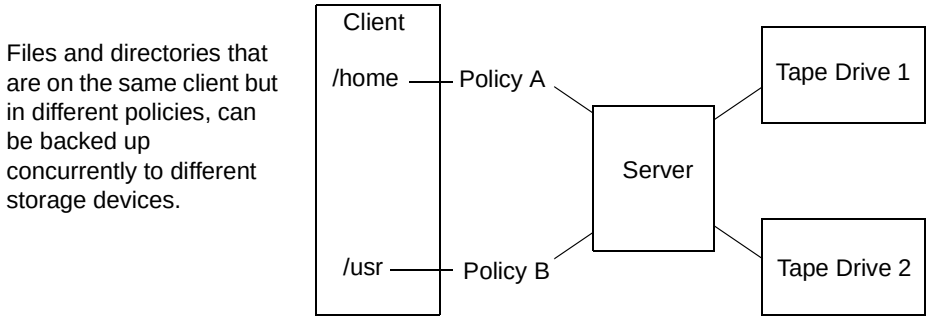
Use this timeout to eliminate excessive waits when it is necessary to manually mount media (for example, when robotic media is out of the robot or off site).

Maximum Jobs per Client

Specifies the maximum number of backup and archive jobs that NetBackup clients can perform concurrently. For NetBackup BusinesServer, the maximum allowed is 8. Default: 1 job.

NetBackup can process concurrent backup jobs from different policies on the same client only if:

- There is more than one storage unit available, or,
- one of the available storage units can perform more than one backup at a time.



You can specify any number of concurrent jobs within the following constraints. Default: 1 job:

- Number of storage devices. NetBackup can perform concurrent backups to separate storage units or to drives within a storage unit. For example, a single Media Manager storage unit supports as many concurrent backups as it has drives. A disk storage unit is a directory on disk so the maximum number of jobs depends on system capabilities.
- Server and client speed. Too many concurrent backups on an individual client interfere with the performance of the client. The actual number that you can use depends on the hardware, operating system, and applications that are running.

  Because **Maximum Jobs per Client** applies to all clients in all policies, set it to accommodate the client that can handle the lowest number of concurrent jobs.
- Network loading. The available bandwidth of the network affects how many backups can occur concurrently. For example, two Exabyte 8500, 8 mm tape drives can create up to a 900-Kilobyte-per-second network load. Depending on other factors, this can be too much for a single Ethernet. If you encounter loading problems, consider backing up over multiple networks or using compression.

  A special case exists when backing up a client that is on the same machine as the server. Here, network loading is not a factor because you do not use the network. Client and server loading, however, is still a factor.

Maximum Backup Copies

Specifies the total number of backup copies that can be created. Choose from between 2 and 10 copies.

Interval for Status Reports

Specifies the default time period during which NetBackup accumulates information to put into a report. For example, a setting of 8 hours provides a report covering the previous 8 hour period. Minimum setting: 1 hour. Default: 24 hours.

Days to Keep Vault Files

Specifies the amount of time that the Vault session directories will be kept. Session directories are found in the following location:

install_path`/netbackup/vault/sessions/`*vaultname*`/sid`*xxxx*

where *xxxx* is the session number. This directory contains vault log files, temporary working files, and report files.

Days to Keep Vault Files is enabled if Vault is installed. Default: 30 days. A value of 0 means that the logs will be maintained forever.

Compress Catalog After

Specifies the number of days that NetBackup waits after a backup before NTFS compressing the image catalog file that has information about the backup. NetBackup uses NTFS file compression and the catalog must be in an NTFS partition for compression to occur.

Default: 0 (Turns off compression and keeps all image catalog files in uncompressed format.)

Administrator E-mail Address

Specifies the address where NetBackup sends notifications of scheduled backups, administrator-directed manual backups, or NetBackup catalog backups. The notification of catalog backups includes the media ID that was used. Specify the address of the NetBackup administrator. Default: no address.

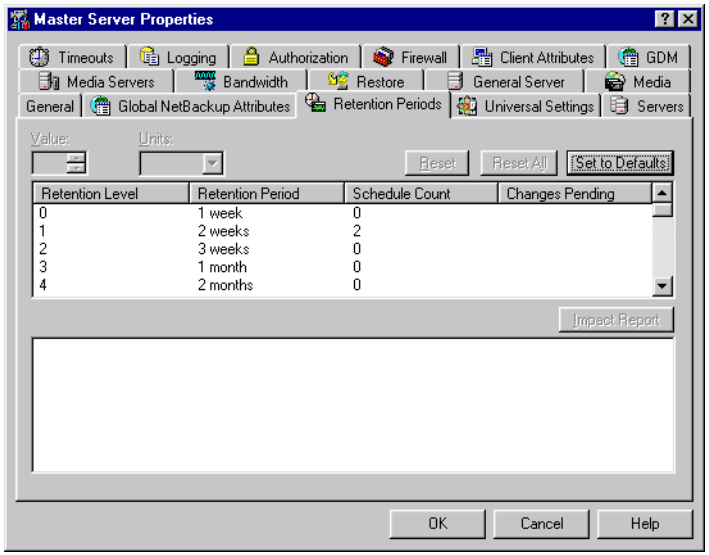
On a Windows NT/2000 NetBackup server, it might be necessary to configure the *install_path*`\NetBackup\bin\nbmail.cmd` script in addition to specifying the above address. This is necessary because, on Windows NT and 2000, NetBackup performs the notification by passing the specified E-mail address, subject and message to the script. The

script then uses the mailing program that you specified in the script to send E-mail to the user. See the comments in the script for configuration instructions. Default: nbmail.cmd does not send E-mail.

Retention Periods Tab

The **Retention Periods** properties tab appears under **Master Server** only.

When setting up a schedule, the selected retention period determines how long NetBackup retains the backups or archives created according to that schedule. There are 25 possible levels of retention from which to select. The properties on the **Retention Period** tab define the length of time associated with each level.



Value

Specifies the retention level setting.

Units

Specifies the units of time for the retention period. The list also includes the special unit, **Infinite**.

Retention Periods List

Lists of the current definitions for the 25 possible levels of retention (0 through 24). The **Schedule Count** column indicates how many schedules currently use each level. If the retention period is changed for a level, it affects all schedules that use that level.

Schedules List

Lists the schedules that use the currently selected retention level, and the policy to which each schedule belongs.

Impact Report Button

Displays a summary of how changes will affect existing schedules. If you change a retention period, click **Impact Report**. The list displays all schedules in which the retention period is less than the frequency period (including schedules that do not use the retention periods that you have just changed.)

Reset Button

Resets the currently selected retention period to its previous value, if it has been changed (as indicated by an asterisk in the Modified column).

Reset All Button

Resets, to their previously configured values, all retention periods that you have changed since the last apply (as indicated by an asterisk in the Modified column).

Set to Defaults

Sets all retention levels to the standard NetBackup defaults.

▼ To change a retention period

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Master Server** > **Host Properties**.
2. If your site has more than one master server, select **File** > **Change Server** to choose the server with the configuration you'd like to change.
3. Double-click the server name in the left pane to display the server's properties.
4. Select the **Retention Periods** tab.
5. Select the retention level that you want to change. Level 9 cannot be changed and remains infinite.

   The policy impact list now displays the names of all schedules that are using the selected retention level as well as the policy to which each schedule belongs.
6. Select the unit of time for the retention period.
7. Type the new retention period in the **Value** box. Values can range from 0 (no retention) to 30 years.

Note After changing either **Units** or **Value**, an asterisk (*) appears in the Changes Pending column to indicate that the period was changed. NetBackup does not change the actual configuration until **Apply** or **OK** is clicked.

8. Click **Impact Report**.

   The policy impact list displays the schedules where the retention period is less than the frequency period (including schedules that do not use the retention periods that you just changed).

   If any schedules are listed, correct the problem by either redefining the retention period or changing the settings for retention or frequency on the schedule.

9. To discard your changes, click one of the following:

   - **Reset**: If you select a retention period that was changed (indicated by an asterisk in the Modified column), clicking **Reset** restores the selection to the value that was set with the last **Apply** or **OK**.

Note The **Reset** button tries to reset the value of the field or entry that was in focus immediately before **Reset** was clicked. To reset an entry, click that entry, then directly click **Reset**.

   - **Reset All**: Restores all retention periods that were changed (indicated by an asterisk in the Modified column), to the values that were set with the last **Apply** or **OK**.
   - **Set to Defaults**: Sets all levels of retention to their standard defaults.
   - **Cancel**: Discards all changes that were made since the last **Apply**, then closes the dialog.

10. To save your changes and update the configuration, click one of the following:

    - **Apply**: Saves changes and leaves the dialog open so you can make further changes.
    - **OK**: Saves changes since the last time you clicked **Apply**. **OK** also closes the dialog.

11. To save the changes, click **OK**.

    To make sure that NetBackup uses the new settings, restart the application.

Note on Redefining Retention Periods

NetBackup, by default, stores each backup on a volume that already has backups at the same retention level. However, NetBackup does not check the retention period defined for that level. This means that redefining the retention period for a level can result in unintentionally storing backups with different retention periods on the same volume. For example, if you change the retention period for level 3 from one month to six months, NetBackup stores future level 3 backups on the same volumes that it previously used (if they are available). That is, they are on the volumes with the level 3 backups that have a retention period of one month.

This is not a problem if the new and old retention periods are of about the same value. However, if you make a major change to a retention period (for example, from one week to infinity), it is best to suspend the volumes that were previously used for that retention level. To do this, proceed as follows:

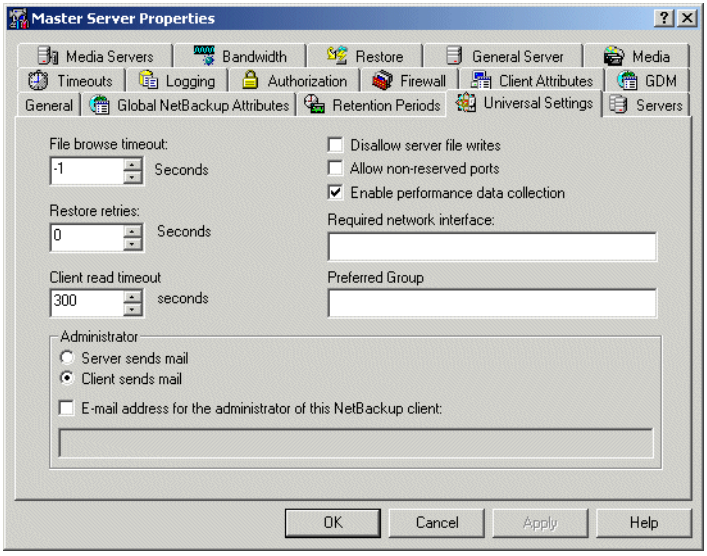
1. Use the NetBackup Media List report to determine which volumes are currently at the level that you are going to suspend.

2. Use the `bpmedia` command to suspend the volumes.

   `bpmedia -suspend -ev` *media_ID*

Universal Settings Tab

The **Universal Settings** properties tab appears under **Master Server**, **Media Servers**, and **Clients**.



File Browse Timeout

Specifies the number of seconds for the client to wait for a response from the NetBackup master server when listing files.

If the **File Browse Timeout** value is set at `-1`, the value will change according to the client type:

- 300 seconds for a Windows client
- 1800 seconds for a UNIX client

Note On a UNIX client, the value in the user's `$HOME/bp.conf` file takes precedence, if it exists, to the setting here.

If **File Browse Timeout** is exceeded, the user receives a socket read failed error even if the server is still processing the request.

Restore Retries

Specifies the number of times a client will try to restore after a failure. Default: 0 (client will not attempt to retry). Change **Restore Retries** only if problems are encountered.

Client Read Timeout

Specifies the number of seconds to use for the client-read timeout on a NetBackup master or remote media server or database-extension client (such as NetBackup for Oracle). Default: 300 seconds.

The client-read timeout on a database-extension client is a special case. Clients can initially require more time to get ready than other clients because database backup utilities frequently start several backup jobs at the same time, slowing the central processing unit.

The sequence on a database-extension client is as follows:

- NetBackup on the database-extension client reads the client's client-read timeout to find the initial value. If the option is not set, the standard five minute default is used.
- When the database-extension API receives the server's value, it uses it as the client-read timeout.

Note For database-extension clients, VERITAS suggests that you set the client-read timeout to a value greater than 5 minutes. 15 minutes is adequate for many installations. For other clients, change **Client read timeout** only if problems are encountered.

Disallow Server File Writes

Prevents the NetBackup server from creating or modifying files on the NetBackup client. For example, checking this box would prevent server-directed restores and remote changes to the client properties.

Once **Disallow Server File Writes** is applied, it can be cleared only by modifying the client configuration. Default: server writes are allowed.

Allow Non-reserved Ports

Specifies that the NetBackup client service (`bpcd`) can accept remote connections from nonprivileged ports (port numbers 1024 or greater). If this entry is not present, `bpcd` requires remote connections to come from privileged ports (port numbers less than 1024). **Allow Non-Reserved Ports** is useful when NetBackup clients and servers are on opposite sides of a firewall.

In addition to changing **Allow Non-Reserved Ports** here, specify that the server use nonreserved ports for this client.

Select **Connect on Non-Reserved Port** on the server properties Client attributes tab.

Enable Performance Data Collection

Specifies to NetBackup to update disk and tape performance object counters. (Applies to only to Windows master and media servers. The NetBackup performance counters can be viewed using the Windows utility, `perfmon`. (See “Using the Performance Monitor” on page 636.)

Required Network Interface

Specifies the network interface that NetBackup uses when connecting to another NetBackup client or server. A NetBackup client or server can have more than one network interface. To force NetBackup connections to be made on a specific network interface, use this entry to specify the network host name of that interface. By default, the operating system determines the one to use.

Example 1 - Client with multiple network interfaces.

Assume a NetBackup client with two network interfaces:

- One network interface is for the regular network. The host name for the regular interface is fred.
- One network interface is for the backup network The host name for the backup interface is fred_nb.

The NetBackup client name setting on both the client and server is fred_nb.

When client fred starts a backup, restore, or list operation, the request goes out on the fred_nb interface and over the backup network. This assumes that fred and the network are set up to do so. If this configuration is not in place, fred can send the request out on the fred interface and over the regular network. The server receives the request from client fred_nb with host name fred and refuses it because the host and client names do not match.

One way to solve this problem is to set up the master server to allow redirected restores for client fred. This allows the server to accept the request, but leaves NetBackup traffic on the regular network.

A better solution is to set **Required Interface** on fred to fred_nb. Now, all backup, restore, and list requests use the fred_nb interface, the server receives requests from client fred_nb with host name fred_nb, and everything works as intended.

Example 2 - Server with multiple network interfaces.

Assume a NetBackup server with two network interfaces:

- One network interface is for the regular network. The host name for the regular interface is barney.
- One network interface is for the backup network The host name for the backup interface is barney_nb

The server list on all NetBackup servers and clients have an entry for barney_nb.

When barney connects to a client for a backup, the request ideally goes out on the barney_nb interface and over the backup network. This assumes that barney and the network are set up to do so. If this configuration is not in place, barney can send the request out on the barney interface and over the regular network. The client now receives the request from barney rather than barney_nb and refuses it as coming from an invalid server.

One way to solve this problem is to add an entry for barney to the server list on the client. The client now accepts requests from barney, but NetBackup traffic continues on the regular network.

A better solution is to set **Required Network Interface** on barney to barney_nb. Now, when barney connects to a client, the connection is always through the barney_nb interface and everything works as intended.

Preferred Group

Specifies the domain group name that is passed by this computer to the server when NetBackup-user authorization is used. The default is the user's primary *domain\group*. The **Preferred Group** entry is intended specifically for use with NetBackup enhanced authorization. The entry is case sensitive and must be in the form *domain\group*. For example:

```
NTDOMAINNAME\Backup Operators
```

When **Preferred Group** is specified, Windows NT global groups are checked to determine if the user is a member of the specified *domain\group*:

- If the specified *domain\group* is a global group and the user is a member, then this *domain\group* value is used.
- If the specified *domain\group* is a local group or the user is not a member, then the user's primary *domain\group* is used. Note that if the domain name is an empty string or is the name of the local machine, it is considered to be local.

Some NetBackup processes also use the **Preferred Group** entry for Media Manager authorization. For more information on this, see "Media Manager Configuration File (vm.conf)" in the *NetBackup Media Manager System Administrator's Guide*.

Adding a Preferred Group entry in the Universal Setting tab has the following effect on UNIX and Windows NT/2000 systems:

On UNIX

The `PREFERRED_GROUP` entry is added to the `bp.conf` file:

`PREFERRED_GROUP` = *netgroup name*

- If the `bp.conf` configuration file has a `PREFERRED_GROUP` entry, the `innetgr()` function is used to determine if the user is in the netgroup (for further details refer to the `innetgr` man page).
- If the `PREFERRED_GROUP` entry does not exist or the user is not a member of the netgroup, the local group name is obtained.

Note Netgroups are not supported for Sequent systems.

On Windows NT/2000

The `PREFERRED_GROUP` NetBackup configuration is added to the KEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config registry key.

A check is made to determine if the user is a member of domain\group. This check is limited to NT global groups. In other words, if **Preferred Group** is set to a domain local group, a match will not occur and the user's primary domain\group will be used.

If the `PREFERRED_GROUP` configuration option does not exist or the user is not a member of the domain\group, the user's primary domain\group is obtained. When the domain name is an empty string or is the name of the local machine, it is considered to be local.

Server Sends Mail

Specifies that the server send the mail to the address specified in the box for the administrator's E-mail address. This is useful if the client cannot send mail.

Client Sends Mail

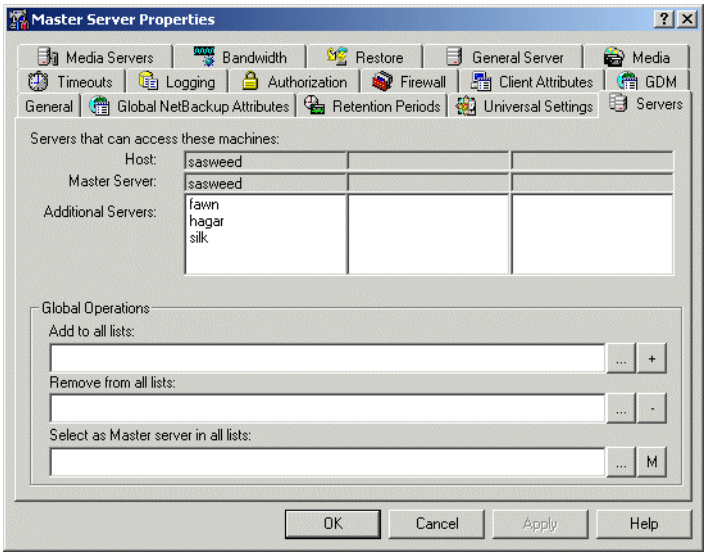
Specifies that the client send the E-mail to the address specified in the box labeled for the administrator's E-mail address. If the client cannot send E-mail, select **Server Sends Mail**.

E-mail Address for Administrator of this NetBackup Client

Specifies the E-mail address of the administrator on the client and is the address where NetBackup sends status on the outcome of automatic or manual backup operations for the client. By default, no E-mail is sent. To enter multiple addresses or a mail aliases, do not include spaces between entries.

Servers Tab

The **Servers** tab displays the NetBackup server list on each host. The server list displays the NetBackup servers that each host recognizes.



Host

Displays the configuration for the host(s) that are currently selected.

Master Server

Specifies the master server for the server specified as **Host**.

During installation, NetBackup sets the master server to the name of the system where the server software is being installed. NetBackup uses the master server value to validate server access to the client and to determine which server the client must connect to in order to list and restore files.

- To add a new server, click **New** and type the name of a server.
- To change the master server, select another server from the list and click **Make Master**.

During installation, NetBackup sets the master server to the name of the host where the server software is being installed. NetBackup uses the master server name to validate server access to the client and to determine which server the client must connect to in order to list and restore files.

- To delete a server, select a server from the list and click **Delete**.
- To configure access to a remote server, add to the server list the name of the host seeking access. For more information, see " Administering a Remote Master Server" on page 320.

Additional Servers

Lists additional servers that can access the server specified as **Host**.

Global Operations

Add to All Lists

Specifies names to add to the lists. To add a name, either type it in the box or click the browse button (...) and select one. Use commas or spaces to separate names. Then, click the + button. (Note that the browse button does not necessarily display all available machines. This is dependent on the network configuration.)

Remove from All Lists

Specifies names to remove from the lists. To remove a name, either type it in the box or click the browse button (...) and select one. Use commas or spaces to separate names. Then, click the - button.

If delete confirmation is selected, NetBackup prompts you for confirmation before making the deletion. To select delete confirmation click **Customize** on the **View** menu in the Configure - NetBackup window and go to the **Preferences** tab in the **Customize** dialog.

Select as Master Server in All Lists

Specifies the master server for all machines in the **Servers That Can Access These Machines** box. To select the master server, either type a name in the box or click the browse button (...) and select one. Then, click the **M** button.

If the server is not already in the server list for a machine, it is added automatically in addition to being selected as the master server.

▼ To change server lists

- To add a name to all lists, use the **Add to All Lists** box.

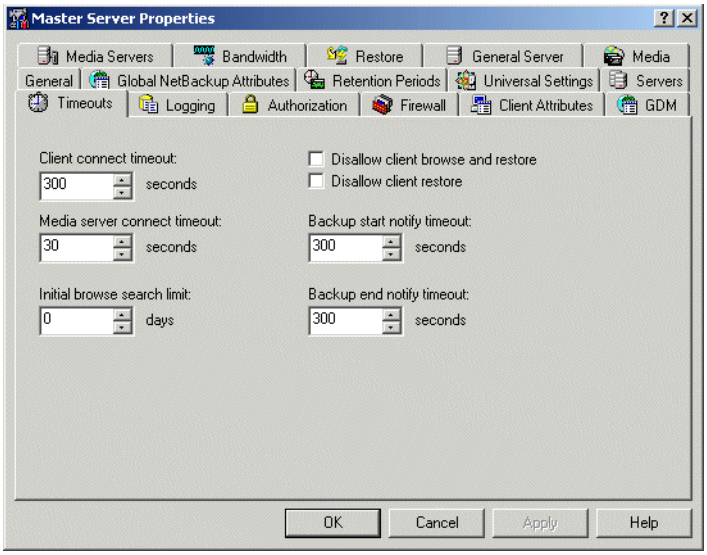
- To delete a name from all lists use the **Remove from All Lists** box.
- To change the master server in all lists, use the **Select as Master Server in All Lists** box.

Right clicking when the pointer is in the **Hosts**, **Master Servers**, or **Additional Servers** fields displays a shortcut menu with commands that apply to that field.

Note If you change the server list on the master server, exit all NetBackup administrator interface programs. Then, stop and restart both the NetBackup request service and NetBackup Database Manager service on that server This ensures that the change is recognized.

Timeouts Tab

The **Timeouts** tab appears under **Master Server**, **Media Server** and **Clients**. The **Timeouts** tab defines the following timeout settings for the selected NetBackup server or client.



Client Connect Timeout

Specifies the number of seconds that the server waits before timing out when connecting to a client. Default: 300 seconds.

Initial Browse Search Limit

Specifies the number of days back that NetBackup searches for files to restore. The value is in days. For example, to limit the browse range to the seven days prior to the current date specify 7.

This limit is specified on the master server and applies to all NetBackup clients. It can also be specified on a client and in this instance applies only to that client and can reduce the size of the search window from what you specify on the server (the client setting cannot make the window larger).

By default, NetBackup includes files from the time of the last-full backup through the latest backup for the client. If the client belongs to more than one policy, then the browse starts with the earliest of the set of last-full backups.

Disallow Client Browse and Restore

Denies list and restore requests for all clients if **List Restore** on the **Client Attributes** tab is set to **Not Specified**. By default, **Disallow Client Browse and Restore** is not selected.

Disallow Client Restore

Denies restore requests for all clients if **List Restore** on the **Client Attributes** tab is set to **Not specified**. By default, **Disallow Client Restore** is not selected.

Backup Start Notify Timeout

Specifies the number of seconds that the server waits for the `bpstart_notify` script on a client to complete. Default: 300 seconds.

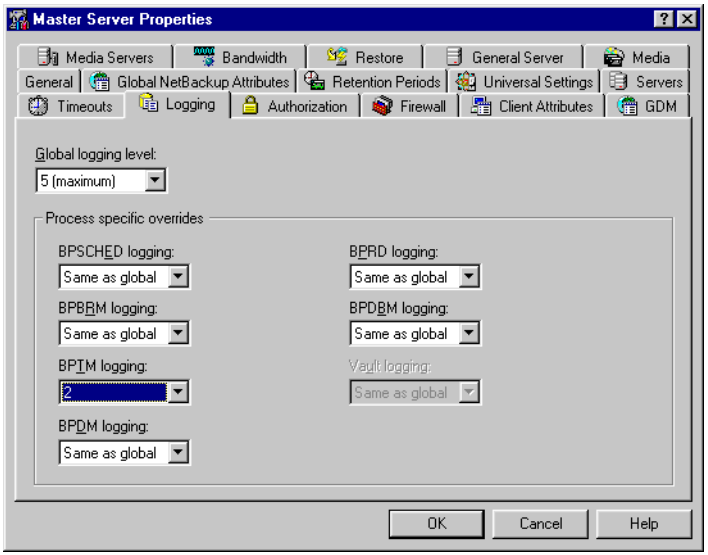
Note If you change this timeout, verify that **Client Read Timeout** is set to the same or higher value.

Backup End Notify Timeout

Specifies the number of seconds that the server waits for the `bpend_notify` script on a client to complete. Default: 300 seconds.

Note If you change this option, verify that **Client Read Timeout** is set to the same or higher value.

Logging Tab



The **Logging** tab appears as a properties tab under **Master Server**, **Media Server** and **Clients**. The available settings differ between a server and a client.

Indicating a logging level does not enable logging. First, you must create a log directory for every process in the following location:

install_path`\NetBackup\logs\`*process_name*

On a Windows server, you can create all of the NetBackup debug log directories at once by double-clicking `mklogdir.bat` in the following directory:

install_path`\NetBackup\logs\`

Enable Logging

Enable Logging appears on the Logging tab under Client properties. Used for debugging purposes, **Enable Logging** controls the amount of information that the NetBackup server writes to logs. To change the value, select **Enable Logging**, then enter the new value in the **Verbose Logging Level** box.

Global Logging Level

Used for debugging purposes, the logging levels control the amount of information that the NetBackup server writes to logs.

Six levels are supported. A value of 0 sets logging to minimum (default) and a value of 5 sets it to maximum.

Caution Use the default setting of 0 unless advised otherwise by VERITAS Technical Support. Other settings can cause the logs to accumulate large amounts of information.

Some NetBackup processes allow individual control over the amount of information the process writes to logs. For those processes, it is possible to specify a different logging level other than the **Global Logging Level**.

BPSCHED Logging

If you wish to override the **Global Logging**, select a logging level for `bpsched`: 0 (minimum) through 5 (maximum).

BPBRM Logging

If you wish to override the **Global Logging**, select a logging level for `bpbrm`: 0 (minimum) through 5 (maximum).

BPTM Logging

If you wish to override the **Global Logging**, select a logging level for `bptm`: 0 (minimum) through 5 (maximum).

BPDM Logging

If you wish to override the **Global Logging**, select a logging level for `bpdm`: 0 (minimum) through 5 (maximum).

BPRD Logging

If you wish to override the **Global Logging**, select a logging level for `bprd`: 0 (minimum) through 5 (maximum).

BPDBM Logging

If you wish to override the **Global Logging**, select a logging level for `bpdbm`: 0 (minimum) through 5 (maximum).

Vault Logging

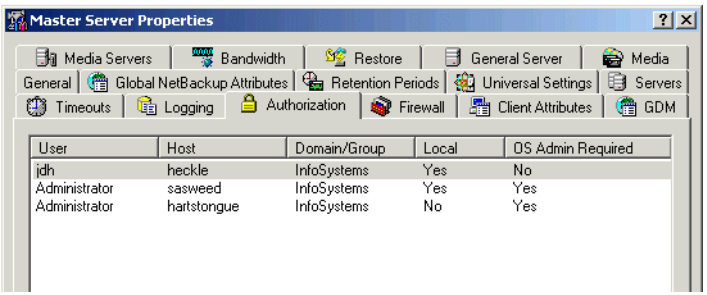
If you wish to override the **Global Logging**, select a logging level for `bpvault`: 0 (minimum) through 5 (maximum).

Verbose Logging Level

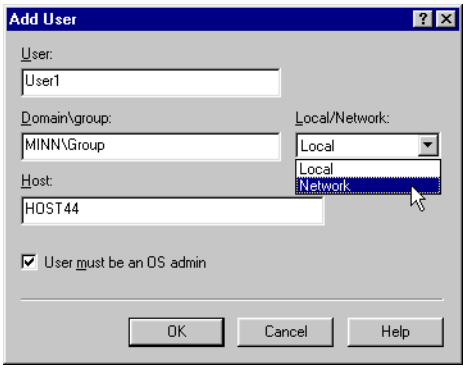
The only configurable logging level for NetBackup clients is the **Verbose Logging Level**. If you wish to override the **Global Logging**, select a **Verbose** Logging Level: 0 (minimum) through 5 (maximum).

Authorization Tab

The **Authorization** tab appears as a properties tab under **Master Server**, **Media Server** and **Clients**.



Click **New** to add an authorized user or click **Change** to change the configuration of an existing authorized user. The Add User or Change User dialog appears.



User

Type the username or * for all users.

Domain\Group

Type the Windows domain and group name in the form `domain\group` or the UNIX local group name or the UNIX netgroup name. Or, enter * for all groups.

Host

Type the remote NetBackup Administrative Console host name, or * for all hosts.

Local/Network

Indicate whether the group is a local or network group.

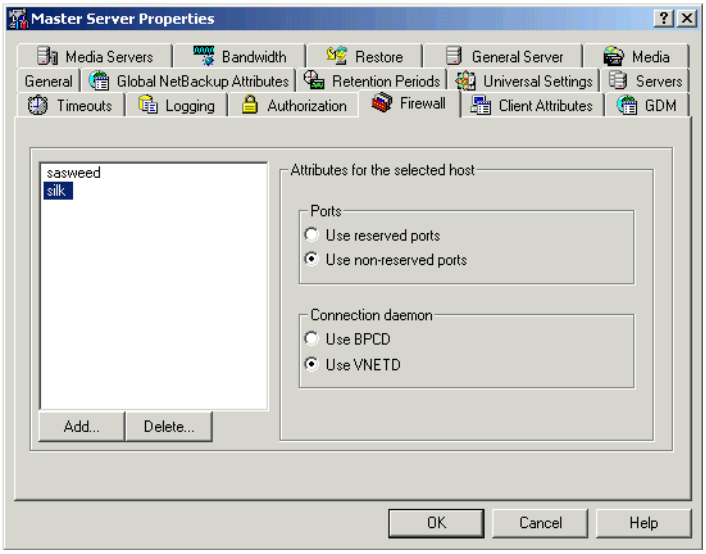
User must be an OS Administrator

Place a check in the box to indicate that the user must be an OS administrator.

For configuration information, see Chapter 1, “Enhanced Authentication and Authorization” on page 371.

Firewall Tab

The **Firewall** tab appears as a properties tab under **Master Server** and **Media Server**.



Add Button

Click **Add...** to add an entry for a host.

Delete Button

Select a host name in the list, then click **Delete** to remove the host from the list.

Use Reserved Ports

Check to specify that the server will be connected to using a reserved port number.

Use Non-reserved Ports

Specifies that the server will be connected to using a non-reserved port number. If you select this option, enable **Allow Nonreserved Ports** for the selected server. See the Universal Settings dialog under **Host Properties** > **Master Servers** or **Host Properties** > **Media Servers**.

Use BPCD

Specifies that the server will be connected to using the traditional call-back method.

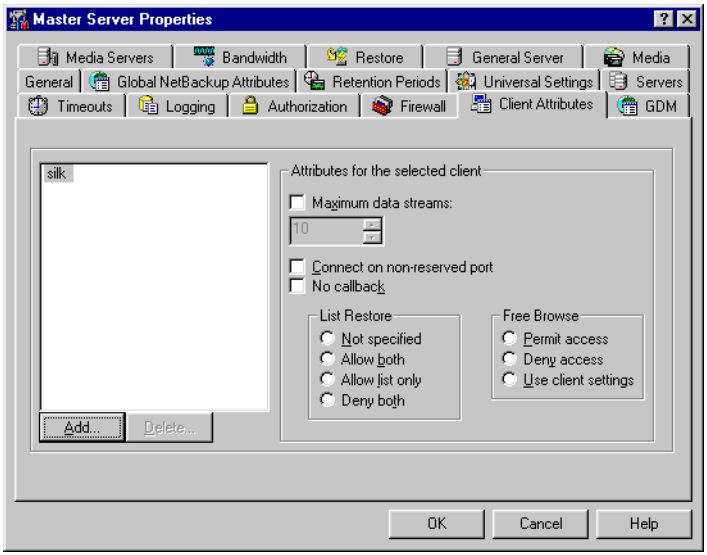
Use VNETD

Specifies that the server will be connected to using the VERITAS Network daemon (`vnetd`).

Client Attributes Tab

The **Client Attributes** tab appears as a properties tab under **Master Server**.

The **Client Attributes** tab allows you to change properties for the clients of the selected master server.



Clients List

Lists the clients that are in the client database on the master server that was selected when you opened this tab. The client must be in this database before you can change its settings on this tab. The client database consists of directories and files in the following directory:

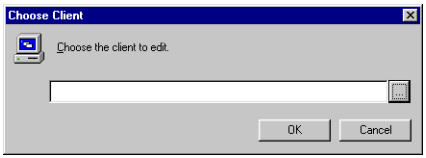
install_path`\NetBackup\db\client`

If the desired clients are not listed, use the **Add** button to add them. Use the **Delete** button to delete clients from the database.

Note If you are using dynamic addressing (DHCP), use the `bpclient` command to add clients to the client database. (See “Dynamic Host Name and IP Addressing” on page 408 for instructions.)

Add Button

Adds a client to the client database. Clicking the **Add** button displays the Choose Client dialog. Type a client name in the field or click the browse button (...) and select a client.



Delete Button

Deletes the selected client from the client database. Select the client in the list box and click the button.

Maximum Data Streams

Specifies the maximum number of concurrent data streams that are allowed for the selected clients. To change the setting, select the clients in the list box and enter a value from 1 to 99. Default: 0 (the setting has no effect).

Maximum Data Streams interacts with the **Maximum Jobs Per Client** (**Host Properties** > **Master Server** > **Global NetBackup Attributes**) and **Limit Jobs Per Policy** (a policy setting) as follows:

- If **Maximum Data Streams** is 0 (default), the lowest value of **Maximum Jobs Per Client** and **Limit Jobs Per Policy** is the limiting factor.
- If **Maximum Data Streams** is nonzero, then NetBackup ignores **Maximum Jobs Per Client** and uses the lowest value of **Maximum Data Streams** and **Limit Jobs Per Policy** as the limiting factor.

Connect on Non-reserved Port

Specifies that the server use a nonreserved port when connecting to the selected clients. To enable this setting:

1. Select the desired client in the list box.
2. Select the **Connect on Nonreserved Port** check box.
3. Enable **Allow Nonreserved Ports** for each of the selected clients. See the **Universal Settings** tab under **Host Properties** > **Clients**.

No Callback

When connecting to the client's `bpcd`, if **No Callback** is clear, the client connects back to the server on a random port number (default). If checked, the client connects back to the server on the `vnetd` port number.

List Restore

Specifies the permissions that client users have for listing and restoring backups and archives. To change the **List Restore** settings, select the clients in the list box and choose the desired action:

- To leave the setting at the default, select **Not Specified**.
- To allow users on the selected clients to list and restore, select **Allow Both**.
- To allow users on the select clients to list but not restore, select **Allow List Only**.
- To prevent both lists and restores, select **Deny Both**.

If you select **Not Specified**, the standard default action is to allow both lists and restores. However, you can change this by selecting **Disallow Client Browse and Restore** or **Disallow Client Restore** on the **Timeouts** tab for this master server.

- Selecting **Disallow Client Browse and Restore** on the **Timeouts** tab changes the default to deny both lists and restores.
- Selecting **Disallow Client Restore** on the **Timeouts** tab changes the default to deny lists.

If you select both the **Disallow Client Browse and Restore** and **Disallow Client Restore**, NetBackup behaves as though only **Disallow Client Browse and Restore** is selected.

See “Disallow Client Browse and Restore” on page 257 and “Disallow Client Restore” on page 257.

Free Browse

Used with a corresponding setting on the client to specify whether users can list and restore automatic backups. By default, users cannot list or restore these backups (this setting does not affect user backups and archives).

▼ To change the Free Browse setting

1. On the master server, select the clients in the list box and specify **Allow**, **Deny**, or **Use** in order to obtain the desired action as shown in the table below.
2. On Microsoft Windows clients, set up the registry to specify the desired action as shown in the table below. For instructions, see the online help or user’s guide for the client.
3. On UNIX clients, the client setting is always **Allow** and cannot be changed.

Free Browse Settings

Server Setting	Client Setting	List and Restore Automatic Backups
Allow (default)	Allow (default)	No
Allow	Deny	No
Allow	Use	Yes

Free Browse Settings (continued)

Server Setting	Client Setting	List and Restore Automatic Backups
Deny	Allow	No
Deny	Deny	No
Deny	Use	No
Use	Allow	Yes
Use	Deny	No
Use	Use	Yes

Examples

▼ To permit lists and restores for all users on a client

1. Expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**. Select the Client Attributes tab.
2. In the client database list box, select the client you wish to change.
3. Under **Free Browse**, click **Use client settings**.
4. On the client, leave the setting at the default (**Allow**).

▼ To permit lists and restores for selected users on a client

Note Applies only to Microsoft Windows clients.

1. Expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**. Select the Client Attributes tab.
2. In the client database list box, select the client you wish to change.
3. Under **Free Browse**, leave the setting for this client at the default (**Allow**).
4. On the client, change the setting to **Use** and give the selected users read access to the **Use** key.

▼ To deny lists and restores for all users on a client

1. Expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**. Select the Client Attributes tab.
2. In the client database list box, select the client you wish to change.
3. Under **Free Browse**, change the setting for the client to **Deny**.
4. On the client, leave the setting at the default (**Allow**).

▼ To deny lists and restores for selected users on a client

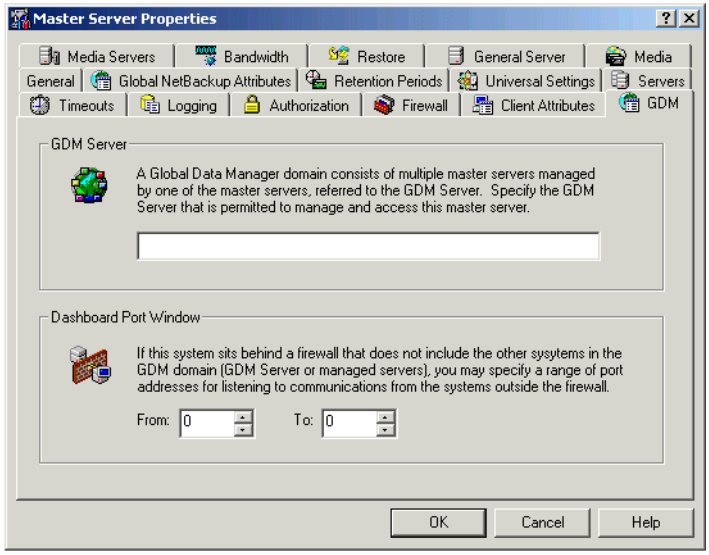
Note Applies only to Microsoft Windows clients.

1. Expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**. Select the Client Attributes tab.
2. In the client database list box, select the client you wish to change.
3. Under **Free Browse**, leave the setting for this client at the default (**Allow**).
4. On the client, change the setting to **Deny** and give the selected users read access to the **Deny** key.

GDM Tab

The **GDM** tab appears as a properties tab under **Master Server**, **Media Servers** and **Clients**.

The **GDM** tab identifies the Global Data Manager server that can administrate the master server selected. A GDM server is a NetBackup server that has GDM software installed. GDM provides features for remote administration of master servers.



GDM Server

Specify the NetBackup server that will be the GDM server. The GDM server is permitted to manage and access the master servers. **GDM Server** does not appear when configuring a client.

Dashboard Port Window

Specifies the range of port addresses that can be used for listening to communications from systems outside of the firewall around this master server.

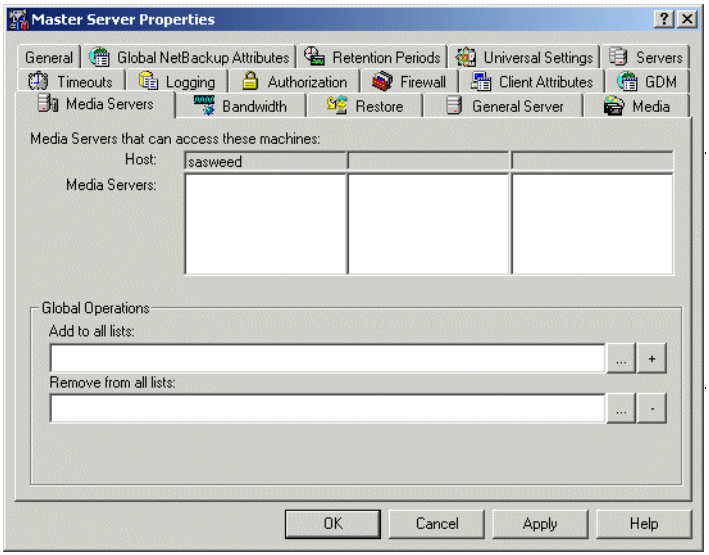
If 0 is specified for the **From** number, the operating system determines the nonreserved port to use. The default range is from 0 to 0, which means the operating system chooses the port.

This setting applies when connecting to a client configured to accept only reserved ports. (Under the Clients host properties, see **Allow Nonreserved Ports** on the **Universal Settings** tab.)

Media Servers Tab

The **Media Servers** tab appears as a properties tab under **Master Server** and **Media Server**.

Note This tab does not apply to NetBackup BusinesServer NetBackup BusinesServer does not support remote media servers.



Additional Servers

Specifies additional servers that can access the server specified as **Host**.

Add to All Lists

Specifies names to add to the lists. To add a name, either type it in the box or click the browse button (...) and select one. Use commas or spaces to separate names. Then, click the + button. (Note that the browse button does not necessarily display all available machines. This is dependent on the network configuration.)

Remove From All Lists

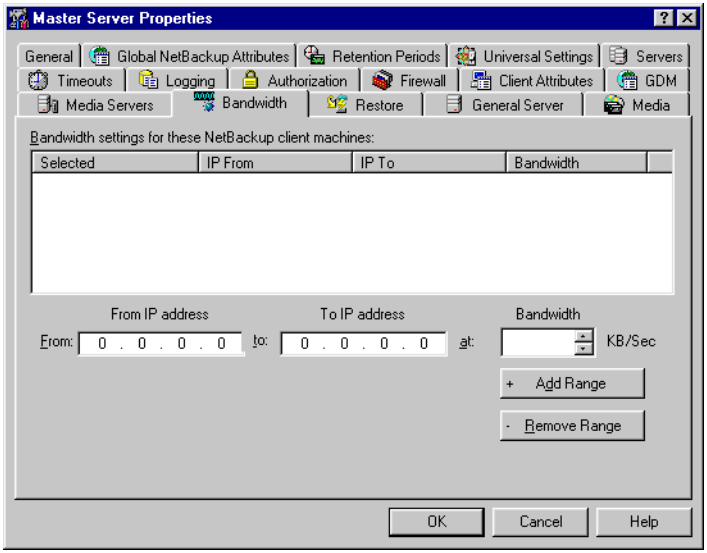
Specifies names to remove from the lists. To remove a name, either type it in the box or click the browse button (...) and select one. Use commas or spaces to separate names. Then, click the - button.

Bandwidth Tab

The **Bandwidth** tab appears as a properties tab under **Master Server** and **Media Server**.

The **Bandwidth** tab specifies limits for the network bandwidth used by one or more NetBackup clients of the selected server.

The limiting occurs on the client side of the backup connection and applies only to backups. Restores are unaffected. By default, the bandwidth is not limited.



Bandwidth Settings for These NetBackup Client Machines

Lists the clients in the range of IP addresses that were added.

From IP Address

The beginning of the IP address range of the clients and networks to which the entry applies. An example is `10.1.1.2`

To IP Address

The end of the IP address range of the clients and networks to which the entry applies. An example is `10.1.1.9`

Bandwidth

The bandwidth limitation in kilobytes per second. A value of 0 disables limiting for the individual client or the range of IP addresses covered by this entry.

For example, a value of 200 indicates 200 kilobytes per second.

Add Range Button

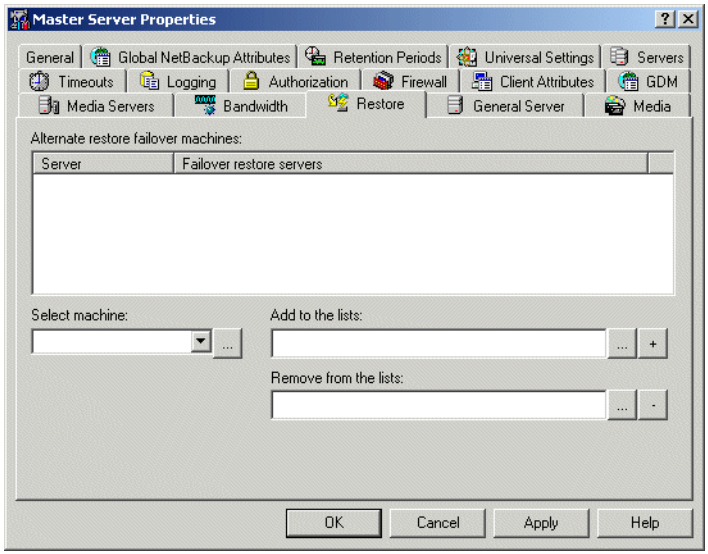
Prepares an entry using the **From**, **To**, and **Bandwidth** fields and adds it to the bandwidth table. An entry is added for each of the selected clients.

Remove Range Button

Removes a selected entry from the bandwidth table.

Restore Tab

The **Restore** tab appears as a properties tab under Master Server and Media Servers.



The **Restore** tab defines properties for controlling how NetBackup performs automatic failover to another NetBackup server in a master and media server cluster, if the regular server is temporarily inaccessible for a restore. The automatic failover does not require administrator intervention. By default, NetBackup does not perform automatic failover.

Examples of when to use this capability:

- Two or more servers are sharing a robot and each has connected drives. When a restore is requested, one of the servers is temporarily inaccessible.
- Two or more servers have standalone drives of the same type. When a restore is requested, one of the servers is temporarily inaccessible.

In these instances, inaccessible means that the connection between `bprd` on the master server and `bptm` on the media server (through `bpcd`) fails. Possible reasons for the failure are:

- Media server is down.
- Media server is up but its `bpcd` is not responding (for example, if the connection is refused or access is denied).

- Media server is up and `bpcd` is all right but `bptm` is having problems (for example, if `vmd` is down or `bptm` cannot find the required tape).

To enable automatic failover to an alternate server in a media and master server cluster, modify the NetBackup configuration on the master server as follows:

1. Specify the failover machines for the server:

   a. In the **Select Machine** box, specify the server for which you want failover protection.

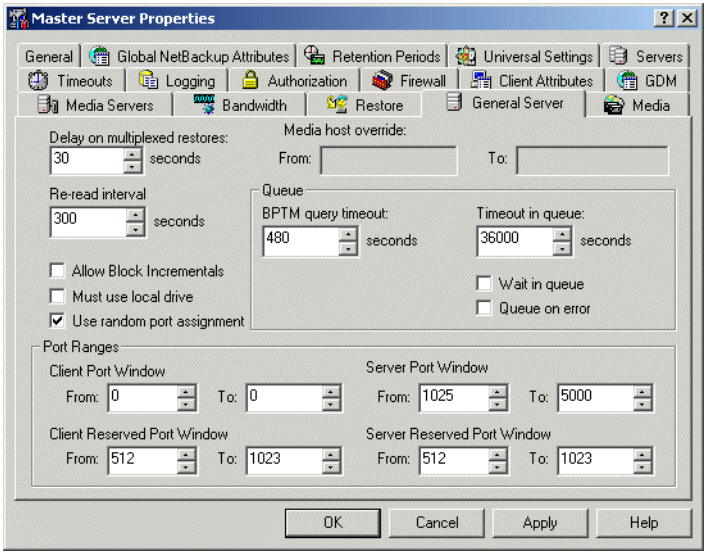
   b. To add a failover server specify it in the **Add to the Lists** box.

   c. To remove a failover server, specify it in the **Remove from the Lists** box.

2. Stop and restart the NetBackup Request daemon on the master server where you are changing the configuration.

General Server Tab

The **General Server** properties tab appears under **Master Server** and **Media Servers**.



Delay on Multiplexed Restores

Applies to multiplexed restores and specifies how long (in seconds) the server waits for additional restore requests of files and (or) raw partitions that are in a set of multiplexed images on the same tape. All the restore requests that are received within the delay period are included in the same restore operation (one pass of the tape). Default: delay of 30 seconds.

Re-read Interval

Determines how often NetBackup checks storage units for available drives. If this value is too high, too much time elapses between drives becoming available and NetBackup discovering their availability, thus delaying backup jobs. If it is too low, checks are made more often than necessary thus wasting system resources. Default: 300 seconds (5 minutes.)

Must Use Local Drive

If the client is a server and this box is selected, backups must occur on a local drive. If the client is not a server, this setting has no effect.

This option increases performance because backups are done locally rather than possibly being sent across the network. For example, in a SAN environment you can create a storage unit for each SAN media server and then mix the media-server clients with other clients in a policy that uses ANY AVAILABLE storage unit. When a backup starts for a client that is a SAN media server, the backups go to the SAN connected drives on that server.

Use Random Port Assignments

Specifies that when NetBackup requires a port for communication with NetBackup on other computers, it will choose one randomly from those that are free in the allowed range. For example, if the range is from 1023 through 5000, it chooses randomly from the numbers in this range.

Default: option is selected. If deselected, NetBackup chooses numbers sequentially, starting with highest number that is available in the allowed range. For example, if the range is from 1023 through 5000, NetBackup chooses 5000 (assuming it is free). If 5000 is being used, port 49999 is chosen.

Timeout in Queue

Determine how long a job can be requeued while NetBackup waits for a required storage unit if it is currently unavailable. Default: 36000 seconds (10 hours.)

Queue

BPTM query timeout

Determines the time that the scheduler waits for a drive-count query to `bptm` to complete. If you have problems with timeouts, you can modify this setting to extend the time that the scheduler waits. Default: 480 seconds (8 minutes).

Timeout in queue

Determines how long a requeued job waits for an unavailable required storage unit.

Wait in queue

Causes jobs to enter the requeued state if the required storage unit becomes unavailable (for example, a drive goes down). The jobs will then run when NetBackup can use the storage unit again. A job fails if its backup window closes or the **Timeout in queue** time expires before the storage unit becomes available. By default, the option is not selected and jobs are not requeued.

Queue on error

Causes jobs to enter the requeued state on startup, if the required storage unit is not available. The jobs will then run when NetBackup can use the storage unit again.

By default, the option is not selected and jobs fail with a status code 219 if the storage unit is not available. This property requires that the `WAIT_IN_QUEUE` entry also be selected or the job will fail immediately anyway with a 219 status if NetBackup cannot use the storage unit.

Client Port Window

Specifies the range of nonreserved ports on this computer that are used for connecting to NetBackup on other computers. This setting applies when connecting to NetBackup on a computer configured to accept nonreserved ports (see **Allow Nonreserved Ports** on the **Universal Settings** tab).

If 0 is specified for the **From** number, the operating system determines the nonreserved port to use. The default range is from 0 to 0, which means the operating system chooses the port.

Client Reserved Port Window

Specifies the range of reserved ports on this computer that are used for connecting to NetBackup on other computers. This setting applies when connecting to NetBackup on a computer configured to accept only reserved ports (see **Allow Nonreserved Ports** on the **Universal Settings** tab).

Default range: 512 through 1023. Note that if you specify 0 for the **From** number, a nonreserved port is used instead and is chosen by the operating system.

Server Reserved Port Window

Default range: 512 through 1023. Note that if you specify 0 for the **From** number, a nonreserved port is used instead and is chosen by the operating system.

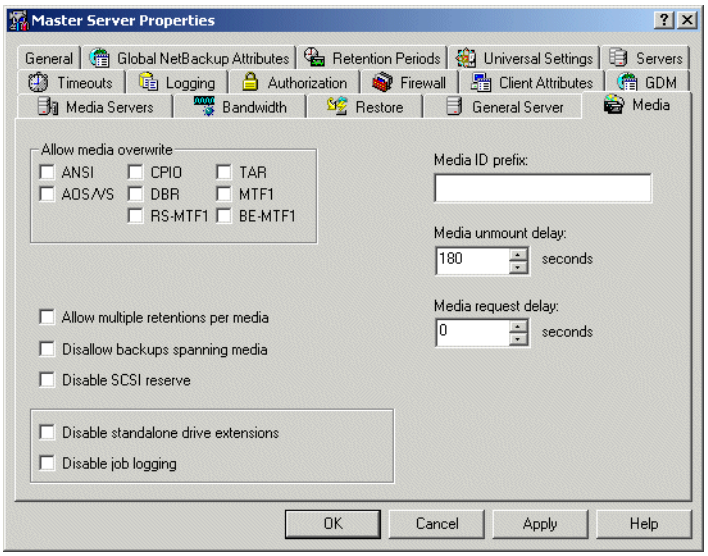
Server Port Window

Specifies the range of nonreserved ports on which this computer accepts connections from NetBackup on other computers. This setting applies when connecting to a client configured to accept only nonreserved ports. (See **Allow Nonreserved Ports** on the **Universal Settings** tab in the **Client Properties** tab.) **Server Port Window** does not appear when configuring a client.

Default range: 1024 through 5000. Note that if you specify 0 for the **From** number, the operating system determines the nonreserved port to use.

Media Tab

The **Logging** tab appears as a properties tab under **Master Server** and **Media Server**. It contains properties that control how NetBackup manages media.



Allow Media Overwrite

Overrides NetBackup's overwrite protection for the following media formats on removable media:

- **ANSI:** ANSI labeled media
- **AOS/VS:** Data General AOS/VS backup format
- **CPIO:** cpio format
- **DBR:** A VERITAS backup format that is no longer used
- **RS-MTF1:** VERITAS Remote Storage MTF1 media format
- **TAR:** Tar format
- **MTF1:** Backup Exec

In the case where only MTF1 is checked, all other MTF formats, apart from Backup Exec MTF will be allowed to be overwritten.

- **BE-MTF1:** When checked, Backup Exec MTF media will be allowed to be overwritten.

To disable overwrite protection, select the desired format. For example, select **CPIO** to permit NetBackup to overwrite the cpio format.

Note You must allow overwriting the MTF1 format if you are using RSM robots. This is necessary because Free Media Labels are in MTF1 format.

By default, NetBackup does not overwrite any of the above formats on removable media, and logs an error if an overwrite attempt occurs. This format recognition requires that the first block on a variable length media be less than or equal to 32 kilobytes.

If media contains one of the protected formats and you do not permit media overwriting, NetBackup takes the following actions:

- If the volume has not been previously assigned for a backup, NetBackup:
  - Sets the volume's state to FROZEN
  - Selects a different volume
  - Logs an error
- If the volume is in the NetBackup media catalog and has been previously selected for backups, NetBackup:
  - Sets the volume's state to SUSPENDED
  - Aborts the requested backup
  - Logs an error
- If the volume is mounted for a backup of the NetBackup catalog, the backup is aborted and an error is logged that indicates the volume cannot be overwritten.
- If the volume is mounted to restore files or list the media contents, NetBackup aborts the request and logs an error that indicates the volume does not have a NetBackup format.

Allow Multiple Retentions Per Media

Allows NetBackup to mix retention levels on media. It applies to media in both robotic and nonrobotic drives. By default, the check box is clear and each volume can contain backups of only a single retention level.

Disallow Backups Spanning Media

Prevents backups from spanning media. If the end of media is encountered and this option is present, the media is set to FULL and the operation terminates abnormally (applies to both robotic and nonrobotic drives). By default, the check box is clear and backups can span media.

Disable SCSI Reserve

Turns off the use of SCSI reserve to all tape devices from this host.

SCSI Reserveblocks access to the device from other host systems. With this disabled, other hosts may send commands to the device that cause a loss of data.

Disable Standalone Drive Extensions

Specifies that during a backup, NetBackup does not automatically attempt to use whatever labeled or unlabeled media it finds in a nonrobotic drive. By default, standalone drive extensions are enabled. (See “How NetBackup Uses Media in Standalone Drives” on page 654.)

Disable Job Logging

Disables the logging of job information used by the NetBackup Activity Monitor. By default, job logging occurs.

Media ID Prefix

Applies to media in nonrobotic drives and specifies the media ID prefix that is used to create media IDs when unlabeled media is found in a nonrobotic drive. The prefix must be one to three alpha-numeric characters. NetBackup appends remaining numeric characters. By default, NetBackup uses A and assigns media IDs such as A00000, A00001, and so on.

For example, if you specify FEB, NetBackup appends the remaining numeric characters so the assigned media IDs become FEB000, FEB001, and so on (note that this does not work with the Configure Volumes wizard).

Media Unmount Delay

Applies only to user operations, including backups and restores of database agent clients, such as those running NetBackup for Oracle. When you specify this option, the media unload is delayed for the specified number of seconds after the requested operation has completed. This delay reduces unnecessary media unmounts and media positioning in cases where the media is requested again a short time later.

The delay can range from 0 to 1800 seconds. (Default: 180 seconds.) If you specify 0, the media unmount occurs immediately upon completion of the requested operation. Values greater than 1800 are set to 1800.

Media Request Delay

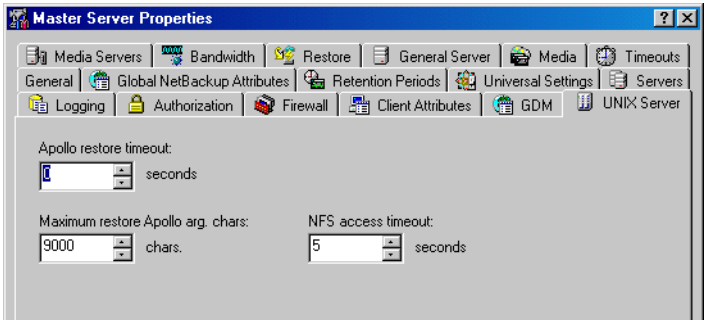
Applies only to nonrobotic drives and specifies the number of seconds that NetBackup waits for a drive to become ready. This is useful if a gravity feed stacker is used on a nonrobotic drive and there is a time delay between the dismount of one media and the mounting of another. Default: 0 seconds.

During the delay period, NetBackup checks every 60 seconds to see if the drive is ready. If the drive is ready, NetBackup uses it. Otherwise, it waits another 60 seconds and checks again. If the total delay is not a multiple of 60, the last wait is the remainder. If the delay is less than 60 seconds, NetBackup checks only once at the end of the delay.

For example, assume you set the delay to 150 seconds. Here, NetBackup waits 60 seconds, checks for ready, waits 60 seconds, checks for ready, and then waits 30 seconds and checks for ready the last time. If the delay had been 50 seconds (this short a delay is not recommended), NetBackup would have checked only once, at the end of 50 seconds.

UNIX Server

The **UNIX Server** tab appears as a properties tab under **Master Server** if the selected master server is a UNIX system.



Apollo Restore Timeout

Applies only to Apollo clients and specifies the number of seconds to use for client-read timeouts for restores. Default: 0 (no timeout). Change this value only if problems are encountered.

Maximum Restore Apollo arg Characters

Applies only to Apollo clients, and specifies the maximum number of characters to allow on an `rbak` command. Default: maximum number of characters is 9000. Change this value only if problems are encountered.

NFS Access Timeout

Specifies the number of seconds that the backup process waits when processing the mount table before considering an NFS file system unavailable. Default: 5 seconds.

Media Server Properties

Property settings that pertain to media servers are found in the NetBackup Administration Console under **Master Server** > **NetBackup Management** > **Host Properties** > **Media Servers**. The following sections point to the **Media Servers** property :

Note After making a change to the NetBackup configuration through any of the Host Properties dialogs, restart all daemons and utilities (including the NetBackup Administration Console) to ensure that the new configuration values are used.

- “General Tab” on page 241
- “Global NetBackup Attributes Tab” on page 242
- “Retention Periods Tab” on page 246
- “Universal Settings Tab” on page 249
- “Servers Tab” on page 254
- “Timeouts Tab” on page 256
- “Logging Tab” on page 258
- “Authorization Tab” on page 260
- “Firewall Tab” on page 261
- “Client Attributes Tab” on page 262
- “GDM Tab” on page 267
- “Media Servers Tab” on page 268
- “Bandwidth Tab” on page 269
- “Restore Tab” on page 270
- “General Server Tab” on page 271

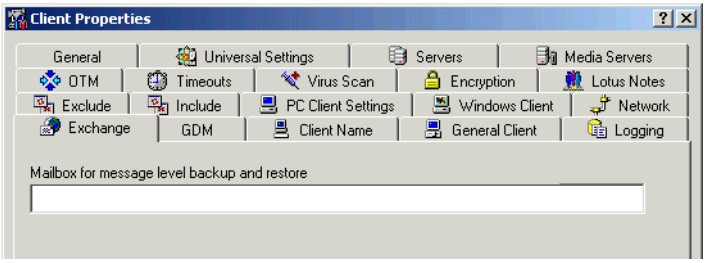
- “Media Tab” on page 274

Client Properties

Property settings that pertain to clients are found in the NetBackup Administration Console under **Master Server** > **NetBackup Management** > **Host Properties** > **Clients**. The following sections describe or point to the **Clients** property tabs.

- “General Tab” on page 241
- “Universal Settings Tab” on page 249
- “Servers Tab” on page 254
- “Media Servers Tab” on page 268
- “Exchange Tab” on page 280
- “Client Name Tab” on page 281
- “General Client Tab” on page 282
- “OTM (Open Transaction Manager) Tab” on page 283
- “Timeouts Tab” on page 292
- “Encryption Tab” on page 292
- “Lotus Notes Tab” on page 294
- “Exclude Tab” on page 295
- “Include Tab” on page 297
- “PC Client Settings Tab” on page 303
- “Windows Client Tab” on page 304
- “Network Tab” on page 306
- “Client Settings Tab (UNIX)” on page 307
- “UNIX Client2 Tab” on page 308
- “Busy File Settings” on page 309
- “NetWare Tab” on page 310

Exchange Tab



The **Exchange** tab under **Clients** defines the mailbox to associate with the NetBackup Client Service account. You must define this mailbox only if the NetBackup client and NetBackup Microsoft Exchange Server agent software are installed on the Microsoft Exchange Server.

The NetBackup Client Service account must be associated with a valid Exchange mailbox for NetBackup to access the mailboxes and folders during backups and restores. We recommend that you create a uniquely named mailbox for the NetBackup Client service account. If a mailbox is not created for the NetBackup Client service, you can use any existing mailbox on the Microsoft Exchange Server to which the NetBackup Client service account is granted logon rights.

The following section explains the mailbox setting. For more information on this mailbox setting, see the *NetBackup for Microsoft Exchange Server System Administrator's Guide*.

The following topic explains the mailbox setting. For more information on this mailbox setting, see the *NetBackup for Microsoft Exchange Server System Administrator's Guide*.

Mailbox for Message Level Backup and Restore

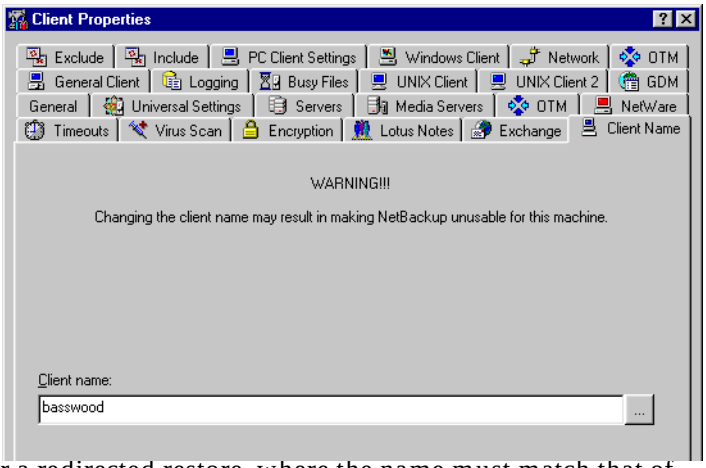
Specifies the mailbox for the NetBackup Client service account. The mailbox can be one of the following:

- An Exchange mailbox name
- A fully qualified name of the form

  /O=*org_name*/OU=*site_name*/CN=*server_name*/CN=*mailbox_name*
- A mailbox alias

Client Name Tab

The **Client Name** tab under Client defines the client name for a single selected client.



Client Name

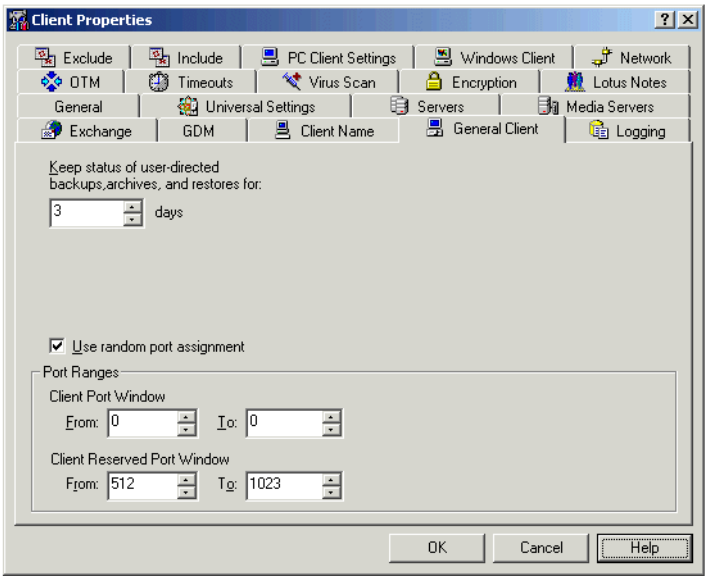
Specifies the NetBackup client name for the selected client. This is the name by which the client is known to NetBackup and it must match the name used by the policy that is backing up the client; the only exception is for a redirected restore, where the name must match that of the client whose files are being restored. The client name is initially set during installation.

If the value is not specified, NetBackup uses the name set in the Network application in the control panel (Windows client) or the `hostname` command (UNIX client).

It can also be added to a `$HOME/bp.conf` file on a UNIX client but this is normally done only for redirected restores. The value in the `$HOME/bp.conf` file takes precedence if it exists.

General Client Tab

The **General Client** tab appears as a properties tab under **Clients** only.



Keep Status of User-directed Backups, Archives, and Restores

Applies to Microsoft Windows clients and specifies the number of days for the system to keep progress reports before automatically deleting them. The minimum allowable value is zero. There is no maximum allowable value. Default: 3 days. Any value less than 0 is set to 3 days.

Random Ports

Specifies that when NetBackup requires a port for communication with NetBackup on other computers, it will choose one randomly from those that are free in the allowed range. For example, if the range is from 1023 through 5000, it chooses randomly from the numbers in this range.

If this option is not selected NetBackup chooses numbers sequentially, starting with highest number that is available in the allowed range. For example, if the range is from 1023 through 5000, NetBackup chooses 5000 (assuming it is free). If 5000 is being used, port 4999 is chosen.

Client Port Window

Specifies the range of nonreserved ports on this computer that are used for connecting to NetBackup on other computers. This setting applies when connecting to NetBackup on a computer configured to accept nonreserved ports. (See “Allow Non-reserved Ports” on page 251.) If you specify 0 for the **From** number, the operating system determines the nonreserved port to use. Default range: 0 to 0, which means the operating system chooses the port.

Client Reserved Port Window

Specifies the range of reserved ports (on this computer) that are used for connecting to NetBackup on other computers. This setting applies when connecting to NetBackup on a computer configured to accept nonreserved ports. (See “Allow Non-reserved Ports” on page 251.) Default range: 512 through 1023. Note that if you specify 0 for the **From** number, a nonreserved port is used instead and is chosen by the operating system.

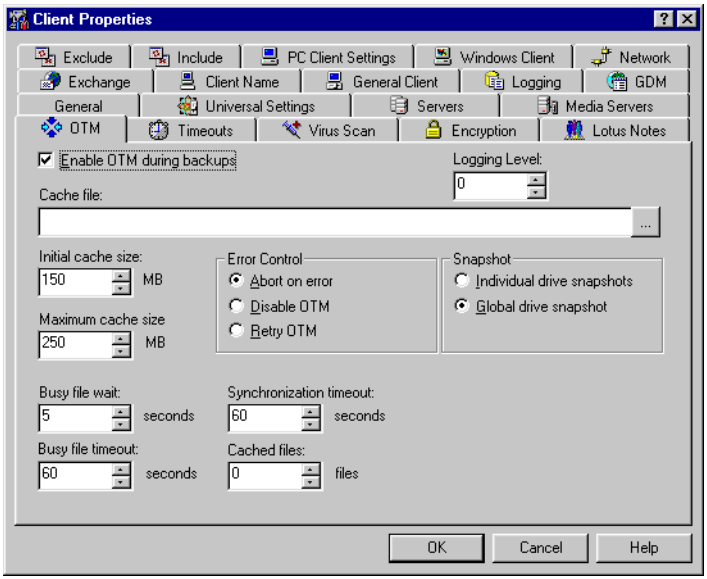
Logging Tab

For a description of the properties on the Logging tab, see “Logging Tab” on page 258.

OTM (Open Transaction Manager) Tab

On Microsoft Windows and NetWare clients, NetBackup uses OTM (Open Transaction Manager) to back up files, databases, and applications that are open or active. The **OTM** tab applies to Microsoft Windows and NetWare clients and contains properties that define the behavior of OTM.

Open Transaction Management is a separately-priced option for NetBackup BusinesServer and can be installed on Microsoft Windows clients from the same CD-ROM as the NetBackup server software. The OTM license is entered on the master server.



The **OTM** tab appears as a properties tab under **Clients** only.

OTM does its job by establishing a point-in-time view (or snapshot) of the data on the drives containing files to be backed up. NetBackup then backs up the selected files as they exist at the time of the snapshot, regardless of file system activity. The snapshot is maintained by using a cache mechanism to store changes that occur during the backup.

In addition to eliminating problems with busy files, OTM keeps all relationships between files in the backup intact. For example, assume that keywords in files A and B must be synchronized for an application to work. Without

OTM, if A is backed up but B is changed before it is backed up, the two files are not synchronized after a restore and the application will not work. With OTM, all files are backed up as they exist at a single point in time so relationships are maintained and these problems cannot occur.

The following steps are the sequence of events during a backup with open transaction management:

1. Before the backup begins, OTM waits for a quiet period to occur when no writes are being performed on the drives that have the data to be backed up. This wait is required to ensure that the file system is in a consistent state.

   The length of the quiet period is defined by the **Busy File Timeout** setting. If a quiet period of sufficient length does not occur within the time specified by **Busy File Timeout**, the backup proceeds without open transaction management.

2. If a quiet period of sufficient length is detected, OTM performs the actions necessary to record the snapshot.

3. The backup begins and NetBackup starts reading data from the client. If an application requests a read or write during the backup, OTM reads or writes the disk or its cache as necessary to maintain the snapshot and provide accurate data to the application.

Enable OTM During Backups

Enables open transaction management. This box must be checked for open transaction management to occur.

Cache File

Specifies the location of the cache file that contains the copy of data that changes during the backup. For best performance, place the cache file on a drive that is not backed up.

By default, NetBackup determines the cache location at run time, which is the system-configured `temp` folder.

If you wish to specify another location, the path must point to a specific file name. If the path points only to a folder, OTM will not create a snapshot.

Initial Cache Size

Specifies the initial size of the cache file in megabytes. If no value is specified, NetBackup sets it to 10 MB.

Maximum Cache Size

Specifies the maximum cache size (in megabytes) of the cache file. The guideline for **Maximum Cache Size** is to set it to 10% of all used disk space. For example, if the used disk space is 1 GB, set the maximum cache to 100 MB. A shortcut is to set maximum cache size to 0 MB and let NetBackup determine the appropriate value at run time. Default: 50 MB maximum cache size.

If the cache file reaches this size and more cache is required, the action depends on the **Error Control** setting:

- If **Error Control** is set to **Abort on Error** (default), the backup aborts.
- If **Error Control** is set to **Disable OTM**, open transaction management is turned off and the backup continues. However, relationships between the backed up files can be lost because the snapshot is not used.
- If **Error Control** is set to **Retry OTM**, NetBackup disables open transaction management and then attempt to enable it again before continuing the backup. This second try starts over with a new snapshot, so as with **Disable OTM**, relationships between backed up files can be lost.

Busy File Wait

Specifies the duration (in seconds) of the quiet period that must occur before NetBackup starts OTM. The quiet period is a period of time during which no writes are being performed on the drives or volumes to be backed up. Default: 5 seconds.

Busy File Timeout

Specifies how many seconds to wait for a quiet period to occur. If this time expires, the backup proceeds but without open transaction management. Default: 60 seconds.

Individual Drive Snapshots

Specifies that OTM takes a snapshot of each drive and backs it up before proceeding to the next drive.

For example, assume that drives `C` and `D` are being backed up. Here, OTM:

1. Takes a snapshot of drive `C`, backs it up, and discards the snapshot.
2. Takes a snapshot of drive `D`, backs it up, and discards the snapshot.

Open transaction management is enabled on only on one drive at a time, depending on which one is being backed up. This mode is useful when it is not necessary to maintain relationships between files on the different drives.

Global Drive Snapshot

Specifies that OTM takes a snapshot that includes all drives that are part of the backup, then backs up the drives.

For example, assume that drives C and D are being backed up. Here, OTM:

1. Takes a snapshot of C and D.
2. Backs up C, then backs up D.
3. Discards the snapshot.

Open transaction management remains enabled on both the C and the D drives for the entire duration of the backup. This mode is useful when it is necessary to maintain the relationships between files on the different drives.

Logging Level

Specifies the logging level for open transaction management but does not affect other logging. This allows you to obtain more information about an open transaction management problem without affecting the logging level for other parts of the backup. The value can range from 0 to 10 with level 10 providing the most information.

Error Control

Specifies the behavior of the backup when an open transaction management error is encountered during a backup. The most likely error is a cache full condition. The possible settings are as follows:

- **Abort on Error:** Abort the backup (default).
- **Disable OTM:** Disable open transaction management and continue the backup. Regarding the file that had a problem during the course of the backup—the user will not be able to see the file in the backup and therefore will be unable to restore the file.
- **Retry OTM:** Disable open transaction management and then attempt to enable it again before continuing the backup. Regarding the file that had a problem during the course of the backup—the user will not be able to see the file in the backup and therefore will be unable to restore the file.

Use **Disable OTM** or **Retry OTM** only if there is no concern about file relationships. With either of these settings, file relationships can be affected if, for example, two files are backed up from different snapshots or one is from a snapshot and the other one is not from a snapshot.

Synchronization Timeout

Synchronization Timeout applies to NetBackup clients using NetBackup 3.2 and is intended for use with multiple data streams. The setting specifies how long NetBackup waits to determine if other backup jobs are going to start for this schedule and client before enabling open transaction management. Default: 60 seconds of wait time. If another backup starts within this time period, the wait cycle restarts.

For example, if **Synchronization Timeout** is at the default, the first backup starts and waits 60 seconds for other backups. If a second backup starts 30 seconds into the wait cycle, the wait cycle restarts for both backups. If no further backups start within the second 60 second period, the first backup will have waited 90 seconds and the second backup will have waited 60 seconds. If **Allow Multiple Data Steams** is not set for the policy, you can eliminate the initial wait period by setting **Synchronization Timeout** to 0.

Regarding any file that has a problem during the course of the backup—the user will not be able to see the file in the backup and therefore will be unable to restore the file. Another backup will be required.

Cached Files

Specifies the frequency with which OTM clears its cache during a backup and can help to reduce the size of the cache file. For example, if this value is set to 50, then after every 50 files that are backed up, OTM clears its cache of data that it possesses for those files. A lower value results in clearing the cache more often but can also decrease performance. The default level is 0, indicating that cache clearing does not occur.

When **Global Drive Snapshot** is also selected, the **Cached Files** setting works as follows. Assume that **Global Drive Snapshot** is selected and you have two drives, C and D. Also, assume both drives are backed up and OTM places the cache on drive C.

- If **Cached Files** is 0, the cache is never cleared and cannot grow past the **Initial Cache Size** setting. This means you must always set **Initial Cache Size** for the maximum amount of data expected.
- If **Cached Files** is greater than 0, OTM clears the cache of data for drive C after the drive C backup is complete. OTM then allows the cache to grow to the **Maximum Cache Size** setting and clears it periodically according to the **Cached Files** setting. This allows you to set **Initial Cache Size** to a lower value because if more space is required, OTM can increase to the **Maximum Cache Size** setting.

Guidelines for Setting OTM Cache

The required settings for **Initial Cache Size** and **Maximum Cache Size** depend on the system that is being backed up and how OTM is configured. OTM always places the cache in the configured system temp folder unless the **Cache File** setting is specified.

The requirement for the **Initial Cache Size** depends on whether the cache is placed on a drive where open transaction management is used:

- If the cache file is on a drive where open transaction management is being used, the size of the cache file does not grow past the initial size. Here, the initial cache size must be large to hold the maximum amount of data that is anticipated (10% of the used disk space is the guideline).
- If the cache file is placed on a drive where open transaction management is not used, the size of the cache file can grow to the maximum size. Here, initial cache size can be set to less than the maximum because it will grow.

The snapshot setting determines the drives where NetBackup uses open transaction management and at what point it is enabled:

- **Individual Drive Snapshot** enables open transaction management on each drive as it is backed up. Here, it is possible to place the cache on a drive where open transaction is not used so a smaller initial cache size is possible.
- **Global Drive Snapshot** attempts to enable open transaction management on all drives that are backed up at the start of the backup. Here, the cache can grow from its initial size only if there is a drive that is not being backed up so the cache can be placed on that drive.

Example

Assume Machine A has four drives: `C`, `D`, `E`, `F`. Also, assume the backup is set to back up only drives `C` and `D`. The following is a description of how NetBackup creates the cache for each snapshot method.

Individual Drive Snapshot

1. The backup starts.
2. Open transaction management is enabled on drive `C` and a snapshot is taken of that drive.
3. The cache file is placed in the system-configured `temp` folder and is allowed to grow, if that folder is not on the `C` drive.
4. Drive `C` is backed up.

5. Open transaction management is disabled and the drive `C` snapshot discarded.

6. Open transaction management is enabled on drive `D` and a snapshot taken of that drive.

7. The cache file is placed in the system-configured `temp` folder and is allowed to grow, if that folder is not on the `D` drive.

8. `D` drive is backed up.

9. Open transaction management is disabled and the drive `D` snapshot discarded.

Global Drive Snapshot

1. The backup starts.

2. Open transaction management is enabled on drives `C` and `D` and a snapshot is taken of both drives.

3. The cache file is placed in the system-configured `temp` folder and is allowed to grow, if that folder is not on the `C` or `D` drive.

4. `C` drive is backed up, then `D` drive is backed up.

5. Open transaction management is disabled and the snapshot is discarded.

In all the methods discussed, the cache file tracks changes on all drives where it is enabled. The probability of the cache filling up depends on the number of drives it is tracking:

- The cache file for the Global Drive Snapshot method has the greatest chance of filling up because it is tracking changes across two drives.
- The cache file for the Individual Drive Snapshot method is least likely to fill up because it is tracking only one drive at a time.

If data does not have to be synchronized across drives or multi-streaming is not used, then the Individual Drive Snapshot method is the best choice. If data must be synchronized across drives, use the Global Drive Snapshot method.

Assuming you choose the correct method, the guideline for maximum cache size is to set it to 10% of all used disk space. For example, if your used disk space is 1 GB, set the **Maximum Cache Size** to 100 MB cache file. A shortcut is to configure the **Maximum Cache Size** to 0 MB and let NetBackup determine the appropriate value at run time.

Possible Causes of a Cache Full Condition

There are two major reasons for a cache full condition:

- Busy system. The cache full condition is usually reached because the system is busy and files are changing at the time of the backup.
- Large numbers of files. As backups proceed, the last-access time is updated on each file and this information is cached. If the system has a many files, a large amount of access-time update information is cached and can cause a cache full condition.

In the second case, if you are not concerned about the last access time, you can disable it from being updated by adding the following registry entry:

Key: `HKEY_LOCAL_MACHINE:\SYSTEM\CurrentControlSet\Control\FileSystem`

Value: `NtfsDisableLastAccessUpdate`

Data Type: `REG_DWORD` with a value of `1`

Reboot the system when you are done.

For example, a machine contains a folder with 10,000 subfolders, each of which contains 20 files. Without this value, the amount of data sent to the cache file is 260 MB. With this value added, the amount of data sent to the cache file is 0 MB.

A status code 11 (system call failed) is one symptom of a full open transaction management cache.

Using OTM with Databases

There are special considerations regarding using OTM (Open Transaction Manager) to back up and restore databases.

Many popular database vendors provide a formal application program interface (API) specifically designed for use with backup products. VERITAS works closely with many database vendors to ensure these interfaces are stable, efficient, and reliable when used in conjunction with NetBackup and the various NetBackup database extension features. Many of these APIs were jointly developed to ensure that data is protected and can be restored when needed. Oracle, Microsoft (SQL Server, Exchange), IBM (Lotus Notes, DB2), NCR (Teradata), Sybase and Informix are examples of database vendors that provide an API for use with backup products. VERITAS strongly recommends that the NetBackup database extension features be used when a backup API is available and when backing up a database in a hot mode is required.

Databases with an API

Hot backups are done on active databases and only by using these formal APIs will the confidence of a backup and the ability to perform a successful restore be achieved. VERITAS does not recommend that OTM be used for hot backups of these databases.

Cold or inactive backups of these databases may be possible with OTM, but success varies with each database vendor. Customers should contact the specific database vendor to identify the recommended method for database backup where data reliability is ensured as database programs recover from a point-in-time restore differently. If the data being backed up and restored does not conform to the specification designed into the database product being used, the integrity of the database can be in question.

Databases without an API

When using OTM to back up databases that do not have a backup and restore API, the safest method is to back up the databases when the database is inactive (cold). For databases where there is no VERITAS database extension product, shut down the database and perform a file system level or cold backup.

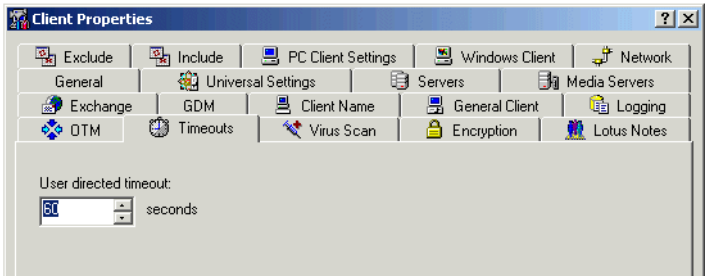
If the databases cannot be backed up cold and the only option is a hot backup, set **Busy File Wait** to 5 seconds. If the file system does not achieve a quiescent or inactive state, it will not perform the OTM snapshot. NetBackup does not fail the backup when a quiescent state is not achieved. Instead, NetBackup continues the backup as if OTM was not being used. The result is that NetBackup skips open, active, or locked files. The backup job ends with an exit status code 1, indicating that the backup job completed but not all files were successfully backed up.

If OTM is used to back up database environments, VERITAS strongly recommends first backing up the data and validating that the backup exited with a Status 0. Then, restore the database and confirm the integrity of the data and the functionality of the database.

Using OTM to back up active databases without using a formal API presents risk. Customers should contact the database supplier to ensure support of database backups using point-in-time technology. Also, significant back up and restore testing should be performed to assure database availability and reliability.

Timeouts Tab

The **Timeouts** tab under **Clients** contains the following setting:



User Directed Timeout

Applies to Microsoft Windows clients and specifies the number of seconds that are allowed between the time that a user makes a backup or restore request and when the operation begins. The operation fails if it does not begin within this time period.

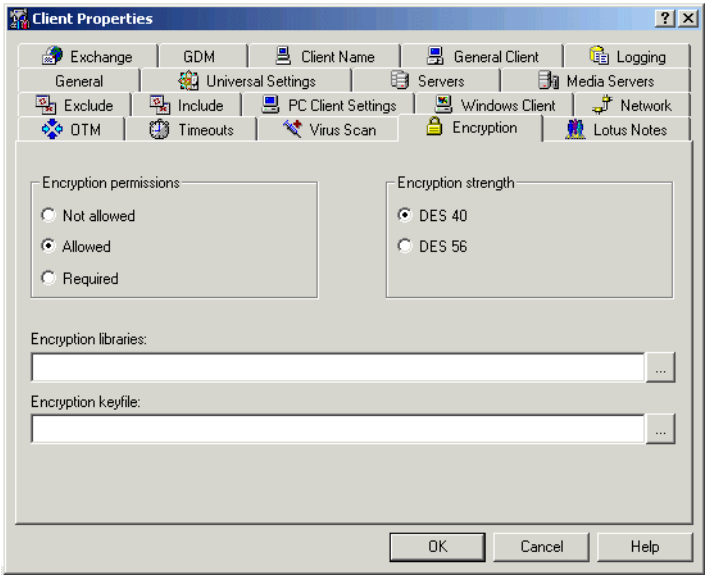
There is no minimum or maximum value. Default: 60 seconds.

Encryption Tab

Encryption is available only if NetBackup Encryption, a separately-priced option, has been installed on both the NetBackup server and the remote clients.

The **Encryption** tab under **Clients** defines properties that control encryption on remote clients.

For more specific information on the Encryption option, see the *NetBackup Encryption System Administrator's Guide*.



Encryption Permissions

Defines the encryption options on NetBackup clients. NetBackup sets this on the client when you run the `bpinst` command on the NetBackup master server. Do not change the setting or create it manually unless it has been accidentally deleted. If it is necessary to change this setting, select the check box and click the desired button:

- **Not Allowed:** Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is an error. This option is the default for a client that has not been configured for encryption.
- **Allowed:** Specifies that the client allows either encrypted or unencrypted backups.
- **Required:** Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is an error.

Encryption Strength

Defines the encryption strength on NetBackup clients. NetBackup sets this option on the client when you run the `bpinst` command on the NetBackup master server.

Do not change this setting or set it manually unless it has been accidentally deleted. If it is necessary to change the setting, select the desired button:

- **DES_40:** Specifies 40-bit DES encryption. This is the default value for a client that has not been configured for encryption.
- **DES_56:** Specifies 56-bit DES encryption.

Encryption Libraries

Defines the folder that contains the encryption libraries on NetBackup clients. NetBackup sets this option on the client when you run the `bpinst` command on the NetBackup master server.

Do not change this setting or set it manually unless it has been accidentally deleted. The default value is

- On Windows systems: *install_path*`\bin\`

  Where *install_path* is the directory where NetBackup is installed and by default is `C:\Program Files\VERITAS`.
- On UNIX systems: `/usr/openv/lib`
- On Macintosh systems: `:System Folder:Extensions:`

If it is necessary to change the setting, specify the new name.

Encryption Keyfile

Defines the file that contains the encryption keys on NetBackup clients. NetBackup sets this attribute on the client when you run the `bpinst` command on the NetBackup master server.

Do not change this setting or set it manually unless it has been accidentally deleted. The default value is:

- On Windows systems: *install_path*`\NetBackup\bin\keyfile.dat`

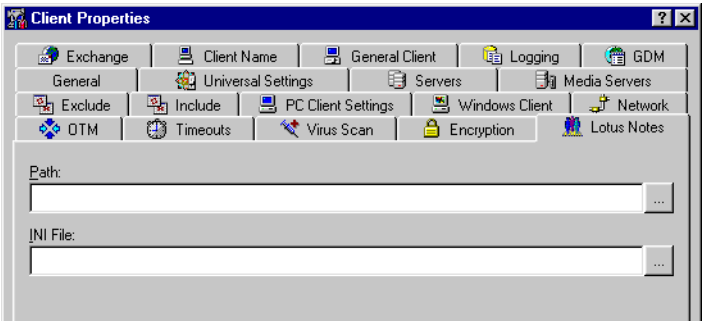
  Where *install_path* is the folder where NetBackup is installed and by default is `C:\VERITAS`.

- On UNIX systems: `/usr/openv/netbackup/keyfile`
- On Macintosh systems: `:System Folder:Preferences:NetBackup:keyfile`

If it is necessary to change the setting, specify the new name.

Lotus Notes Tab

The **Lotus Notes** properties tab contains settings that apply when the client is running NetBackup for Lotus Notes. The following topics explain the settings. For more information, see the *NetBackup for Lotus Notes System Administrator's Guide*.



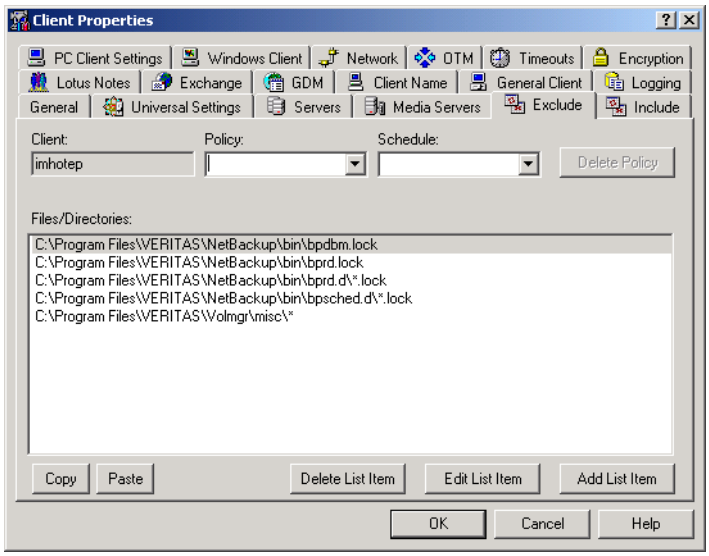
Path

Specifies the path where the Lotus Notes program files reside on the client. NetBackup must know where these files are in order to perform backup and restore operations. The value in this box overrides the one specified by the Lotus registry key, if both are defined.

.INI File

Specifies the absolute path to the `NOTES.INI` file associated with the server instance to be used to back up and restore a Lotus database. Use this setting to specify the correct `.INI` file when backing up and restoring from Domino partitioned servers. It is not necessary to specify the .INI file for non-partitioned servers.

Exclude Tab



The **Exclude** tab under **Clients** allows you to create and modify the exclude lists on Microsoft Windows clients. An exclude list names files and directories that you want to exclude from automatic backups.

The **Files/Directories** list displays the lists for clients that were selected when you opened the tab.

If multiple clients were selected, a scroll bar is present at the bottom of the list box. Move the bar to display the list for the desired client. You can modify only one list at a time.

- To add a file or directory to the list that is being displayed, click **Add List Item**.
- To modify a file or directory entry, select it in the list, click **Edit List Item**, and make the change.
- To Delete a file or directory entry, select it in the list and click the **Delete** key.

Also see “Include Tab” on page 297and “Syntax Rules for Exclude and Include Lists” on page 300

Note This tab applies only to Windows clients. On NetWare target clients, you specify the exclude and include lists when adding the targets (see the NetBackup user’s guide for the client). NetWare NonTarget, Macintosh, and OS/2 clients do not support exclude and include lists.

Client

Displays the client containing the list you are creating or modifying.

Policy

Specifies the policy (if any) to which the list applies. To display lists that already exist for specific policies, click in the box and select the policy name. If no policies are selected, the list applies to all policies.

Delete Policy

Deletes all lists for the specified policy.

Schedule

Specifies the schedule (if any) to which the list applies. To display existing lists for schedules, click in the box and select from the list. If no schedules are selected, the list applies to all schedules.

Files and Directories

Displays the lists on the clients that were selected when you opened this dialog. If multiple clients were selected, move the scroll bar at the bottom of the box to display the list for the desired client.

Copy

Copies the selected items so you can paste the items to the Include tab.

Paste

Copies the selected items so you can paste the items to the Include tab.

Delete List Item

Delete the selected item from the list by selecting the item in the list and clicking **Delete List Item**.

Edit List Item

Permits you to edit file or directory entries. To edit an entry:

1. Click **Edit List Item** to open an edit box around the selected entry.

2. Modify the path or click either the Remote file or Remote folder browse button that is at the right side of the edit box and select a path. To remove the entry, click the - button. Clicking the **Delete** key also removes the selected entry.

3. To complete the change, click **Apply** (or click outside the edit box). Clicking another tab also changes the entry.

Add List Item

Specifies directories or files to add to the lists on the selected client. To add a directory or file:

1. Click **Add List Item** to open an edit box where you can specify a path.

2. Type the path in the edit box or click the Remote file or Remote folder browse button that is at the right side of the edit box and select a path.

3. To complete the addition, click **Apply** (or click outside the edit box). Clicking another tab also adds the entry.

You can also select files or directories in Explorer and drag them to the list.

Include Tab

The **Include** tab under **Clients** allows you to create and modify the include lists on Microsoft Windows clients. An include list adds back in files or folders that were excluded by the exclude list. This is useful, for example, if you want to exclude all files in a directory but one.

The **Files/Directories** box displays the lists for UNIX and Microsoft Windows clients that were selected when you opened the dialog. If multiple clients were selected, a scroll bar is present at the bottom of the list box. Move the bar to display the list for the desired client (you can modify only one list at a time).

- To add a file or directory to the list that is being displayed, click **Add List Item**.
- To modify a file or directory entry, select it in the list, click **Add List Item**, and make the change.
- To Delete a file or directory entry, select it in the list and click the **Delete** key.

Also see “Exclude Tab” on page 295 and “Syntax Rules for Exclude and Include Lists” on page 300.

Note The **Include** properties do not apply to NetWare, Macintosh, and OS/2 clients. On NetWare target clients, you specify exclude and include lists when adding the targets (see the NetBackup user's guide for the client). NetWare NonTarget, Macintosh, and OS/2 clients do not support exclude and include lists. For UNIX clients, see the *NetBackup System Administrator's Guide for UNIX*.

Files/Directories

Displays the include lists on the clients that were selected when you opened this dialog. If multiple clients were selected, move the scroll bar at the bottom of the box to display the list for the desired client.

Copy

Copies the selected items so you can paste them to the Exclude tab.

Paste

Copies the selected items so you can paste them to the Exclude tab.

Add List Item

Same as on **Exclude** tab.

Edit List Item

Same as on **Exclude** tab.

Permits you to edit file or directory entries. See **Edit List Item** under **Exclude Tab**.

Exclude and Include Lists for Specific Policies or Schedules

▼ **To create an exclude or include list for a specific policy**

Assume you want to create a list that affects all scheduled backups in an existing policy named nt_wkstations for the client selected in the **Client**.

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Host Properties** > **Clients**.

2. Open the Properties dialog for the selected client. Click the Exclude or Include tab.

3. In the **Policy** box, select **`nt_wkstations`**.

4. Click **Add List Item** to add files and directories to the exclude list or the include list.

5. Click **OK**.

▼ To create an exclude or include list for a specific policy and schedule

Assume you want to create a list that affects all scheduled backups for the schedule named weekly_fulls in the policy named nt_wkstations for the client selected in the **Client** box.

1. In the **Policy** box, select **`nt_wkstations`**.

2. In the **Schedule** box, select **`weekly_fulls`**.

3. Click **Add List Item** to add files and directories to the exclude list or the include list.

4. Click **OK**.

Which List is Used If there is More Than One?

If there is more than one exclude or include list for a client, NetBackup uses only the most specific one. For example, assume a client has three exclude lists:

- An exclude list for a policy and schedule.
- An exclude list for a policy.
- An exclude list for the entire client. This list does not specify a policy or schedule.

In this example, NetBackup uses the first exclude list (for policy and schedule) because it is the most specific.

Syntax Rules for Exclude and Include Lists

Note VERITAS suggests that you always specify automounted directories and CD-ROM file systems in the exclude list. Otherwise, if the directories are not mounted at the time of a backup, NetBackup must wait for a timeout before proceeding.

The following syntax rules apply to exclude lists:

- Only one pattern per line is allowed.
- The following special or wildcard characters are recognized:

  ```
  [ ]
  ?
  *
  ```

- To use special or wildcard characters literally (that is, as nonwildcard characters), precede them with a backslash (`\`). For example, assume the brackets in the following are to be used literally

  `C:\abc\fun[ny]name`

  In the exclude list, precede them with a backslash as in

  `C:\abc\fun\[ny\]name`

Note A backslash (`\`) acts as an escape character only when it precedes a special or wildcard character as in the above example. This means that NetBackup normally interprets a backslash literally and it is a legal character to use in pathnames.

- Spaces are considered legal characters. Do not include extra spaces unless they are part of the file name.

  For example, if you want to exclude a file named

  `C:\testfile` (with no extra space character at the end)

  and your exclude list entry is

  `C:\testfile` (with an extra space character at the end)

  NetBackup cannot find the file until you delete the extra space from the end of the file name.

- End a file path with `\` to exclude only directories with that path name (for example, `C:\users\test\`). If the pattern does not end in `\` (for example, `C:\users\test`), NetBackup excludes both files and directories with that path name.
- To exclude all files with a given name, regardless of their directory path, just enter the name. For example:

  `test`

rather than

```
C:\test
```

This is equivalent to prefixing the file pattern with

```
\
\*\
\*\*\
\*\*\*\
```

and so on.

The following syntax rules apply only to UNIX clients:

- Do not use patterns with links in the names. For example, assume `/home` is a link to `/usr/home` and `/home/doc` is in the exclude list. The file is still backed up in this case because the actual directory path, `/usr/home/doc`, does not match the exclude list entry, `/home/doc`.
- Blank lines or lines beginning with a pound sign (#) are ignored.

Windows Client Example Exclude List

Assume that an exclude list contains the following entries:

```
C:\users\doe\john
C:\users\doe\abc\
C:\users\*\test
C:\*\temp
core
```

Given the example exclude list, the following files or directories would be excluded from automatic backups:

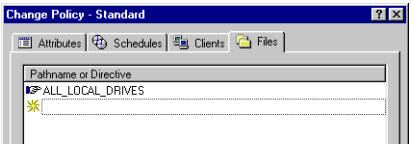
- The file or directory named `C:\users\doe\john`.
- The directory `C:\users\doe\abc\` (because the exclude entry ends with `\`).
- All files or directories named `test` that are two levels below users on drive C.
- All files or directories named `temp` that are two levels below the root directory on drive C.
- All files or directories named `core` at any level and on any drive.

Traversing Excluded Directories

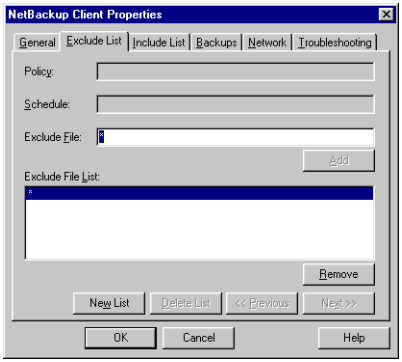
If the exclude list for a client indicates a directory for exclusion, but the client uses an include list to override the exclude list, NetBackup will traverse the excluded directories if necessary, in order to satisfy the client's include list.

Assume the following settings for a Windows client named silk:

- The backup policy file list for silk indicates `ALL_LOCAL_DRIVES`. When a scheduled backup runs, the entire client is backed up. The entire client would also be backed up if the file list consisted of only:
  `/`



- The exclude list on the client consists of only:
  `*`
  This indicates that all files will be excluded from the backup.

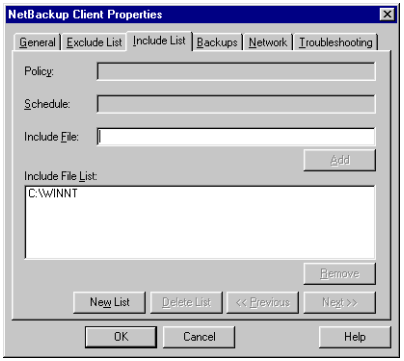


- However, since the include list on Windows client silk includes the following file:

  `C:\WINNT`

  the excluded directories are traversed in order to back up `C:\WINNT`.

  If the include list did not contain any entry, no directories would be traversed.



In another example, assume the following settings for a UNIX client named hagar:

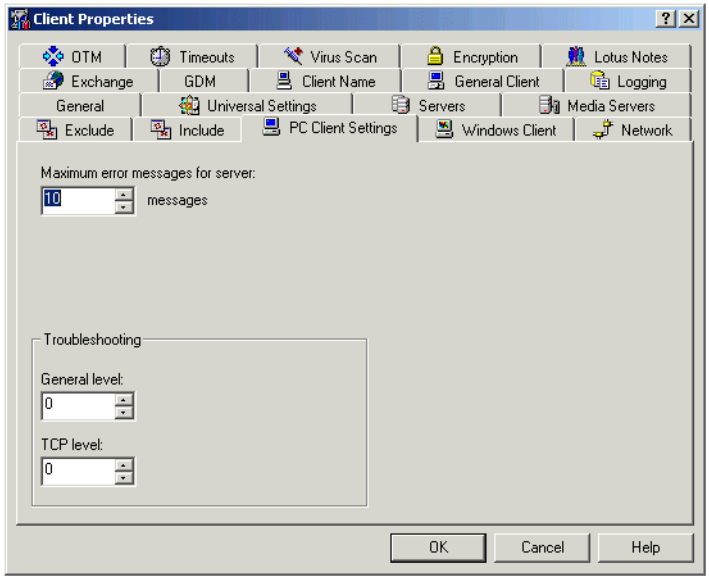
- The file list for client hagar consists of the following: `/`
- The exclude list for UNIX client hagar consists of the following: `/`
- UNIX client hagar's include list consists of the following directories:

  ```
  /data1
  /data2
  /data3
  ```

In both examples, because the include list specifies full paths and the exclude list excludes everything, NetBackup will replace the file list with the client's include list.

PC Client Settings Tab

The **PC Client Settings** tab under **Clients** defines how NetBackup logs repetitive error messages on PC clients.



Maximum Error Messages for Server

Defines the maximum number of times to send repetitive error messages to the NetBackup server from the NetBackup client. For example, if the archive bits cannot be reset on some files, this setting limits the number of times the message appears in the logs on the server. A value of 0 indicates unlimited. Default: 10.

General Level Troubleshooting

Applies to Microsoft Windows clients and controls the amount of information that NetBackup writes to the `BPCD` logs. Supported values are 0, 1, or 2. The higher the level, the more information is written. Default: 0.

Troubleshooting - TCP Level

Applies to Microsoft Windows clients and enables TCP debugging. To change this value, select the check box and enter the new value in the text field. Supported values are:

0 No extra logging (default).

1 Log basic TCP / IP functions.

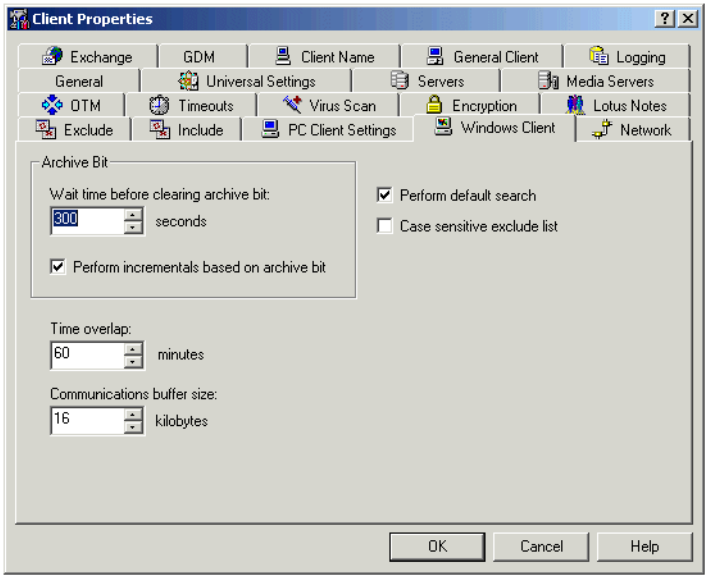
2 Log all TCP / IP functions, including all read and write requests.

3 Log contents of each read / write buffer.

Note Setting Debug TCP Level to 2 or 3 can cause the status reports to be very large. It can also slow a backup or restore operation.

Windows Client Tab

The **Windows Client** tab under **Clients** defines NetBackup properties for Microsoft Windows clients.



Wait Time Before Clearing Archive Bit

Specifies the number of seconds for the client to wait before clearing the archive bits for a differential incremental backup. The minimum allowable value is 300 (default). The client waits this long for acknowledgment from the server that the backup was successful. If the server does not reply within this time period, the archive bits are not cleared.

This option applies only to differential-incremental backups. Cumulative-incremental backups do not clear the archive bit.

Perform Incrementals Based on Archive Bit

Specifies that NetBackup will include files in an incremental backup only if their archive bit is set. The system sets this bit whenever a file is changed and it normally remains set until NetBackup clears it.

A full backup always clears the archive bit. A differential-incremental backup clears the archive bit if the file is successfully backed up within the number of seconds indicated by **Wait Time Before Clearing Archive Bits**. A cumulative-incremental or user backup has no effect on the archive bit.

Clear this check box to have NetBackup include a file in an incremental backup only if the datetime stamp for the file has been changed since the last backup. For a differential-incremental backup, NetBackup compares the datetime stamp to the last full or incremental backup. For a cumulative-incremental backup, NetBackup compares the timestamp to the last full backup.

If you install or copy files from another computer, the new files retain the datetime stamp of the originals. If the original date is before the last backup date on this computer, then the new files are not backed up until the next full backup.

Time Overlap

Applies to Microsoft Windows clients and specifies the number of minutes to add to the date range for incremental backups when using date-based backups. This value compensates for differences in the speed of the clock between the NetBackup client and server. Default: 60 minutes.

Communications Buffer Size

Applies to Microsoft Windows clients and specifies the size (in kilobytes) of the TCP/IP buffers used to transfer data between the NetBackup server and client. For example, specify 10 for a buffer size of 10 kilobytes. The minimum allowable value is 2. If you specify a number less than 2, buffer size is set to 2. There is no maximum allowable value. Default: 32 kilobytes.

Perform Default Search for Restore

Applies to Microsoft Windows clients. Selecting this option causes NetBackup to automatically search the default range of backup images and display the backed up folders and files whenever a restore window is opened.

Clear this box to disable the initial search. The NetBackup Restore window will then not display any files or folders when initially opened. Clicking a backup image, or selecting a range of backup images, starts a search. Default: option is selected.

Case Sensitive Exclude List

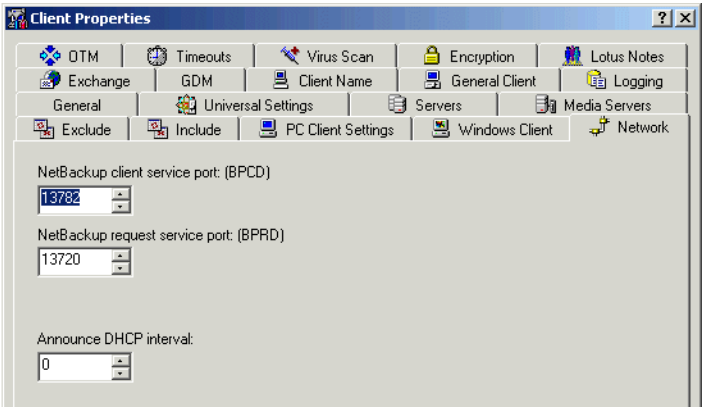
Applies to Microsoft Windows clients and makes the exclude list case sensitive. Clear the box to make the lists not case sensitive (default). Using case-sensitive exclude lists can improve performance.

Case sensitive means that when comparing the contents of the exclude file to the files that are being backed up, a match occurs only when the capitalization is the same. For example, *Cat* matches *Cat* but not *cat*.

Not case-sensitive means capitalization is not considered when comparing names. For example, *Cat* matches *cat*.

Network Tab

The **Network** tab under **Clients** contains settings which define requirements for communications between clients and the master server.



NetBackup Client Service Port (BPCD)

Applies to Microsoft Windows clients and specifies the port that the NetBackup client uses to communicate with the NetBackup server. Default: 13782.

Note If you change this port number, remember that it must be the same for all NetBackup servers and clients that communicate with one another.

NetBackup Request Service Port (BPRD)

Applies to Microsoft Windows clients and specifies the port for the client to use when sending requests to the NetBackup request service (`bprd` process) on the NetBackup server. Default: 13720.

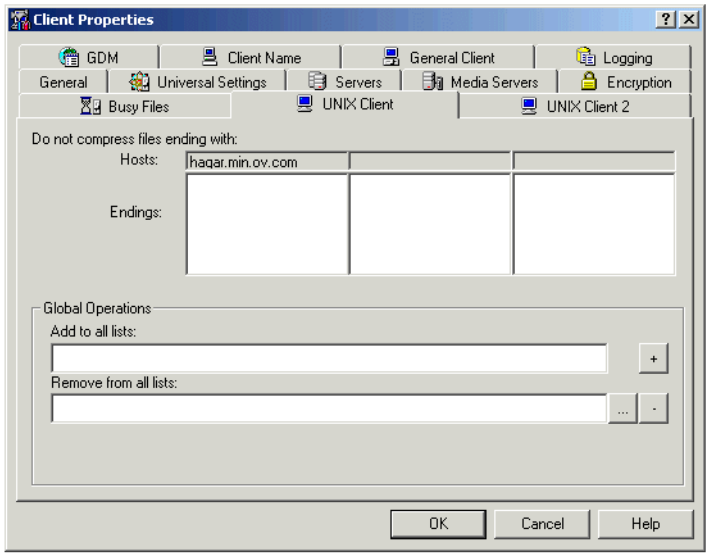
Note If you change this port number, remember that it must be the same for all NetBackup servers and clients that communicate with one another.

Announce DHCP Interval

Applies to Microsoft Windows clients and specifies how many minutes the client waits before announcing that it is using a different IP address. The announcement occurs only if the time period has elapsed and the address has changed since the last time the client announced it. Default: 0 (no announcement).

Client Settings Tab (UNIX)

The **Client Settings** dialog under **Clients** defines NetBackup properties for UNIX clients.



Do Not Compress Files Ending With

Specifies a list of file extensions. During a backup, NetBackup does not compress files with these extensions because the file can already be in a compressed format.

You cannot use wildcards when specifying these extensions. For example, you can specify `.A1` but not `.A*` or `.A[1-9]`

Files that are already compressed become slightly larger if compressed again. On UNIX clients, if this type of file exists and it has a unique file extension, exclude it (and others with the same extension) from compression by adding it to this list.

Add to All Lists

Specify the file endings that you do not want to compress and add the endings to the lists. To add a file ending, type it in the box, then click the + button. Use commas or spaces to separate file endings.

Remove from All Lists

Specify the file endings that you want to remove from the lists. To remove a name, either type it in the box or click the browse button (...) and select a file ending. Use commas or spaces to separate names. Then, click the – button.

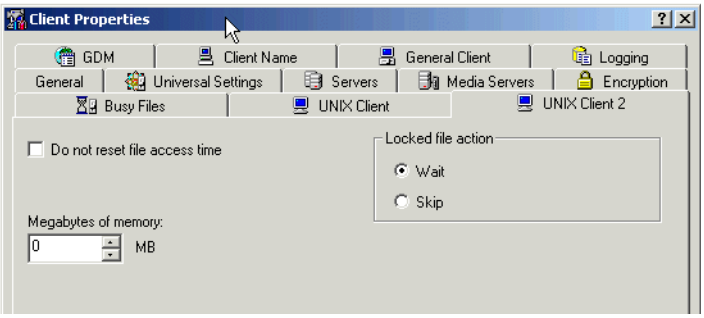
Frozen Image Configuration

The **Frozen Image Configuration** button appears if the Core Frozen Images license is installed. The **Frozen Image Configuration** button allows configuration of Frozen Image Methods that can be used when backing up a client. (See “Allow Frozen Image Clients” on page 64.)

Note On Windows, the NetBackup Administration Console and the Remote Administration Console are not supported for configuring ServerFree Agent features or for running backups that were configured with ServerFree Agent.

UNIX Client2 Tab

The **UNIX Client2** tab under **Clients** defines NetBackup properties for UNIX clients.



Do Not Reset File Access Time

Specifies that if a file is backed up, its access time (`atime`) will display the time of the backup. By default, NetBackup preserves the access time by resetting it to the value it had before the backup.

Note This setting affects software and administration scripts that examine a file's access time. DO NOT use this option or `USE_CTIME_FOR_INCREMENTALS` if you are running Storage Migrator on the system. Setting these options causes the `atime` for files to be updated every time they are backed up. This makes it appear as if the files are frequently used and stops Storage Migrator from selecting them for migration.

Megabytes of Memory

Note This option has a reasonable default and has to be changed only if problems are encountered.

Specifies how much memory is available on the client to use when compressing files during backup. If you select compression, the client software uses this value to determine how much space to request for the compression tables. The more memory that is available to the compress code, the greater the compression and the greater the percentage of machine resources used. If other processes also need memory, it is generally best to use a maximum value of 1/2 the actual physical memory on a machine to avoid excessive swapping.

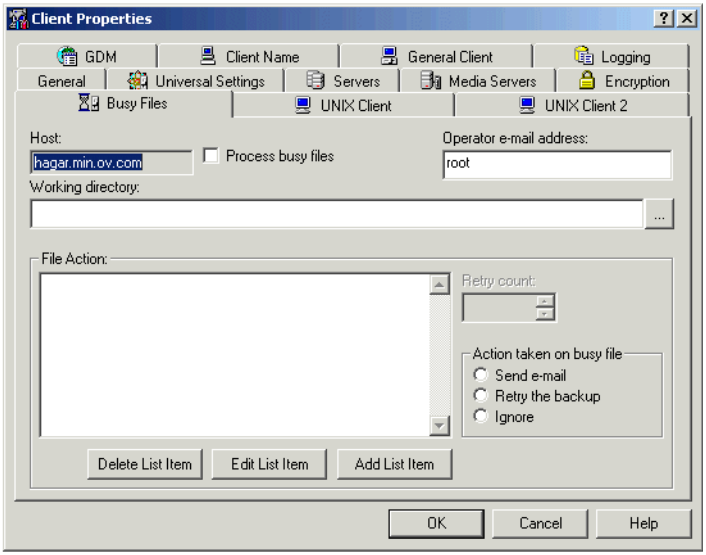
Locked File Action

Specifies the behavior of NetBackup when it tries to back up a file that has mandatory file locking enabled in its file mode.

- **Wait:** By default, NetBackup waits for files to become unlocked.
- **Skip:** NetBackup skips files that currently have mandatory locking set by another process and logs a message to this effect.

Busy File Settings

The **Busy Files** tab under **Clients** defines what occurs when NetBackup encounters a busy file during a backup of a UNIX client.



Host

Displays the current host.

Working Directory

Specifies the path to the busy-files working directory.

On a UNIX client, the value in the user's `$HOME/bp.conf` file takes precedence if it exists. By default, NetBackup creates the `busy_files` directory in the `/usr/openv/netbackup` directory.

Operator's E-mail Address

Specifies the recipient of the busy-file notification message when the action is set to **Send e-mail**. By default, the mail recipient is the administrator.

On a UNIX client, the value in the user's `$HOME/bp.conf` file takes precedence if it exists. By default, BUSY_FILE_NOTIFY_USER is not in any `bp.conf file` and the mail recipient is `root`.

Process Busy Files

Causes NetBackup to process busy files according to the settings on this tab, if it determines that a file is changing while it is being backed up. By default, this is not selected and NetBackup does not process the busy files.

File Action File List

Specifies the absolute pathname and file name of the busy file. The metacharacters `*`, `?`, `[]`, `[ - ]` can be used for pattern matching of filenames or parts of filenames.

Action Taken On Busy File

Directs the action that NetBackup performs on busy files when busy-file processing is enabled by selecting **Process Busy Files** on this tab. On a UNIX client, the value in the user's `$HOME/bp.conf` file takes precedence if it exists.

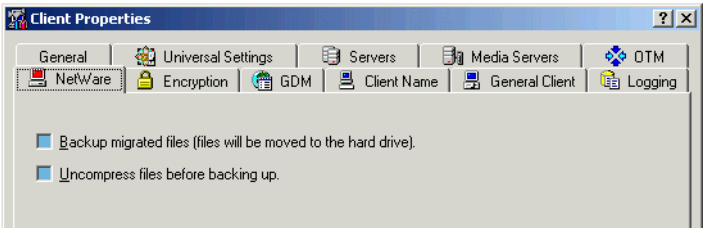
- **Send e-mail:** Directs NetBackup to mail a busy file notification message to the user specified in the **Operator's E-mail Address** field in this tab.
- **Retry the Backup:** Directs NetBackup to retry the backup on the specified busy file. The number of times NetBackup will attempt the backup is determined by the **Retry Count** value.
- **Ignore:** Directs NetBackup to exclude the busy file from busy file processing. The file will be backed up and a log entry indicating that it was busy will appear in the All Log Entries report.

Retry Count

Specifies the number of times to attempt the backup. Default retry count: 1.

NetWare Tab

The **NetWare** tab is available under **Clients** only when NetBackup client software for NetWare is installed on the client.



Backup Migrated Files (Files will be Moved to the Hard Drive)

Specifies that files that have been moved to secondary storage will be moved back to primary storage and backed up by NetBackup. If the option is not selected (default), only the metadata for the file is backed up and the file is not moved back to primary storage. The metadata, in this case, is the information that is still in primary storage that marks where the file would be and any information needed to retrieve the file from secondary storage.

Uncompress Files Before Backing Up

Specifies that compressed files will be uncompressed before backing up. This is useful if the file will be restored to a version of NetWare that does not support compression. If the option is not selected (default), the file will be backed up in its compressed state.

Managing NetBackup 8

This chapter contains the following topics related to the administration and management of NetBackup:

- Powering Down and Rebooting NetBackup Servers
- Managing NetBackup Services
- Administering NetBackup Licenses
- Administering a Remote Master Server
- Managing Client Restores
- Configuring NetBackup Ports
- Load Balancing

Powering Down and Rebooting NetBackup Servers

▼ **To power down a server**

1. In the NetBackup Administration Console, click **Activity Monitor**, then select the Jobs tab to make sure no backups or restores are running.

2. Stop the NetBackup services using the NetBackup Administration Console or the command line:

   From the NetBackup Administration Console:

   a. Click **Activity Monitor**, then select the Services tab.

   b. Right-click services that are running and select **Stop Service**.

   From the command line, run:

   install_path`\NetBackup\bin\bpdown.exe`

▼ **To reboot a NetBackup master server**

1. Restart the system.

2. If the required NetBackup services are not set up to start automatically:

   a. Start the NetBackup Client service.

   b. Start the NetBackup Device Manager service. This automatically starts the NetBackup Volume Manager service.

   c. Start the NetBackup Request Manager service to start the NetBackup Database Manager service.

Managing NetBackup Services

To start and stop the individual NetBackup services, use the Services tab in the NetBackup Activity Monitor window or the Services application in the Windows Control Panel. VERITAS suggests that you set up the NetBackup services so they start automatically each time you boot the system.

You can also start or stop all the NetBackup services at once as follows:

- To start all NetBackup services, run:

  install_path`\NetBackup\bin\bpup.exe`

- To stop all NetBackup services and any robotic control processes that are running, run:

  install_path`\NetBackup\bin\bpdown.exe`

NetBackup Request Manager Service

The NetBackup Request Manager service (`bprd.exe`) runs on the master server. This service starts the NetBackup scheduler and receives requests from clients. The NetBackup Request Manager service must be running in order to perform any backups or restores.

NetBackup Database Manager Service

The NetBackup Database Manager service (`bpdbm.exe`) manages the NetBackup internal databases and catalogs. The DataBase Manager service must be running on the master server during all NetBackup administrative operations, including when modifying a backup policy.

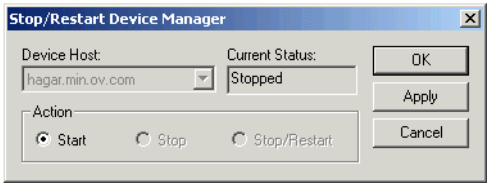
NetBackup Device Manager Service

The NetBackup Device Manager service (`ltid.exe`) starts the robotic control processes and controls the reservation and assignment of volumes. When there is a request for a volume, the NetBackup Volume Manager service finds the volume and the NetBackup Device Manager has the robot mount it. If the desired volume is not available, a mount request appears in the **Device Monitor**.

In addition to using the Activity Monitor and Windows NT/2000 Control Panel, you can start and stop this service by doing the following:

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

2. Click **Actions** > **Stop/Restart Device Manager Service**. The Start/Restart Device Manager dialog appears containing options for starting, stopping, or stopping and restarting the service on a selected host.



The Activity Monitor cannot control daemons on a UNIX system. However, you can use the above Device Monitor and Media and Device Management commands to start and stop the Media Manager Device daemon (`ltid`) on a UNIX NetBackup server.

NetBackup Volume Manager Service

The NetBackup Volume Manager service (`vmd.exe`) finds volumes when NetBackup needs them for a backup or restore. For example, if a volume is in a robot, the NetBackup Volume Manager service informs the NetBackup Device Manager service so the volume can be mounted.

NetBackup Client Service

The NetBackup Client service (`bpinetd.exe`) listens for connections from NetBackup servers in the network and when an authorized connection is made, starts the necessary NetBackup process to service the connection.

Administering NetBackup Licenses

The license key for each computer is initially entered when the software is installed. At some point you may need to modify the licensing, for example, when changing to a different level of NetBackup or adding separately-priced options.

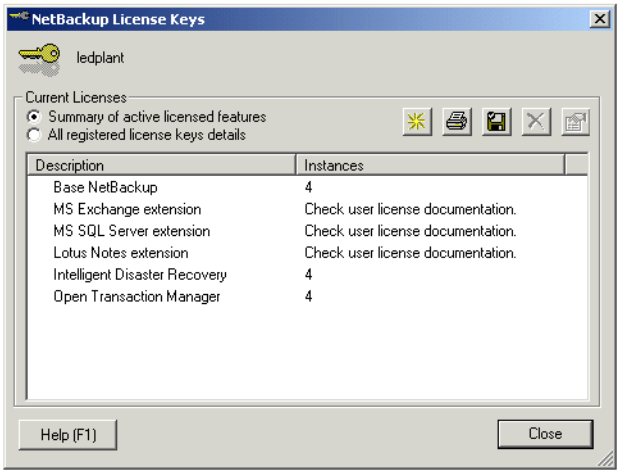
▼ To access license keys for a NetBackup server

1. Select a server:

   a. To view the license keys of the current server:
   In the NetBackup Administration Console, click **Help** > **License Keys**. The NetBackup License Keys dialog appears.

   b. To view the license keys of another server:

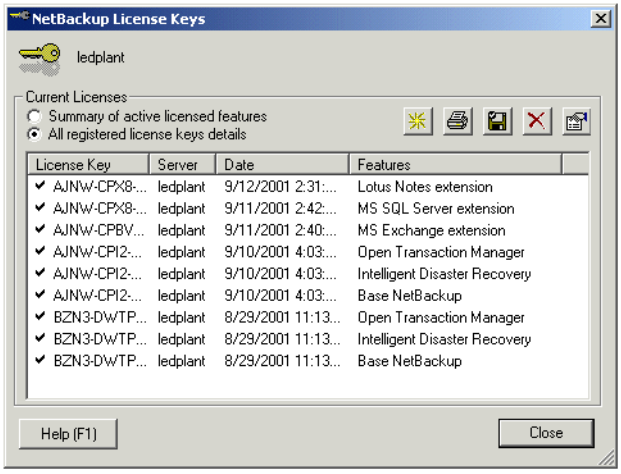
   Click **File** > **Change Server**, then select another server. Click **Help** > **License Keys**.



2. Choose to display either a summary listing or the details for each license key:

   - Select **Summary of active licensed features** to show a summary of the active features that are licensed on this server. This view lists each feature and how many instances of it are permitted.

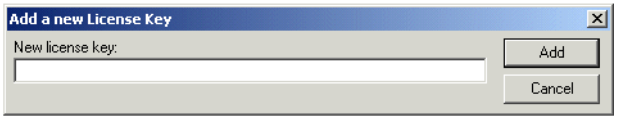
   - Select **All registered license keys details** to show the details of the license keys registered on this server. This view lists each license key, the server where it is registered, when it was registered, and the features that it provides, and whether the feature is active or inactive.



3. From the NetBackup License Keys dialog, you can:
   - Add a new license
   - Print a license
   - Delete a license
   - View the properties of one license
   - Export the license listing

▼ To add a new license key

1. In the NetBackup License Keys dialog, click the **New** button. The Add a New License Key dialog appears.



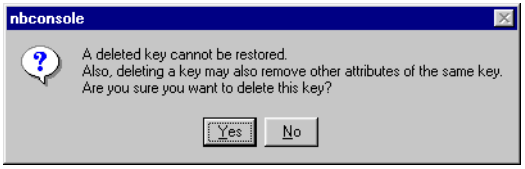
2. Enter the license key and click **Add**. The new license key appears in the list.

▼ To print a license key list

1. In the NetBackup License Keys dialog, select the license key you wish to print from the list.
2. In the NetBackup License Keys dialog, click the **Print** button. The Print dialog appears.
3. Make your print selections and click **OK**.

▼ To delete a license key

1. Select the license key you wish to delete from the license key list. If the key has more than one feature, all the features are listed in the dialog.
2. In the NetBackup License Keys dialog, click the **Delete** button. A confirmation dialog appears stating that the license key cannot be restored once it is deleted.

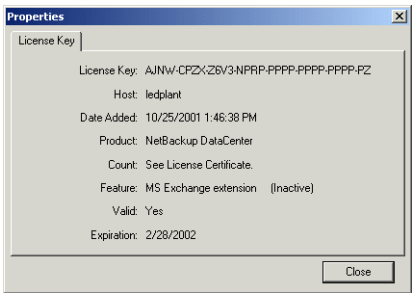


3. Click **OK** to delete the key and all features associated with the key.

   If the key appears more than once in the list, deleting one instance also deletes all other instances of the key from the list.

▼ To view the properties of one license key

In the NetBackup License Keys dialog, select one license and click the **Properties** button.



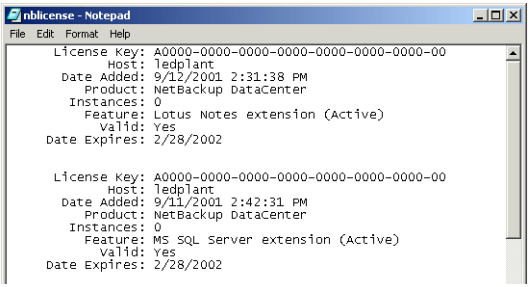
▼ To export the license keys

1. In the NetBackup License Keys dialog, click the **Export** button.
   The **Save As** dialog appears.

2. Select the directory and type a file name where you'd like the key properties of all licenses to be exported.

   The file contains a list of each license key, along with the:

   - Name of the host
   - Date the license was added
   - Name of the product
   - Number of instances
   - Name of the feature
   - Whether or not the license is valid
   - Expiration date for the license



Administering a Remote Master Server

If your site has more than one NetBackup master server, you can configure the systems so multiple servers can be accessed from one NetBackup Administrator Console.

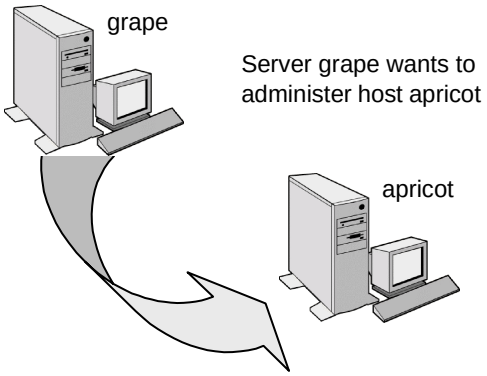
In order to access remote servers:

- First, make the remote server accessible to the local server. See the following section, "Adding a NetBackup Server to a Server List."
- Second, use **File** > **Change Server** to access the remote server.

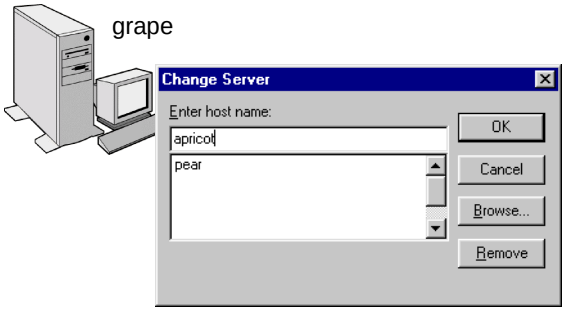
Adding a NetBackup Server to a Server List

In order for a local host to administer a remote server, the name of the local host must appear in the server list of the remote server.

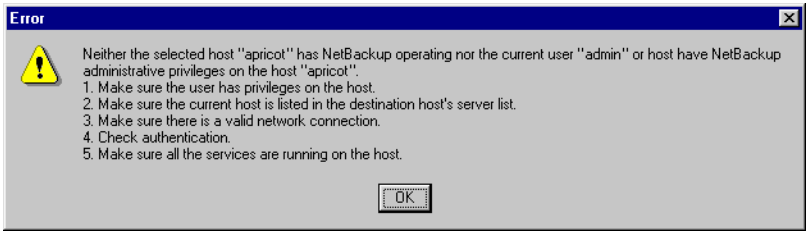
For example, assume Windows server grape wants to remotely administer Windows host apricot.



Grape selects **File** > **Change Server** and types apricot as the host name.



If grape is not listed on apricot's server list, grape receives an error message after trying to change servers to apricot.



Assuming apricot is a valid NetBackup server, the message that appears may indicate that grape is considered invalid because it does not appear in the apricot's server list.

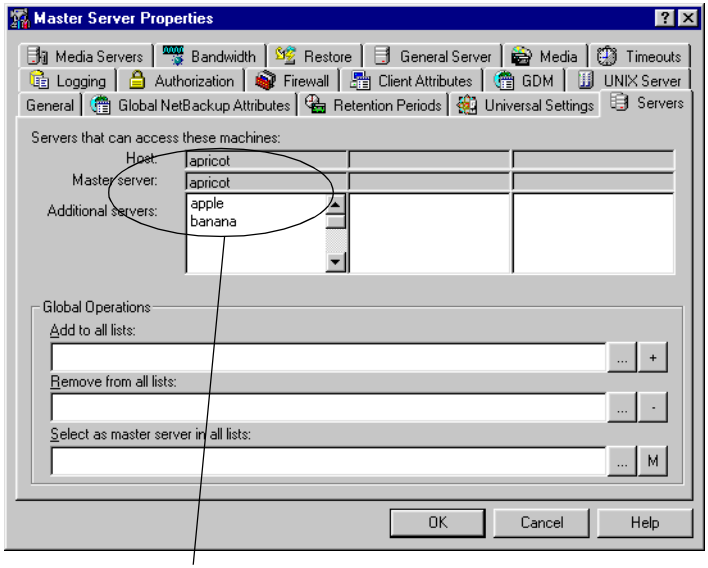
To add grape to apricot's server list, follow the steps in "To add a server to a Windows server list" on page 321. For other reasons why a remote server may be inaccessible, see "If You Cannot Access a Remote Server" on page 323.

Note This section also addresses the case of a Remote Administration Console seeking access to a remote server. Every server being administered remotely must have the name of the machine running the Remote Administration Console in its server list.

▼ To add a server to a Windows server list

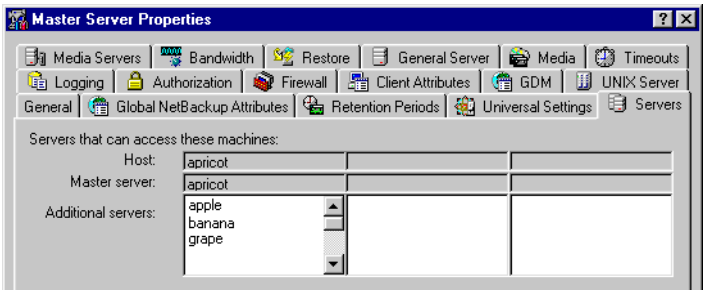
1. Go to the destination host (apricot) and start the NetBackup Administration Console.
2. Expand **Master Server** > **NetBackup Host Properties** > **Master Server**.
3. Double-click the server name (apricot) to view the properties.
4. Select the **Servers** tab to display the server list.

   The server list contains, as the dialog explains, "Servers that can access these machines." Since the server list does not include server grape, apricot considers grape to be an invalid server.
5. To add a server to the server list, type the server name (grape) in the field labeled **Add to All Lists**.



Currently, apricot allows remote access by two additional servers: apple and banana

6. Click the **+** button next to the **Add to All Lists** field. The server name appears in the server list.



Apricot now includes grape among the servers to which it allows remote access

7. As when changing any NetBackup property through the Host Properties dialogs, restart all services on the server where the change was made to ensure that the new configuration values are used. Restart the NetBackup Administration Console, as well.

▼ To add a server to a UNIX server list

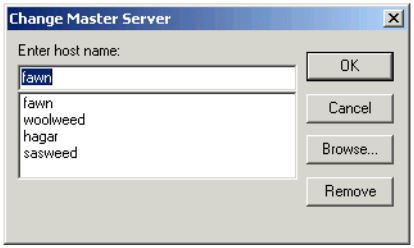
1. Go to the destination host and start the NetBackup Administration Console (`jnbSA`).
2. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Host Properties** > **Master Servers**.
3. Double-click the server name to view the properties.
4. Select **Servers** to display the server list.
5. To add a server to the server list, click **New** next to the **Additional Servers** list.
6. Type the server name and click **OK**. The server name appears in the server list.
7. Restart all daemons and utilities on the server where the change was made to ensure that the new configuration values are used. Restart the NetBackup Administration Console, as well.

Note The `bp.conf` file on every UNIX server contains `SERVER` and possibly `MEDIA_SERVER` entries. The server list in the properties dialog represents these entries. Hosts listed as media servers have limited administrative privileges.

Choosing a Remote Server to Administer

▼ **To use the Change Server command to administer a remote server**

1. Select **File** > **Change Server**.
2. Type or select the host name and click **OK**.



If You Cannot Access a Remote Server

In order to administer a server from another master server or the NetBackup Remote Adminstration Console, make sure that the following conditions are true:

- The destination server is operational.
- NetBackup services are running on both hosts.
- There is a valid network connection.
- The user has administrative privileges on the host.
- The current host is listed in the destination host's server list as explained in "Adding a NetBackup Server to a Server List" on page 320.This is not required for a media server, client, media and device management, or device monitoring.

  To ensure that the new server entry is used by all NetBackup processes that require it, stop and restart:

  - The NetBackup Database Manager and NetBackup Request Manager services on the remote server if it is Windows.
  - The NetBackup Database Manager (`bpdbm`) and NetBackup Request Manager (`bprd`) on the remote server if it is UNIX.
- Authentication is set up correctly, if used.
- If you have problems changing servers when configuring media or devices or monitoring devices:
  - If the remote server is Windows, verify that the NetBackup Volume Manager service is running on that server and start it if necessary.
  - If the remote server is UNIX, verify that the Media Manager Volume daemon is running on that server and start it if necessary.

- If you cannot access devices on the remote host, it may be necessary to add a `SERVER` entry to the `vm.conf` file on that host. See the *Media Manager System Administrator's Guide* for instructions.
- If you cannot start or stop processes or services through the Activity Monitor, verify the following:
  - The remote server is a Windows system. It is possible to monitor and control processes only on another Windows system.
  - You have the required permissions on the other server. Windows security must allow access to the user that is running the Activity Monitor.

Using the Remote Administration Console

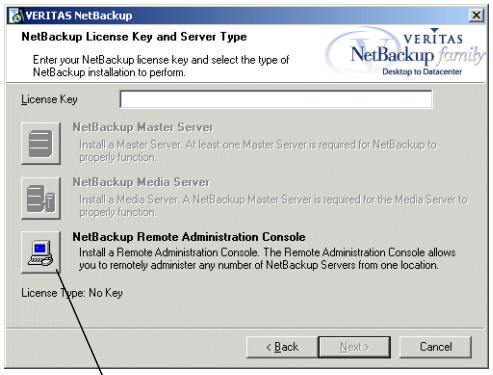
You can install the Remote Administration Console on a Windows machine to fully administer or manage any remote NetBackup server—Windows or UNIX. No license is required to install the Remote Administration Console.

Upon installation, the Administration Console and the client software is installed. No NetBackup master or media server software is installed. The presence of the client software enables the machine to be backed up like any other client.

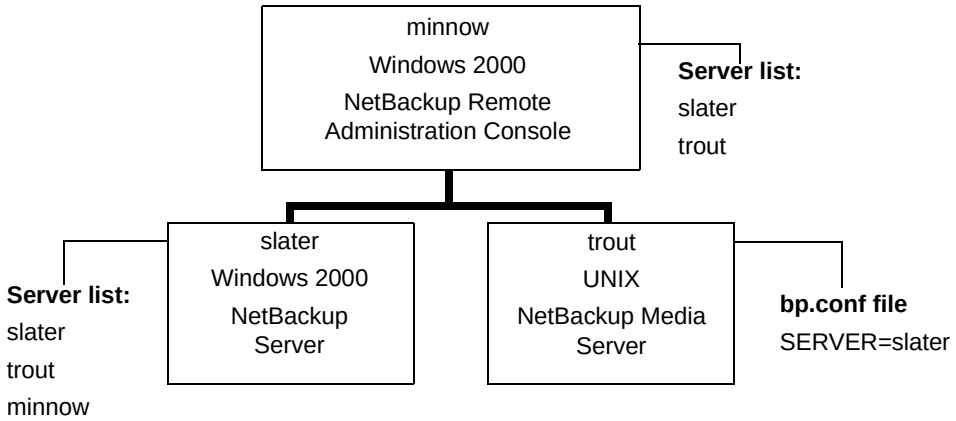
In the following figure, the administrator can use the Remote Administration Console on minnow to add a comment for a drive in the configuration on the server trout.

The administrator can manage NetBackup on slater or trout from any of the systems shown.

minnow must be listed in the server list on slater but does not need to be listed on trout because trout is a media server.



Installing the Remote Administration Console installs the administration console and client software, but no server software



To add a server to a server list, follow the steps in “To add a server to a Windows server list” on page 321 or “To add a server to a UNIX server list” on page 322.

After starting the Remote Administration Console, change to a NetBackup server by clicking **File** > **Change Server** as described in “Choosing a Remote Server to Administer” on page 323.

Managing Client Restores

The topics in this section cover the following aspects of managing restores for NetBackup clients.

- "Server-Directed Restores"
- "Allowing Redirected Restores"
- "Improve Search Times by Creating an Image List"

A related topic is "Rules for Using Host Names in NetBackup" on page 630. Incorrectly specified host names are often a factor in file restore problems.

Server-Directed Restores

An administrator can use the Backup, Archive, and Restore interface on the NetBackup master server to direct restores to any client, providing NetBackup on the client is configured to permit them. See NetBackup UNIX or Windows NT/2000 user's guide for more information.

Allowing Redirected Restores

The Backup, Archive and Restore client interface contains options for restoring files that were backed up by other clients. The operation is called a *redirected restore*.

A client can restore files belonging to other clients only with the necessary configuration on the NetBackup master server. Create the following directory on the master server:

install_path`\NetBackup\db\altnames`

Add files to it as explained in this section. To undo the changes, remove the `altnames` directory and its files.

Caution The *install_path*`\NetBackup\db\altnames` directory can present a potential breach of security: If users permitted to select and restore files from other clients also have permission to locally create the files found in the backup.

How NetBackup Enforces Restore Restrictions

By default, NetBackup permits restores only by the client that backs up the files. NetBackup enforces this restriction by ensuring that the name specified by the NetBackup client name setting on the requesting client matches the peer name used in the connection to the NetBackup server.

Where:

The NetBackup client name is normally the client's short host name, such as `mercury` rather than a longer form such as `mercury.null.com`.

- On Microsoft Windows clients (includes NetWare NonTarget), specify the client name in the Specify NetBackup Machines dialog. To display this dialog, start the Backup, Archive, and Restore interface on the client and select click **File** > **Specify NetBackup Machines**.
- On NetWare target clients, specify the client name in the `bp.ini` file.
- On Macintosh and UNIX clients, specify the client name in the user interface.

peer name is the name that the client uses when it connects to the NetBackup server during the file restore request. Unless clients share an IP address due to the use of a gateway and token ring combination, or have multiple connections, the *peer name* is equivalent to the client's *host name*. When a client connects through a gateway, the gateway can use its own *peer name* to make the connection.

Note Do not add a suffix to the files created in the `altnames` directory.

Allowing All Clients to Perform Redirected Restores

The administrator can allow all clients to restore backups belonging to other clients by creating the following empty file on the NetBackup master server:

install_path`\NetBackup\db\altnames\No.Restrictions`

When this file exists on the master server, clients can access backups belonging to other clients if the NetBackup client name setting on the requesting client matches the name of the client for which the backup was created. The peer name of the requesting client does not have to match the NetBackup client name setting.

Example

Assume Windows 2000 client freddie wants to restore a file that was backed up by client oscar:

1. The administrator creates the following file on the NetBackup master server:

   install_path`\NetBackup\db\altnames\No.Restrictions`

2. The user starts the Backup, Archive, and Restore application (`jbpSA`) and specifies **`freddie`** in the login dialog.

3. The user changes the NetBackup source client name setting in the Backup, Archive, and Restore user interface to **`oscar`**.

4. Client freddie restores the file backed up by client oscar.

Allowing a Single Client to Perform Redirected Restores

The administrator can give a single client permission to restore backups belonging to other clients by creating an empty file on the NetBackup master server:

install_path`\NetBackup\db\altnames\`*peername*

Where *peername* is the client that is to possess restore privileges.

In this case, the client named by *peername* can access files backed up by another client if the NetBackup client name setting on the client named peername matches the name of the other client.

Example

Assume Windows 2000 client freddie wants to restore files that were backed up by client oscar:

1. The administrator creates the following file on the NetBackup master server:

   install_path`\NetBackup\db\altnames\freddie`

2. The user starts the Backup, Archive, and Restore application (`jbpSA`) and specifies **`freddie`** in the login dialog.

3. The user changes the NetBackup source client name setting in the Backup, Archive, and Restore user interface to **`oscar`**.

4. Client freddie restores the files backed up by client oscar.

Allowing Redirected Restores of Specific Client's Files

The administrator can give a single client permission to restore backups belonging to specific other clients. First, create the following file on the NetBackup master server:

install_path`\NetBackup\db\altnames\`*peername*

Then, add the client names to *peername*.

The client(s) named *peername* can restore files backed up by another client if:

- The name of the other client appears in the peername file, and
- The NetBackup client name setting on the client named peername is changed to match the client name in the peername file.

Example

Assume Windows 2000 client freddie wants to restore files backed up by client oscar:

1. The administrator creates the following file on the NetBackup master server:

   install_path`\NetBackup\db\altnames\freddie`

2. The administrator enters the name `oscar` on a separate line in the freddie file.

3. The user changes the NetBackup source client name setting in the Backup, Archive, and Restore user interface to oscar.

4. Client freddie restores the files backed up by client oscar.

Redirected Restore Examples

This section provides examples of configuring NetBackup to allow clients to restore files that were backed up by other clients. These example methods can be required when a client connects through a gateway or has multiple Ethernet connections. In all cases, the client you are restoring to must have an image-catalog directory on the master server in

install_path`\NetBackup\db\images\`*client_name*

or be a member of an existing NetBackup policy.

Caution Not all file system types on all machines support the same features and you may run into problems when restoring from one file system type to another. For example, the S51K file system on SCO machines does not support symbolic links nor does it support names greater than 14 characters long. If you restore to a machine or file system that does not support all the features of the machine or file system from which you performed the restore, you may not be able to recover all the files.

In the following examples:

- *restore_to_client* is the client that is requesting the restore.
- *backed_up_client* is the client that created the backups that the requesting client wants to restore.
- *install_path* is the path where you have installed the NetBackup software. By default, this path is `C:\Program Files\VERITAS`.

Note You must have the necessary permissions in order to perform the following steps.

Example 1

Assume you must restore files to *restore_to_client* that were backed up from *backed_up_client*. The *restore_to_client* and *backed_up_client* names are those specified by the NetBackup client name setting on the clients.

In the nominal case, follow these steps to perform the restore:

1. Log in on the NetBackup server and edit the file to include the name of *backed_up_client*:

   install_path`\NetBackup\db\altnames\`*restore_to_client*

2. Log in on *restore_to_client* and change the NetBackup client name on the client to *backed_up_client*.

3. Restore the file.

4. Undo the changes made on the server and client.

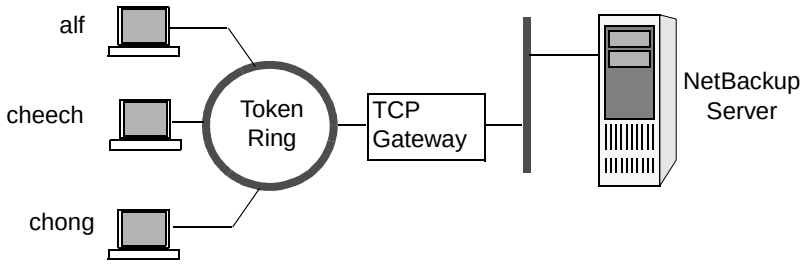
Example 2

This example explains how the `altnames` file can provide restore capabilities to clients that do not use their own host name when connecting to the NetBackup server.

By default, the NetBackup client name of the requesting client must match the peer name used in the connection to the NetBackup server. When the NetBackup client name is the host name for the client and matches the peer name (normal case), this requirement is met.

However, problems arise when clients connect to multiple Ethernets or connect to the NetBackup server through a gateway. Consider the configuration in the following figure.

Example Restore from Token Ring Client



In this example network, restore requests coming from clients, alf, cheech, and chong, are routed through the TCP gateway. Because the gateway uses its own peer name rather than the client host names for connection to the NetBackup server, NetBackup refuses the requests. This means that clients cannot restore even their own files.

To correct this situation proceed as follows:

1. Determine the peer name of the gateway:

   a. Attempt a restore from the client in question. In this example, the request fails with an error message similar to the following:

      ```
      client is not validated to use the server
      ```

   b. Examine the NetBackup problems report and identify the peer name used on the request. Entries in the report will be similar to:

      ```
      01/29/93 08:25:02 bpserver - request from invalid
      server or client bilbo.dvlp.null.com
      ```

   In this example, the peer name is `bilbo.dvlp.null.com`.

2. After determining the peer name, create the following file on the NetBackup master server:

   install_path`\NetBackup\db\altnames\`*peername*

   In our example, the file is:

   install_path`\NetBackup\db\altnames\bilbo.dvlp.null.com`

3. Edit the *peername* file to include the desired client names.

   For example, if you leave the file *install_path*`\NetBackup\db\altnames\bilbo.dvlp.null.com` empty, clients alf, cheech, and chong can all access the backups corresponding to their NetBackup client name setting. See "Allowing a Single Client to Perform Redirected Restores" on page 328.

   If you add the names cheech and chong to the file, you give these two clients access to NetBackup file restores, but exclude alf. See "Allowing Redirected Restores of Specific Client's Files" on page 328.

   Note that this example requires no changes on the clients.

4. Restore the files.

Example 3

If the files cannot be restored by using the method in Example 2, perform the following steps:

1. On the master server, check the checkbox for **Host Properties** > **Master Server** > **Enable Performance Data Collection**.

2. Create the debug log directory for the NetBackup Request Manager service:

   install_path`\NetBackup\logs\bprd`

3. On the master server, stop and then restart the NetBackup Request Manager service. This ensures that this service is running in verbose mode and logs information regarding client requests.

4. On *restore_to_client*, attempt the file restore.

5. On the master server, identify the peer-name connection used by *restore_to_client*.

   Examine the failure as logged in the All Log Entries report or the debug log for the NetBackup Request Manager service to identify the failing name combination:

   install_path`\NetBackup\logs\bprd\`*mmddyy.log*

6. On the master server, perform one of the following:

   - Create an *install_path*`\NetBackup\db\altnames\No.Restrictions` file. This lets any *restore_to_client* access any *backed_up_client* backups by changing its NetBackup client name setting to specify *backed_up_client*.
   - Create an *install_path*`\NetBackup\db\altnames\`*peername* file. This lets *restore_to_client* access any *backed_up_client* backups by changing its NetBackup client name setting to specify *backed_up_client* client.
   - Add the *backed_up_client* name to the file *install_path*`\NetBackup\db\altnames\`*peername*. This lets *restore_to_client* access only the backups created on *backed_up_client*.

7. On *restore_to_client*, change the NetBackup client name setting to match what is specified on *backed_up_client*.

8. Restore the files from *restore_to_client*.

9. Perform the following:

   - Delete *install_path*`\NetBackup\logs\bprd` (and its contents).
   - On the master server, clear the **Logging Enabled** property.

10. If you do not want the change to be permanent:

    - Delete *install_path*`\NetBackup\db\altnames\No.Restrictions` (if you created it)

- Delete *install_path*`\NetBackup\db\altnames\`*peername* (if you created it).
- On *restore_to_client*, change the NetBackup client name to its original value.

Improve Search Times by Creating an Image List

To improve search performance when you have many small backup images, run the following command (one line) as administrator on the master server:

install_path`\netbackup\bin\admincmd\bpimage -create_image_list -client` *name*

Where name is the name of the client that has many small backup images.

This creates the following files in the *install_path*`\netbackup\db\images\`*name* directory:

`IMAGE_LIST` - List of images for this client

`IMAGE_INFO` - Information about the images for this client

`IMAGE_FILES` - The file information for small images

Do not edit these files because they contain offsets and byte counts that are used for seeking to and reading the image information.

These files take 35 to 40 percent more space in the client directory and if you use them, verify that there is adequate space. Also, they improve search performance only when there are thousands of small backup images for a client.

Configuring NetBackup Ports

NetBackup communicates between computers by using a combination of *registered* and *dynamically allocated* ports.

- Registered ports are registered with the Internet Assigned Numbers Authority (IANA) and are permanently assigned to specific NetBackup services. For example, the port for the NetBackup client daemon service (`bpcd`) is 13782. These ports are specified in a system configuration file.

  On UNIX systems: `/etc/services`

  On Windows systems:
  `%system root%\system32\drivers\etc\services`

Registered Ports

NetBackup Services					
`bpcd`	13782	`bpjobd`	13723	`visd`	9284
`bpdbm`	13721	`bprd`	13720	`vnetd`	13724
`bpjava-msvc`	13722	`nbdbd`	13784	`vopied`	13783
Media Manager Services					
`acsd`	13702	`tlhcd`	13717	`tshd`	13715
`lmfcd`	13718	`tlmd`	13716	`tl4d`	13713
`odld`	13706	`tl8cd`	13705	`vmd`	13701
`rsmd`	13719	`ts8d`	13709		
`tldcd`	13711	`tsdd`	13714		

  Media Manager services include tape library control daemons, which accept connections from daemons on other servers that are sharing the same library. See the `services` file on the media server to determine the ports required for a specific library.

- Dynamically-allocated ports are assigned, as needed, from ranges that you can specify on NetBackup clients and servers. In addition to the range of numbers, you can configure the following for dynamically allocated ports:

- Whether NetBackup selects a port number at random from the allowed range or starts at the top of the range and uses the first one available.
- Whether connections to `bpcd` on a client use reserved or nonreserved ports.

These settings are useful in environments that use firewalls for security and are explained later in this section.

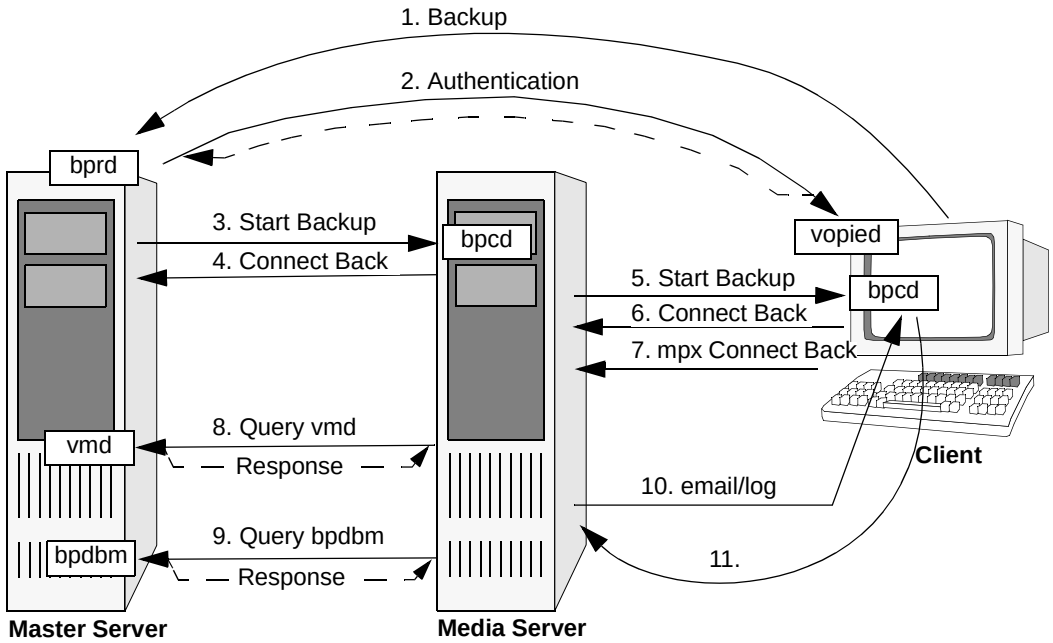
Server and Client Connections: General Case

This section explains the ports that NetBackup uses for connections between clients and servers when using the standard interfaces. The connections for alternative interfaces, such as the Windows Display Console are explained later.

Backups

A backup can be started by either the scheduler on the master server or a request from a client. The following figure shows the connections that occur for a client-requested backup. A scheduled backup works the same way, except there is no client request.

Backup Port Connections



The table “Connections for Backups” describes each connection and defines the ports that NetBackup uses:

- For registered ports, the table shows the port number (for example, 13720).
- For dynamically-allocated ports, the table indicates *Reserved* or *Nonreserved*. Some `bpcd` connections are shown as *Reserved or NonReserved*, depending on the allow non reserved port setting.

In addition to the ports in the “Backup Port Connections” figure and “Connections for Backups” table, the master and media server can have connections to robotic control daemons (`tl8cd` and so on). See the `services` file on the computers that share the tape library for those port numbers.

Connections for Backups

	Connect From [1]		Connect To [1]	
Description	**Host**	**Port**	**Host**	**Port**
1. Backup request to `bprd` on master server.	Client	Nonreserved	Master Server	13720 (`bprd`)
2. If NetBackup authentication is being used, and the request is from a nonprivileged user, `bprd` requests authentication from vopied on the client. Further communication between `vopied` and `bprd` is over the same connection.	Master Server	Nonreserved	Client	13783 (`vopied`)
3. The master server sends a backup request to `bpcd` on the media server. As part of the bpcd protocol, the master server also sends a port number for connecting back (see next step). The master server then listens on that port.	Master Server	Reserved	Media Server	13782 (`bpcd`)
4. Connect back to master server. Each backup has its own connect back.	Media Server	Reserved	Master Server	Reserved port specified during request in **3** above.
5. Backup request to `bpcd` on client. Again, as part of the `bpcd` protocol, the media server sends a port for connecting back.	Media Server	Reserved or Nonreserved (whichever `bpcd` on the client is configured to accept)	Client	13782 (`bpcd`)
6. Connect back to media server. Each backup job has its own connect back.	Client	Reserved or Nonreserved (whichever is used during request in **5** above)	Media Server	Reserved or NonReserved port specified during request in **5** above.

Connections for Backups (continued)

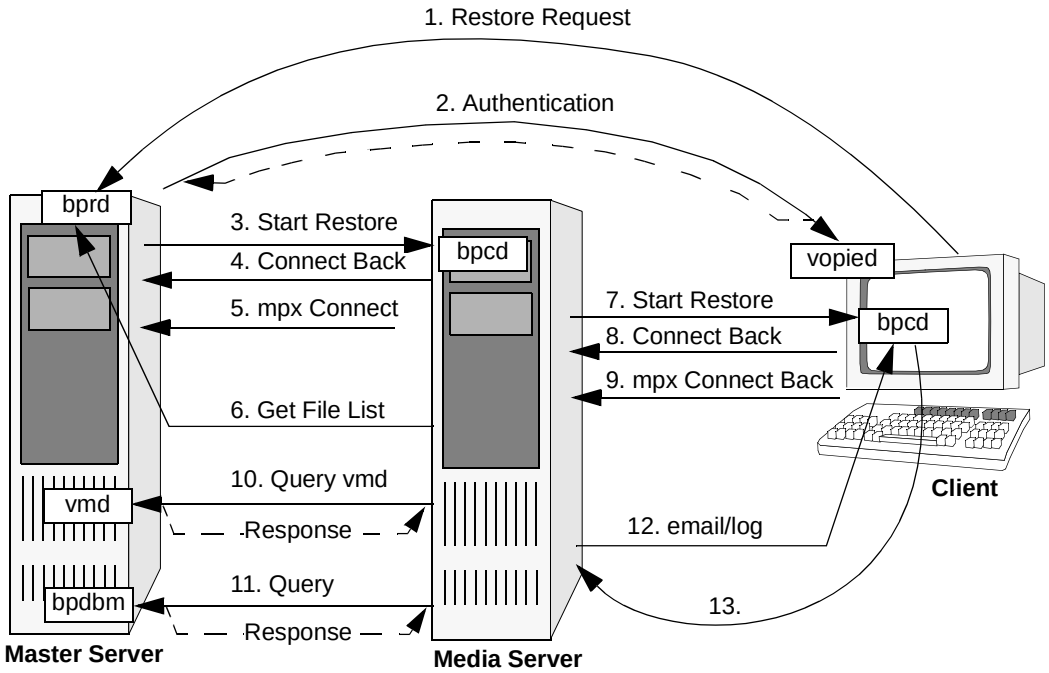
	Connect From [1]		Connect To [1]	
Description	**Host**	**Port**	**Host**	**Port**
7. If multiplexing (MPX) is used, each backup job requires an additional client-to-server connection.	Client	Reserved or Nonreserved (whichever is used during request in **5** above)	Media Server	Reserved or NonReserved port specified during request in **5** above.
8. Queries to `vmd`. During the backup, the media server sends queries to `vmd` on the master server. Responses are over the same connection.	Media Server	Nonreserved	Master Server	13701 (`vmd`)
9. Queries to `bpdbm`. During the backup, the media server sends queries to `bpdbm` on the master server. Responses are over the same connection.	Media Server	Nonreserved	Master Server	13721 (`bpdbm`)
10. Email notifications or log entries to `bpcd` on client. These connections also use the `bpcd` protocol, where the client connects back on a port specified by the server.	Media Server	Reserved or Nonreserved (whichever `bpcd` on the client is configured to accept)	Client	13782 (`bpcd`)
11. Connect back to media server.	Client	Reserved or Nonreserved (whichever is used during request in **10** above)	Media Server	Reserved or NonReserved port specified during request in **10** above.

1. For configuration instructions, see “Configuring Ports for Backups and Restores” on page 349.

Restores

A restore can be started by a restore request from a client. The following figure shows the connections that occur for a restore.

Restore Port Connections



The following table, “Connections for Restores,” describes each connection and defines the ports that NetBackup uses:

- For registered ports, the table shows the port number (for example, 13720).
- For dynamically-allocated ports, the table indicates *Reserved* or *Nonreserved*. Some `bpcd` connections are shown as *Reserved or NonReserved*, depending on the allow non reserved port setting.

In addition to the ports in the “Restore Port Connections” figure and “Connections for Restores” table, the master and media server can have connections to robotic control daemons (`tl8cd` and so on). See the `services` file on the computers that share the tape library for those port numbers.

Connections for Restores

	Connect From [1]		Connect To [1]	
Description	**Host**	**Port**	**Host**	**Port**
1. Restore request to `bprd` on master server.	Client	Nonreserved	Master Server	13720 (`bprd`)
2. If NetBackup authentication is being used, and the request is from a nonprivileged user, `bprd` requests authentication from `vopied` on the client. Further communication between `vopied` and `bprd` is over the same connection.	Master Server	Nonreserved	Client	13783 (`vopied`)
3. The master server sends a restore request to `bpcd` on the media server. As part of the bpcd protocol, the master server also sends `bpcd` a port number for connecting back (see next step). The master server then listens on that port.	Master Server	Reserved	Media Server	13782 (`bpcd`)
4. Connect back to master server. Each restore has its own connect back.	Media Server	Reserved	Master Server	Reserved port specified during request in **3** above.
5. If multiplexing (MPX) is used, each backup job requires an additional connect back to the master server.	Client	Reserved or	Media Server	Reserved port specified during request in **3** above.
6. Get file list.	Media Server	Reserved	Master Server	Reserved port specified during initial request in **1** above.

Connections for Restores (continued)

	Connect From [1]		Connect To [1]	
Description	**Host**	**Port**	**Host**	**Port**
7. Restore request to `bpcd` on client. Again, as part of the `bpcd` protocol, the media server sends `bpcd` ports for connecting back.	Media Server	Reserved or Nonreserved (whichever `bpcd` on the client is configured to accept)	Client	13782 (`bpcd`)
8. Connect back to media server. Each restore job has its own connect back.	Client	Reserved or Nonreserved (whichever is used during request in **6** above)	Media Server	Reserved or NonReserved port specified during request in **6** above.
9. If multiplexing (MPX) is used, each restore job requires an additional client-to-server connection.	Client	Reserved or Nonreserved (whichever is used during request in **6** above)	Media Server	Reserved or NonReserved port specified during request in **6** above.
10. Queries to `vmd`. During the backup, the media server sends queries to `vmd` on the master server. Responses are over the same connection.	Media Server	Nonreserved	Master Server	13701 (`vmd`)
11. Queries to `bpdbm`. During the backup, the media server sends queries to `bpdbm` on the master server. Responses are over the same connection.	Media Server	Nonreserved	Master Server	13721 (`bpdbm`)

Connections for Restores (continued)

	Connect From [1]		Connect To [1]	
Description	**Host**	**Port**	**Host**	**Port**
12. Email notifications or log entries to `bpcd` on client. These connections also use the `bpcd` protocol, where the client connects back on a port specified by the server.	Media Server	Reserved or Nonreserved (whichever `bpcd` on the client is configured to accept)	Client	13782 (`bpcd`)
13. Connect back to media server.	Client	Reserved or Nonreserved (whichever is used during request in `11` above)	Media Server	Reserved or NonReserved port specified during request in `11` above.

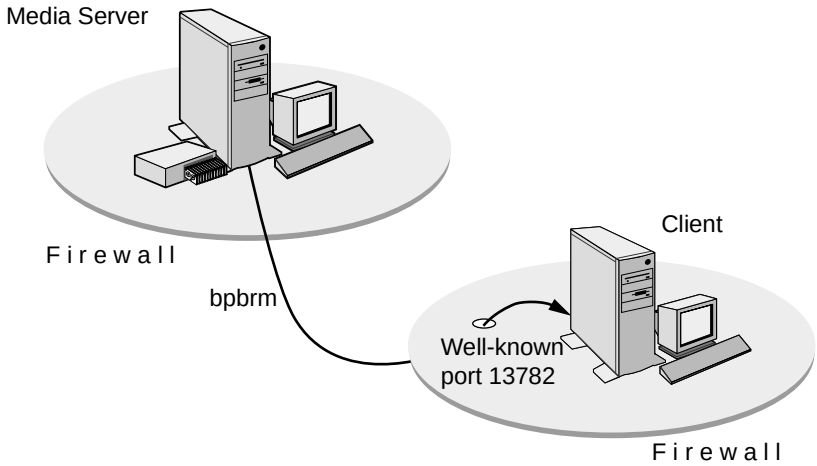
1. For configuration instructions, see “Configuring Ports for Backups and Restores” on page 349.

Using vnetd to Enhance Firewall Protection

The VERITAS Network Daemon (`vnetd`) was designed to enhance firewall efficiency with NetBackup during server-to-server and server-to-client communications. `Vnetd` runs on both UNIX and Windows platforms.

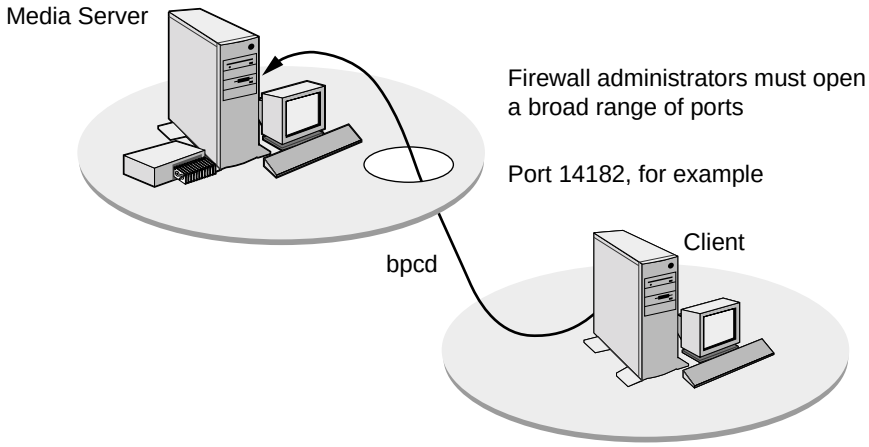
For example, when a media server running `bpbrm` is communicating with a client running `bpcd`, the situation does not pose a firewall problem because `bpbrm` is using a well-known port.

Media Server Running `bpbrm` and Client Running `bpcd`



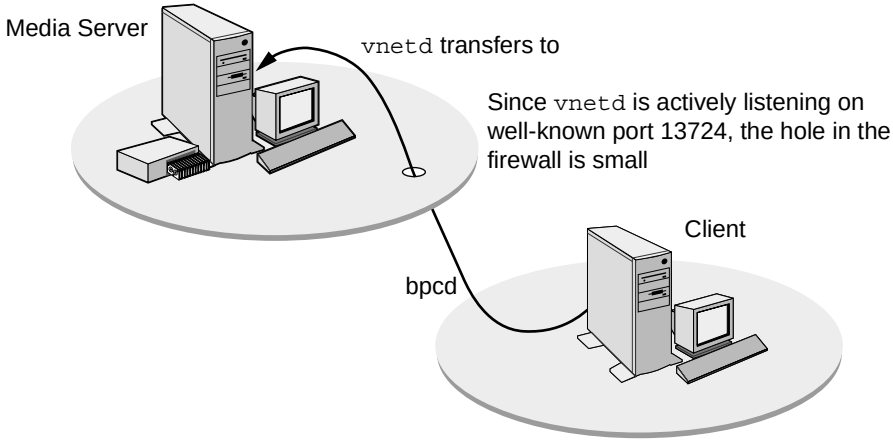
Using the traditional call-back method, `bpbrm` is not actively listening on a port for a specific connection from `bpcd`. Because `bpcd` could connect back to the media server on one of many ports, firewall administrators must make more ports available on the firewall to accommodate that communication.

Traditional Call-back Method



The new, no call-back method uses `vnetd`. `Vnetd` uses the well-known port 13724 to actively listen for a specific connection from another NetBackup process. If a firewall is in place, administrators need only to leave port 13724 open. `Vnetd` will transfer a socket from itself to another process on the same machine.

No Call-back Method Using vnetd



Note Both servers and clients must have NetBackup 4.5 installed for `vnetd` to work.

▼ To set up vnetd between a server and a client

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**.
2. In the right pane, double-click the host you wish to configure.
3. Select the **Client Attributes** tab.
4. In the client database list box, select the client you wish to change.
5. Check **No Callback**.
6. Click **OK**.

Or, add the client to the client database by running the `bpclient.exe` command, located in `\Program Files\VERITAS\NetBackup\bin\admincmd`. See "bpclient" on page 451.

▼ To set up vnetd between servers

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**.
2. In the right pane, double-click the host you wish to configure.
3. Select the **Firewall** tab.
4. In the client database list, select the client you wish to change.
5. Check **Use VNETD**.
6. Click **OK**.

▼ To enable logging for vnetd

Create a `vnetd` directory in the following location, then restart `vnetd`:

On Windows: *install_path*`\NetBackup\logs\vnetd`

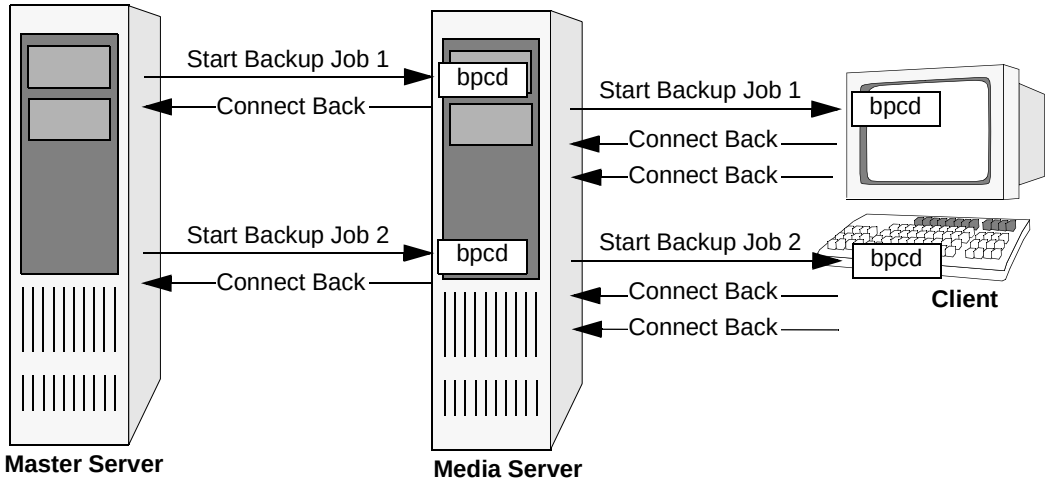
On UNIX: `/usr/openv/logs/vnetd`

Or, double-click `mklogdir.bat in the` *install_path*`\NetBackup\logs\` directory to populate the `logs` directory with log subdirectories, including one for `vnetd`.

Multiplexing

As was mentioned in earlier discussions, multiplexing requires an extra connect back for each job. With this exception, the connections are the same as for other backups and restores. The following figure shows the connections when multiplexing results in two backup jobs.

Connections for Multiplexed Backups



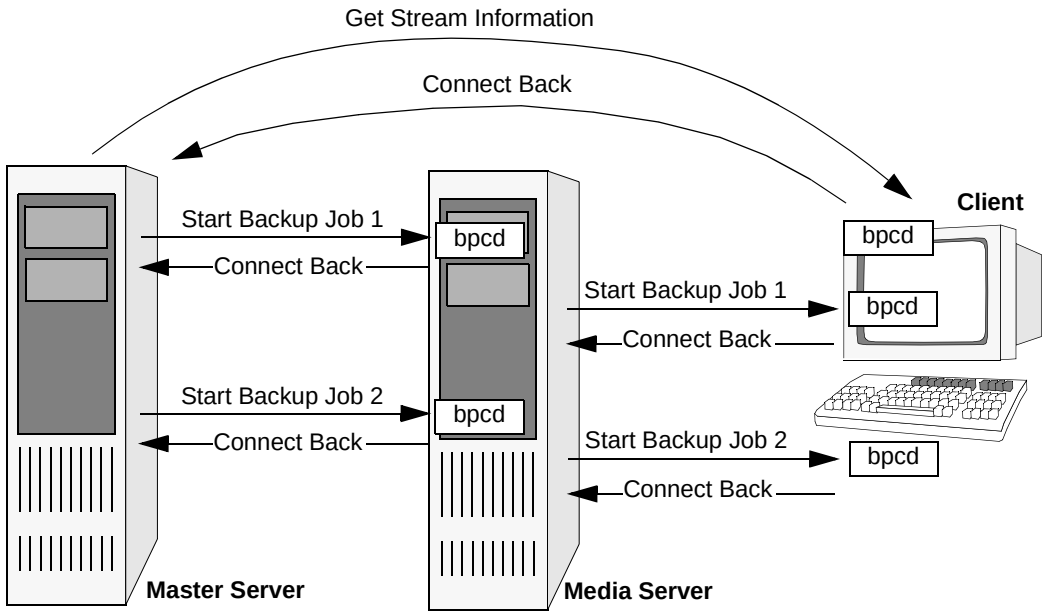
Multiple Data Streams

The connections for multiple jobs (streams) started as a result of using **Allow multiple data streams** are the same as for other backups. That is, NetBackup creates a separate set of connections for each job.

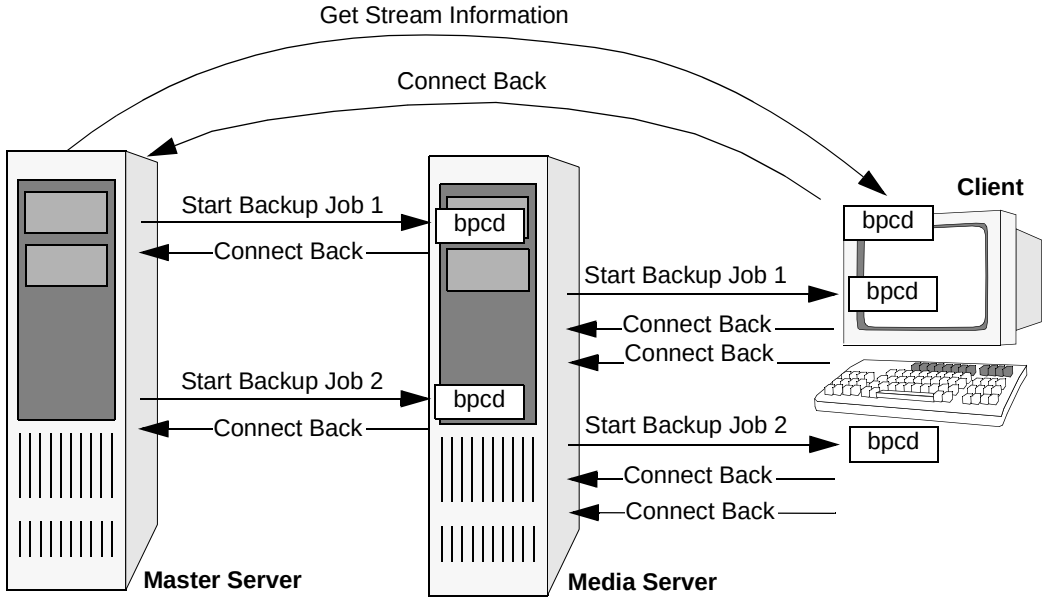
If auto-discover streaming mode is enabled (for example, by using the `ALL_LOCAL_DRIVES` directive), the master server opens an additional connection to `bpcd` on each client in order to obtain the required number of streams. This connection is to either a reserved or nonreserved port, depending on what the client is configured to accept for `bpcd`. The connect back is to the port specified during the `bpcd` connection and also is reserved or nonreserved according to what was used for `bpcd`.

The next two figures show backup connections both with and without multiplexing. Multiplexing results in an additional connect back for each job in the same way as when **Allow multiple data streams** is not used.

Connections for Multiple Data Streams - Without Multiplexing



Connections for Multiple Data Streams - With Multiplexing



Configuring Ports for Backups and Restores

The following explains the NetBackup configuration settings for ports. Registered port numbers (for example, 13782 for `bpcd`) are not configurable with these settings and VERITAS recommends that you do not attempt to change the registered port numbers.

Ports from which NetBackup originates connections to other hosts

These are the *Connect From* ports in tables "Connections for Backups" and "Connections for Restores." You can set the following on each host:

- Range of reserved ports from which NetBackup can originate connections. Use **Client Reserved Port Window**.
- Range of nonreserved ports from which NetBackup can originate connections. Use **Client Port Window**.
- Random or nonrandom port selection. By default, NetBackup chooses a port at random from those available in the allowed range. To have NetBackup start at the top of the allowed range and choose the first available port, clear **Use Random Port Assignments**.

Ports where NetBackup listens for connections from other hosts

These are the *Connect To* ports in tables "Connections for Backups" and "Connections for Restores." You can set the following on each host:

- `bpcd` to accept connections from nonreserved ports (the default is to not accept these connections). To permit connections from nonreserved ports, select **Allow Non-Reserved ports** for that host.

Note For clients, use the `bpclient` command on the master server to specify nonreserved port usage for the client. (See "Connect on Non-reserved Port" on page 263.)

- Range of reserved ports where NetBackup can listen for connections to this host. Use **Server Reserved Port Window**.
- Range of nonreserved ports where NetBackup can listen for connections to this host. Use **Server Port Window**.
- Random or nonrandom port selection. By default, NetBackup chooses a port at random from those available in the allowed range. To have NetBackup start at the top of the allowed range and choose the first available port, clear **Use Random Port Assignments.**

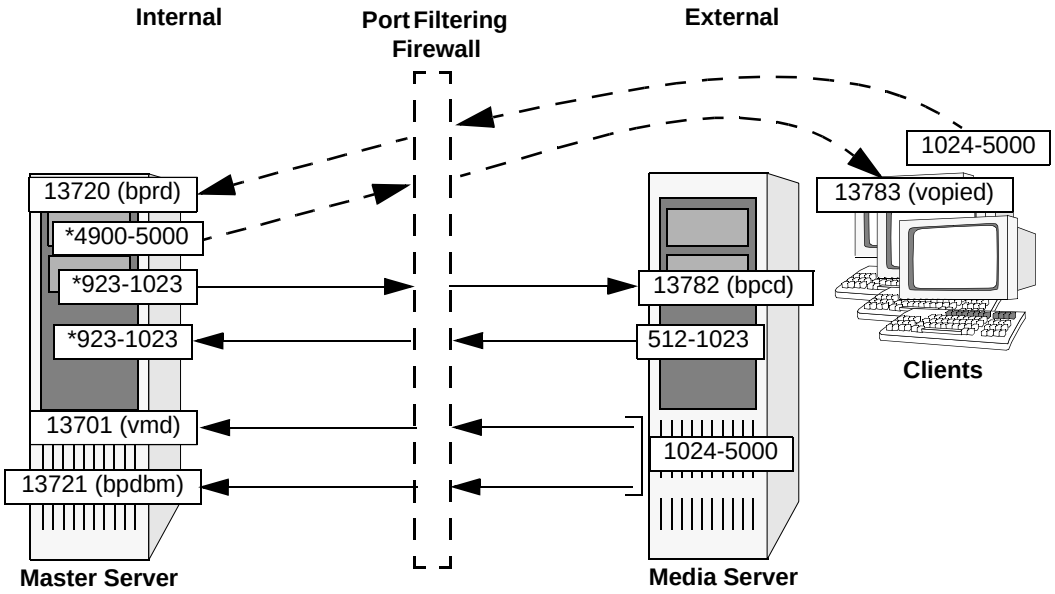
Configuration Example

The example network in the next figure "Master to Media Server and Clients Example," shows a master server in a private (internal) network that is inside a firewall. The clients and media server are outside the firewall. To meet the port requirements shown in this figure, you must configure NetBackup to:

- Limit external connections to NetBackup in the private network by allowing the master server to accept reserved connections only on ports 923 through 1023 (the default is 512 through 1023).
- Limit NetBackup connections out of the private network by allowing the master server to:
  - Use only ports 4900 through 5000 for nonreserved-port connections to the clients (the default is 1024 through 5000).
  - Use only ports 923 through 1023 for reserved-port connections to `bpcd` on the media server (the default is 512 through 1023).

Note Any port limitations you configure on a NetBackup host apply to connections with *all* other NetBackup hosts, not just those on the other side of the firewall. Therefore, leave enough ports available to allow the necessary connections. The main factors to consider are the number of clients and whether multiplexing is used. If NetBackup runs out of ports, backups and restores cannot occur.

Master to Media Server and Clients Example



* This setting is not the default.

To configure NetBackup, perform the following on the master server (no changes are required on the media server or clients):

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**.

2. In the right pane, double-click the host you wish to configure.

3. Select the **General Server** tab:

   a. Set **Client Reserved Port Window** to range from 923 through 1023.

      This specifies the reserved ports that the master server can use to originate connections, including those to `bpcd` on the media server.

   b. Set **Client Port Window** to range from 4900 through 5000.

      This specifies the reserved ports that the master server can use to originate connections, including those to `vopied` on the client.

   c. Set **Server Reserved Port Window** to range from 923 through 1023

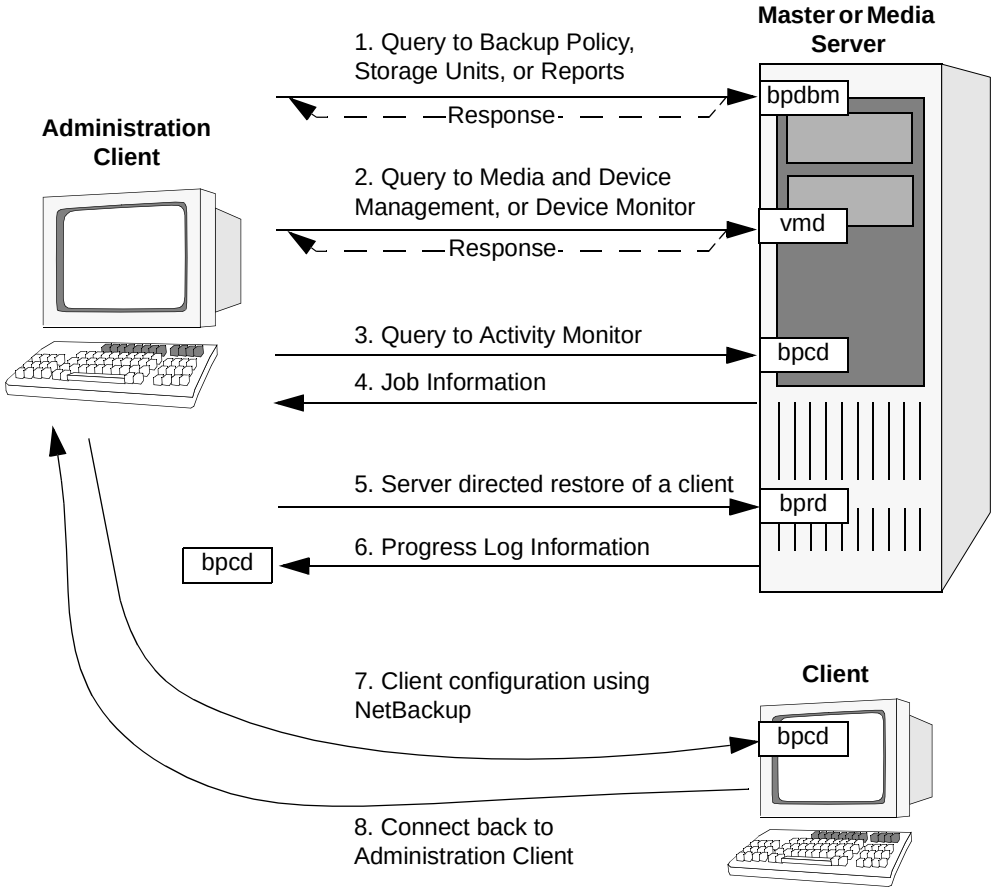
      This specifies the reserved ports where the master server can elect to listen for connections.

The master server chooses from this range when it specifies the ports where it will listen for call back connections from `bpcd`.

Administration Client Connections

An administration client is a Windows system that has NetBackup Administration Console installed. You can use this client to perform all the administrative tasks that can be performed from a NetBackup server. The following figure shows the connections between an Administration Client and a NetBackup server. The accompanying table, "Connections for Administration Client," describes each connection and defines the ports that NetBackup uses.

Administration Client Connections



Connections for Administration Client

Description	Connect From		Connect To	
	Host	**Port**	**Host**	**Port**
1. Request Backup policy, storage unit, or report information. The response is over the same connection. Each application requires its own connection	Administration Client	Non-reserved	Master server	13721 (bpdbm)

Connections for Administration Client (continued)

Description	Connect From		Connect To	
	Host	**Port**	**Host**	**Port**
2. Request information from Media and Device Management or Device Monitor. The response is over the same connection. Each application requires its own connection	Administration Client	Nonreserved	Master or media server	13701 (`vmd`)
3. Request to Activity Monitor for job information.	Administration Client	Reserved or Nonreserved (whichever the server is configured to accept for `bpjobd`)	Master server	13723 (`bpjobd`)
4. Connect back to pass job information to Administration Client.	Master server	Reserved or Nonreserved (whichever is used during request in **3** above)	Administration Client	Reserved or nonreserved port specified during request in **3** above.
5. Request server-directed restore of a client.	Administration Client	Nonreserved	Master server	13720 (`bprd`)
6. Send progress log information to the Administration Client.	Master or media server	Reserved or Nonreserved (whichever the client is configured to accept)	Administration Client	13782 (`bpcd`)
7. Configure the NetBackup client. As part of the `bpcd` protocol, the Administration Client also sends `bpcd` a port number for connecting back (see next step). The Administration Client then listens on that port.	Administration Client	Reserved or Nonreserved (whichever the client is configured to accept)	Client	13782 (`bpcd`)

Connections for Administration Client (continued)

Description	Connect From		Connect To	
	Host	**Port**	**Host**	**Port**
8. Connect back to Administration Client.	Client	Reserved or Nonreserved (whichever is used during request in **7** above)	Administration Client	Reserved port specified during request in **7** above.

Configuring Ports When Using an Administration Client

The following section explains the NetBackup configuration settings for ports. Registered port numbers (for example, 13782 for `bpcd`) are not configurable with these settings and VERITAS recommends that you do not attempt to change the registered port numbers.

Ports from which NetBackup originates connections to other hosts

These are the *Connect From* ports in the "Connections for Administration Client" table. You can set the following on each host:

- Range of reserved ports from which NetBackup can originate connections:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab. Set the range for the reserved ports in the **Client Reserved Port Window** fields.

- Range of nonreserved ports from which NetBackup can originate connections:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab. Set the range for the nonreserved ports in the **Client Port Window** fields.

- Random or nonrandom port selection. By default, NetBackup chooses a port at random from those available in the allowed range. To have NetBackup start at the top of the allowed range and choose the first available port:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab. Clear the check for **Use Random Port Assignment**.

Ports where NetBackup listens for connections from other hosts

These are the *Connect To* ports in the table "Connections for Administration Client." You can set the following on each host:

- `bpcd` to accept connections from nonreserved ports (the default is to *not* accept these connections). To permit connections from nonreserved ports:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **Universal Settings** tab. Check **Allow Non-reserved Ports**.

Note To specify nonreserved port usage for the client:
On the master, expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **Client Attributes** tab. Check **Connect on Non-reserved Port**. Or, see "Connect on Non-reserved Port" on page 263.

- Range of reserved ports where NetBackup can listen for connections to this host:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab. Set the range for the reserved ports in the **Server Reserved Port Window** fields.

- Range of nonreserved ports where NetBackup can listen for connections to this host:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab. Set the range for the nonreserved ports in the **Server Port Window** fields.

- Random or non-random port selection. By default, NetBackup chooses a port at random from those available in the allowed range.

  To have NetBackup start at the top of the allowed range and choose the first available port:

  Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab. Clear the check in **Use Random Port Assignment**.

Configuration Example

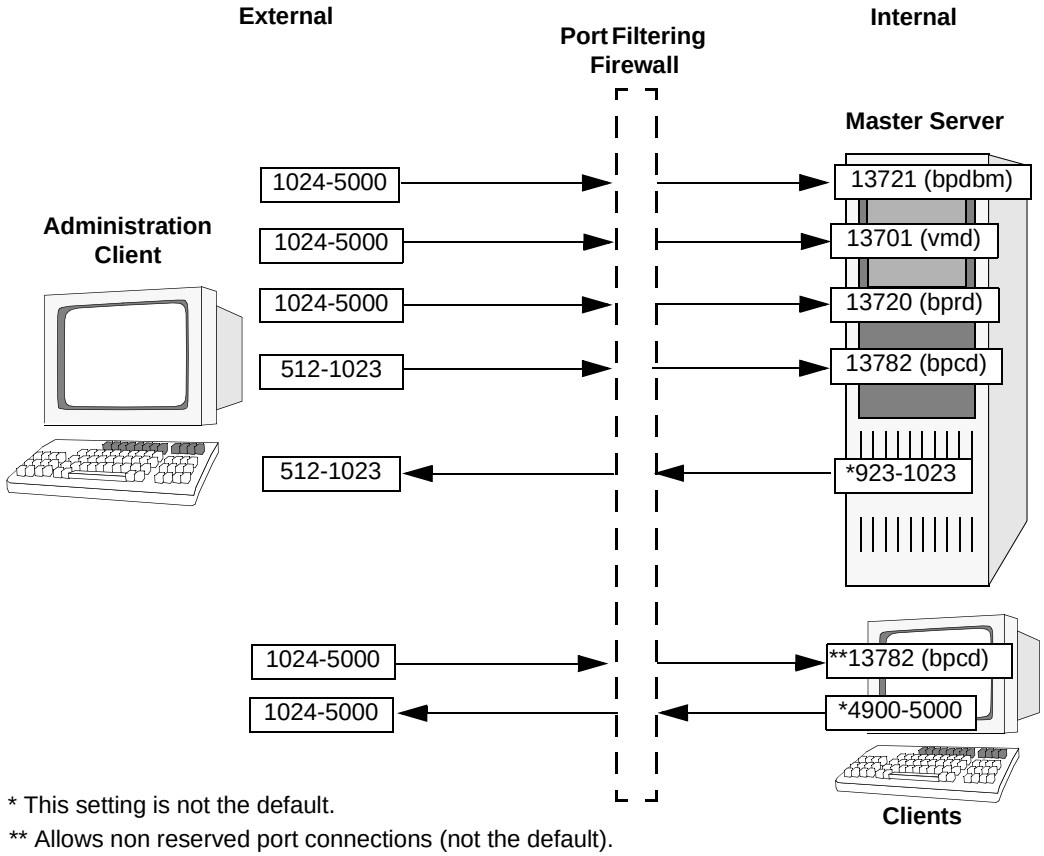
The example network in the next figure, "Master to Media Server and Clients Example," shows a master server in a private (internal) network that is inside a firewall. You are going to use the administration client to manage the master server from outside the firewall. To meet the port requirements shown in this figure, you must configure NetBackup to:

- Limit external connections to NetBackup in the private network by allowing nonreserved port connections to `bpcd` on the master server and the clients.
- Limit NetBackup connections out of the private network by:

- Allowing the master server to use only ports 923 through 1023 for reserved-port connections to the administration client (the default is 512 through 1023).
- Allowing the clients to use only ports 4900 through 5000 for nonreserved-port connections to the administration client (the default is 1024 through 5000).

Note Any port limitations you configure on a NetBackup host apply to connections with *all* other NetBackup hosts, not just those on the other side of the firewall. Therefore, leave enough ports available to allow the necessary connections. The main factors to consider are the number of clients and whether multiplexing is used. If NetBackup runs out of ports, backups and restores cannot occur.

Master to Media Server and Clients Example



To configure NetBackup, perform the following steps on the master server. No configuration is required on the administration client.

1. In the NetBackup Administration Console, expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server**.

2. In the right pane, double-click the host you wish to configure.

3. Select the **General Server** tab:

   Set **Client Reserved Port Window** to range from 923 through 1023. This specifies the reserved ports that the master server can use to originate connections, including those to the administration client.

4. Select the **Universal Settings** tab and put a check in **Allow Non-reserved Ports**.

5. Select the **Client Attributes** tab.

   a. Select the clients in the list box.

   b. Select **Connect on Non-reserved Port**. Requests to `bpcd` on the clients will now originate from nonreserved ports.

6. Double-click on **Clients** to display properties.

   a. Select the **Universal Settings** tab. Check **Allow Non-reserved Ports**.

   b. Select the **General Client** tab:

      Set **Client Port Window** to range from 4900 through 5000. This specifies the nonreserved ports the clients can use to originate connections, including those to the administration client.

NetBackup-Java Console Connections

The NetBackup-Java Console is a system (UNIX or Windows) that has the NetBackup-Java interface software installed.

Running the NetBackup-Java Console on a UNIX Platform

When the NetBackup-Java Console is running on a UNIX platform, the system can perform all the administrative tasks that can be performed from a NetBackup UNIX server or Windows server. The NetBackup-Java Console can also perform backups or restores of UNIX clients.

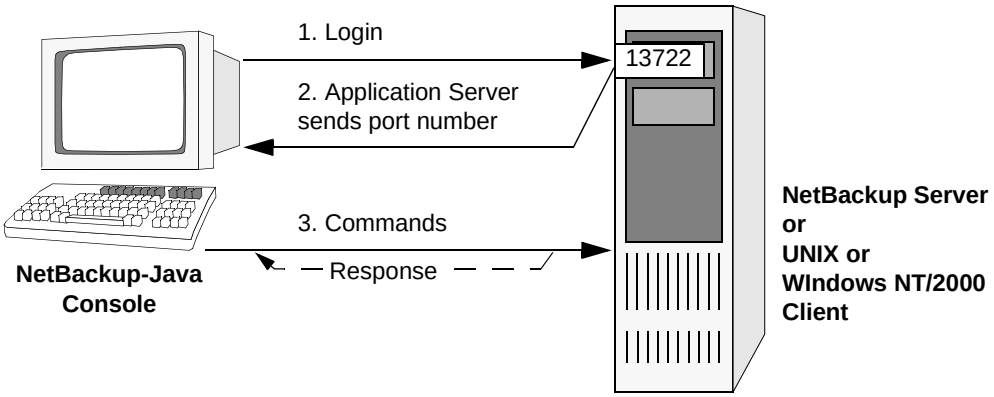
Running the NetBackup-Java Console on a Windows Platform

When the NetBackup-Java Console is running on a Windows platform, the system administrator can perform only backups or restores of UNIX clients. Administrator applications are not available from the NetBackup-Java Console running on a Windows system.

If you need to administer other systems from Windows, consider installing the NetBackup Administration Console on the Windows machine. After the Administration Console is installed, you can use the **File** > **Change Server** command to select another server (UNIX or Windows) to administer.

The following figure shows the connections between a NetBackup-Java Console and the NetBackup-Java Application Server on a NetBackup server or client. The accompanying table, “Connections for the NetBackup-Java Console,” provides a brief description of each connection and defines the ports that the NetBackup Console and its application server uses.

NetBackup-Java Console Connections



Connections for the NetBackup-Java Console

Description	Connect From		Connect To	
	Host	**Port**	**Host**	**Port**
1. Log in to the NetBackup-Java Application Server on the NetBackup server or client.	Where the NetBackup-Java Console was started	Chosen by local host or (A)	UNIX server or client	13722 (`bpjava-msvc`)
2. The NetBackup-Java Application Server on the server or client responds by sending the port number where the display console must connect in order to send commands. This response is over the same connection. The server then listens on that port for commands. A unique port (C) is specified for each user that is logged in or (B).	UNIX server or client	13722	Where the NetBackup-Java Console was started	Chosen by local host or (A)

Connections for the NetBackup-Java Console

Description	Connect From		Connect To	
	Host	Port	Host	Port
3. Send commands (for example, to start Backup Policy Management). Responses from the server or client are over the same connection. A unique port (C) and connection is established for each user that is logged in. When a connection is established, it is used for all further commands and responses for that user or (B).	Where the NetBackup-Java Console was started	Chosen by local host or (A)	UNIX server or client	Nonreserved port specified in the login response (see step 2) or (B)
4. Request to Activity Monitor for job information.	Where the NetBackup-Java Console was started	Chosen by local host or (A)	UNIX or Windows server	13724 (`vnetd`) to ultimately connect to `bpjobd`

A. One of the ports in the range specified by the NetBackup-Java Console configuration option, NBJAVA_CLIENT_PORT_WINDOW.

B. If the NetBackup-Java Console configuration option, NBJAVA_CONNECT_OPTION is set to 1, no additional ports will be used.

C. This unique port can be restricted to a configured range of ports using the SERVER_PORT_WINDOW option on the server or client.

Configuring Ports When Using the NetBackup-Java Console

On UNIX systems, all settings are in the `/usr/openv/netbackup/bp.conf` file on the respective server, or in the `/usr/openv/java/nbj.conf` file.

On Windows NT/2000 systems, all settings are made with the Host Properties dialog in the NetBackup Administration Console, or in the `<`*install_path*`>\Veritas\java\<`*hostname*`>.vrtsnbuj` files.

Port configurations may include:

- Range of nonreserved ports where the server or client can listen for connections. These are the *Connect To* ports in the preceding table, “Connections for the NetBackup-Java Console.” Use **Server Port Window** for this setting.

  The server or client selects a port from this range to listen for commands from the display console. Note that the highest port available in the allowed range is always used internally by the NetBackup-Java Application Server on the server or client.

- Random or nonrandom port selection. By default, the NetBackup-Java Application Server chooses a port at random from those available in the allowed range. To have the NetBackup-Java Application Server start at the top of the allowed range and choose the first available port, clear **Use Random Port Assignments.**

Note Registered port numbers (for example, 13782 for `bpcd`) are not configurable with these settings and VERITAS recommends that you do not attempt to change the registered port numbers.

On all NetBackup-Java capable platforms you can configure the following:

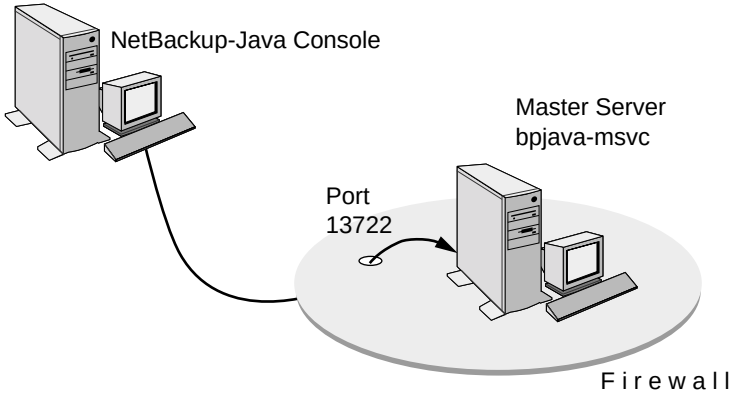
- The range of nonreserved ports on the console available for connecting to the NetBackup-Java Console configuration.
- Configure the NetBackup-Java Console to *not* use a unique port for every user using the console via the NetBackup-Java Console configuration option. This requires access to the `vnetd` daemon on its port.

Note These options cannot be configured using the NetBackup-Java Console **Host Properties** dialog. The `nbj.conf` file or the *hostname*`.vrtsnbuj` file on the relevent host must be edited.

Configuration Example

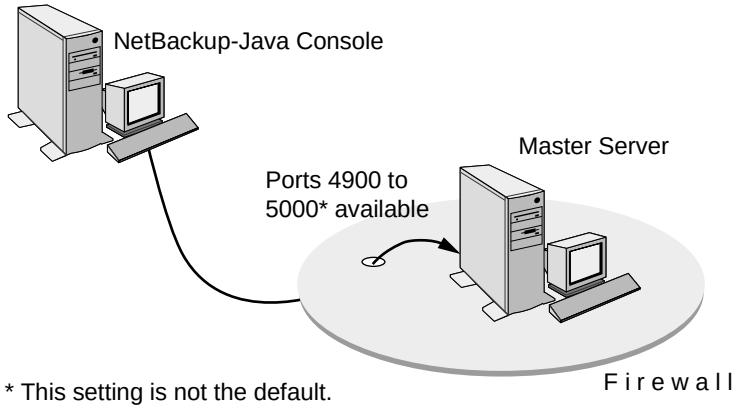
This example concerns using the NetBackup-Java Console to manage a master server that is inside a firewall.

NetBackup-Java Console to Server Example



The port requirements in this example are as follows:

- Limit external connections to the master server by allowing the master server to accept nonreserved-port connections only on ports 4900 through 5000 (the default is 1024 through 5000).
- Ports are to be selected by using the first one available, starting at the top of the allowed range.



Note Any port limitations you configure on a master server apply to connections with all other master servers, not just those on the other side of the firewall. Therefore, leave enough ports available to allow the necessary connections. The main factors to consider are the number of clients and whether multiplexing is used. If NetBackup runs out of ports, backups and restores cannot occur.

In order to effect the configuration of the master server, perform the following steps in the **Host Properties** dialog using the NetBackup-Java Console:

To configure the master server per the example:

1. In the NetBackup Administration Console on the master server, expand **Master Server** > **NetBackup Management** > **Host Properties > Master Server**.
2. In the right pane, double-click the host you wish to configure.
3. Select the **General Servers** tab:

   The **General Servers** settings specify the range of nonreserved ports from which the master selects a port to listen for command connections. Note that the highest port available in the range is always used internally by NetBackup-Java (in this example, the highest port that can be available is 5000).
4. Clear the checkbox for **Use Random Port Assignments**.

With this option unselected, NetBackup uses the first port available, starting at the top of the allowed range. In the example, the highest port that can be available is 4999 because 5000 is claimed by NetBackup-Java.

Note On a NetBackup UNIX client, add the following to the `/usr/openv/netbackup/bp.conf` file:

```
SERVER_PORT_WINDOW = 4900 5000
RANDOM_PORTS = NO
```

▼ To configure the master server to use vnetd per the example

1. In `/usr/openv/java/nbj.conf`, indicate that the NetBackup-Java Console should use the no call-back method when communicating with other NetBackup machines:

   ```
   NBJAVA_CONNECT_OPTION=1
   ```

   Setting `NBJAVA_CONNECT_OPTION` to 1 means that the NetBackup-Java Console will use only one port, the `vnetd` port, for communication with its application server.

2. If desired, specify a range of nonreserved outgoing ports on which the NetBackup-Java Console requires to connect to its application server. For example:

   ```
   NBJAVA_CLIENT_PORT_WINDOW=5700 5900
   ```

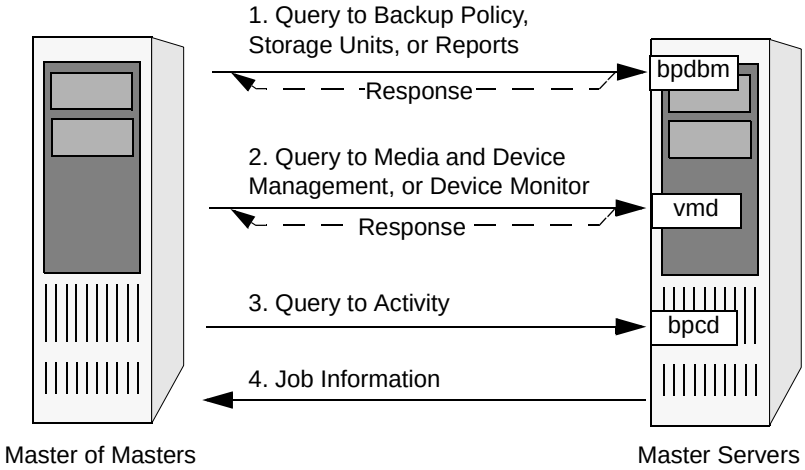
   The minimum range size for successful operation of the NetBackup-Java Console is 120.

Note Performance is somewhat reduced with the use of `NBJAVA_CONNECT_OPTION` or `NBJAVA_CLIENT_PORT_WINDOW`.

Global Data Manager Connections

The following figure shows the connections between a Master of Masters and a NetBackup Master server. The accompanying table, “Connections for Master of Masters,” provides a brief description of each connection and defines the ports that NetBackup uses.

Global Data Manager Connections



Connections for Master of Masters

Description	Connect From [1]		Connect To [2]	
	Host	Port	Host	Port
1. Request Backup policy, storage unit, or report information. The response is over the same connection.	Master of Masters	Nonreserved and chosen by the local host	Master server	13721 (`bpdbm`)
2. Request information from Media and Device Management or Device Monitor. The response is over the same connection.	Master of Masters	Nonreserved and chosen by the local host	Master server	13701 (`vmd`)
3. Request to Activity Monitor for job information. As part of the `bpcd` protocol, the Master of Masters also sends `bpcd` a port number for connecting back (see next step) and then listens on that port.	Master of Masters	Reserved The actual number is chosen by the local host	Master server	13782 (`bpcd`)
4. Connect back to pass job information to the Master of Masters.	Master server	Reserved	Master of Masters	Reserved port specified in the login response (see **3** above).

Configuring Ports When Remotely Administering More than One Master Server

The following section describes port configuration in the situation where a user logs into one server (Server A), then changes to another server (Server B).

On the initial server (Server A), you can configure the following:

- Range of reserved ports where the initial server can listen for connections. This applies to the port that the Master of Masters listens on for the connect back (see step 4 in the table “Connections for Master of Masters.”) Use **Server Reserved Port Window** for this setting.

- Random or nonrandom port selection. By default, NetBackup chooses a port at random from those available in the allowed range. To have NetBackup start at the top of the allowed range and choose the first available port, clear **Use Random Port Assignments.**

On each master server you can configure the following:

- Range of reserved ports where the master server can originate connections to other hosts. This applies to the port that the master server uses for the connect back (see step 4 in the table "Connections for Master of Masters.") To do this, use **Client Reserved Port Window**.
- Random or nonrandom port selection. By default, NetBackup chooses a port at random from those available in the allowed range. To have NetBackup start at the top of the allowed range and choose the first available port, clear **Use Random Port Assignments.**

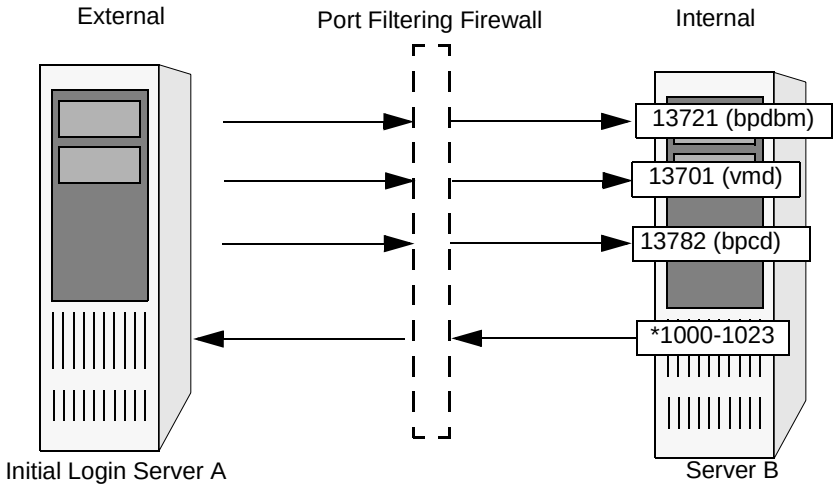
Configuration Example

The example network in the "Global Data Manager Connections" figure shows a master server in a private (internal) network that is inside a firewall. You are going to use the Master of Masters to manage the master server from outside the firewall. To meet the port requirements shown in this figure, you must configure NetBackup to:

- Limit the range of reserved ports that the master server can use to send job information to the Master of Masters to be from 1000 to 1023.

Note Any port limitations you configure on a NetBackup host, apply to connections with *all* other NetBackup hosts, not just those on the other side of the firewall. Therefore, leave enough ports available to allow the necessary connections. The main factors to consider are the number of clients and whether multiplexing is used. If NetBackup runs out of ports, backups and restores cannot occur.

Global Data Manager Connections



* This setting is not the default.

To configure NetBackup, perform the following on each server you plan to administer in addition to the initial server (Server A above).

1. Set the range of reserved ports from which NetBackup can originate connections:

   Expand **NetBackup Management** > **Host Properties** > **Master Server**. Double-click the host, then select the **General Server** tab.

2. Specify a range from 1000 through 1023 for the **Client Reserved Port Window**. These are the reserved ports that the master server can use to originate connections.

Load Balancing

NetBackup provides ways to balance loads between servers, clients, policies, and devices. These features are explained in the following topics. When making changes, remember that these settings are interactive, and compensating for one problem can cause another. The best approach to configuring these attributes is to use the defaults unless you anticipate or encounter a problem.

Adjust Backup Load on Server

Change the **Limit Jobs Per Policy** attribute for one or more of the policies that the server is backing up. For example, decreasing **Limit Jobs Per Policy** reduces the load on a server on a specific network segment. Reconfiguring policies or schedules to use storage units on other servers also reduces the load. Another possibility is to use NetBackup's bandwidth limiting on one or more clients.

Adjust Backup Load on Server Only During Specific Time Periods

Reconfigure schedules that run during those time periods, so they use storage units on servers that can handle the load (assuming you are using media servers).

Adjust Backup Load on Client

Change the **Maximum Jobs Per Client** global attribute. For example, increasing **Maximum Jobs Per Client** increases the number of concurrent jobs that any one client can process and therefore increases the load.

Reduce Time To Back Up Clients

Increase the number of jobs that clients can perform concurrently, or use multiplexing. Another possibility is to increase the number of jobs that the server can perform concurrently for the policy or policies that are backing up the clients.

Give Preference To a Policy

Increase the **Limit Jobs Per Policy** attribute for the preferred policy relative to other policies. Or, increase the priority for the policy.

Adjust Load Between Fast and Slow Networks

Increase the **Limit Jobs Per Policy** and **Maximum Jobs Per Client** for policies and clients in a faster network and decrease these numbers for slower networks. Another solution is to use NetBackup's bandwidth limiting.

Limit the Backup Load Produced By One or More Clients

Use NetBackup's bandwidth limiting to reduce the bandwidth used by the clients.

Maximize Use of Devices

Use multiplexing. Also, allow as many concurrent jobs per storage unit, policy, and client as possible without causing server, client, or network performance problems.

Prevent Backups From Monopolizing Devices

Limit the number of devices that NetBackup can use concurrently for each policy or the number of drives per storage unit. Another approach is to not put some devices under Media Manager control.

You can also place some drives in a down state or limit the number used concurrently in a specific storage unit. For example, if there are four drives in a robot, allow only two to be used concurrently.

Enhanced Authentication and Authorization 9

Enhanced authentication allows each side of a NetBackup connection to verify the host and user on the other side of the connection. By default, NetBackup runs without enhanced authentication.

Enhanced authorization determines if authenticated users (or groups of users) have NetBackup administrative privileges. By default, NetBackup gives administrative privileges to UNIX root administrators or Windows system administrators on NetBackup servers. In order to use enhanced authorization, you must configure enhanced authentication.

This chapter contains the following sections:

- Common Configuration Elements
- Enhanced Authentication
- Enhanced Authorization

Common Configuration Elements

The following sections describe elements involved in configuring enhanced authentication and enhanced authorization.

Configuration Files

The following configuration files are used by enhanced authentication, enhanced authorization, or both. Some may need to be modified during configuration.

Location of Configuration Files

Option	File	Master or Media Server Platform	Path to Directory
Enhanced Authentication and Enhanced Authorization	methods.txt template.methods.txt* methods_allow.txt template.methods_allow.txt* methods_deny.txt template.methods_deny.txt* names_allow.txt template.names_allow.txt* names_deny.txt template.names_deny.txt*	UNIX	`/usr/openv/var/auth`
		Windows	*install_path*`\NetBackup\var\auth`
		Macintosh	`:System Folder:Preferences:NetBackup:var:auth`
Enhanced Authorization	authorize.txt	UNIX	`/usr/openv/var/`
		Windows NT/2000	*install_path*`\NetBackup\var\`
* If it is necessary to create a new .txt file, base the new .txt file on the template file.			

methods.txt

The `methods.txt` file is an essential file which defines the supported enhanced authentication methods.

By default, `methods.txt` lists the two supported methods:

- `vopie` – one-time password authentication. The `vopie` method authenticates user name, host names, and group/domain names.

- `noauth` authentication – The `noauth` method exchanges user name, host names, and group / domain names, but makes no attempt to verify that the information is correct.

Each method is listed on a separate line in the file, and shows the method number, method name, and the path to a shared library:

Entries in methods.txt File

Platform	Line in methods.txt
UNIX (except HP-UX)	`128 vopie /usr/openv/lib/libvopie.so` `0 noauth /usr/openv/lib/libvnoauth.so`
UNIX (HP-UX only)	`128 vopie /usr/openv/lib/libvopie.sl` `0 noauth /usr/openv/lib/libvnoauth.sl`
Windows	`128 vopie` *install_path*`\NetBackup\lib\libvopie.dll` `0 noauth` *install_path*`\NetBackup\lib\libvnoauth.dll`
Macintosh	`128 vopie libvopie.dll` `0 noauth libvnoauth.dll`

The order in which the methods are listed in the file is important: The method listed first indicates that it is preferred to the second method.

Syntax rules for `methods.txt`

- Empty lines are ignored
- The # character and all following characters on a line are ignored.

methods_allow.txt

The `methods_allow.txt` file defines the authentication methods that NetBackup servers and clients can use.

When a client or server attempts a connection, it specifies the authentication method it is using. The other server or client then checks its `methods_allow.txt` file to determine if that method is allowed for the system that is attempting the connection. If an entry in this file matches the host and method, the method is allowed. Otherwise, NetBackup checks the `methods_deny.txt` file.

Example methods_allow.txt File

```
# All hosts in the ourcompany.com domain and host name
```

```
# bob.theircompany.com can use the vopie method.
vopie : .ourcompany.com, bob.theircompany.com
#
# Hosts with IP addresses in the 12.123.56 network and IP address
# 2.123.57.23 can use all methods.
ALL : 12.123.56.
ALL : 12.123.57.23
```

The keyword `ALL` is used to specify all valid methods, as in the previous example, or all possible hosts.

The default file is empty.

Syntax Rules for methods_allow.txt

- Each entry must be on a separate line.
- Empty lines are ignored.
- The # character and all following characters on a line are ignored.
- If a domain name is preceded by a dot (.), all hosts in that domain will match.
- If a network number is followed by a dot (.), all IP numbers in that network will match.
- A comma separated list of name patterns and number patterns can be specified on a single line.

methods_deny.txt

The `methods_deny.txt` file defines the authentication methods that NetBackup servers and clients *cannot* use.

NetBackup checks this file only if the `methods_allow.txt` file does not have a matching entry for the host and method. If a matching entry is found in `methods_deny.txt` the method is not allowed and authentication is not used. Otherwise, the method is used and authentication proceeds.

Example methods_deny.txt File

```
# All hosts in the ourcompany.com domain cannot use the vopie method.
vopie : .ourcompany.com
#
# Hosts with IP addresses in the 12.123.56 network cannot use all
# methods.
ALL : 12.123.56.
```

The default file contains only the following entry:

```
ALL : ALL
```

This means that all methods are denied for all hosts, unless it is specified otherwise in the `methods_allow.txt` file.

Syntax Rules for methods_deny.txt

The syntax rules for `methods_deny.txt` are the same as for `methods_allow.txt`. (See "Syntax rules for methods.txt" on page 373.)

names_allow.txt

The `names_allow.txt` file defines the network host names that a NetBackup client or server can use when establishing connections. This file is required when NetBackup client or server names do not correlate to their host names and IP addresses.

For example, when:

- NetBackup clients are using DHCP or another dynamic addressing scheme. Here, a client probably uses a different IP address each time it attempts a connection.
- A NetBackup server or client has more than one network interface. Here, the host name associated with the IP address can be different than the NetBackup server or client name.
- A NetBackup server or client connects through a gateway. Here, the peername for the gateway can be different than the NetBackup server or client name.

In the above instances, when a client or server attempts a connection, NetBackup checks the `names_allow.txt` file to determine if the network-host name for the connection correlates to a NetBackup name. If a match is found, the connection is allowed. Otherwise, NetBackup checks the `names_deny.txt` file.

If NetBackup client and server names correlate to their host names and IP addresses, then neither `names_allow.txt` file or `names_deny.txt` are used.

Each line in `names_allow.txt` contains a logical name (usually, a NetBackup client name) followed by a colon and then a list of host names or IP addresses.

Example names_allow.txt File

```
# The next three client entries can match IP numbers in the
# 123.123.56 network.
client1 : 123.123.56.
client2 : 123.123.56.
client3 : 123.123.56.
#
# The entry below permits the name fred to be used for hosts
# dhcp0 and dhcp1 in the ourcompany.com domain.
```

```
fred : dhcp0.ourcompany.com, dhcp1.ourcompany.com
```

The default file is empty.

Syntax Rules for names_allow.txt

The syntax rules for `names_allow.txt` are the same as for `methods_allow.txt`. The only variation is the `ALL` keyword, which in this case specifies all valid names or all possible hosts. (See “Syntax rules for methods.txt” on page 373.)

names_deny.txt

The `names_deny.txt` file defines the NetBackup client or server names that hosts cannot use. NetBackup checks this file only if the `names_allow.txt` file does not have a matching entry for the host and name. If a matching entry is found in `names_deny.txt` the name is not allowed and authentication fails. Otherwise, the name is used and authentication proceeds.

Example names_deny.txt File

```
# The entry below prevents the name fred to be used for hosts
# in the theircompany.com domain.
fred : .theircompany.com
#
# The entry below prevents any names from being used for hosts
# with IP addresses in the 12.123.53 network.
ALL : 123.123.53.
```

The default file contains only the following entry:

```
ALL : ALL
```

This means that all names are denied for all hosts, unless it is specified otherwise in the `names_allow.txt` file.

Syntax Rules for names_deny.txt

The syntax rules for `names_deny.txt` are the same as for `names_allow.txt` (See “Example names_allow.txt File” on page 375.)

authorize.txt

The `authorize.txt` file is created when a user is added to the list of authorized users. (See “To create a list of authorized users” on page 395.)

File Location of authorize.txt

Platform	Path
UNIX	`/usr/openv/var/authorize.txt`
Windows NT/2000	*install_path*`\NetBackup\var\authorize.txt`

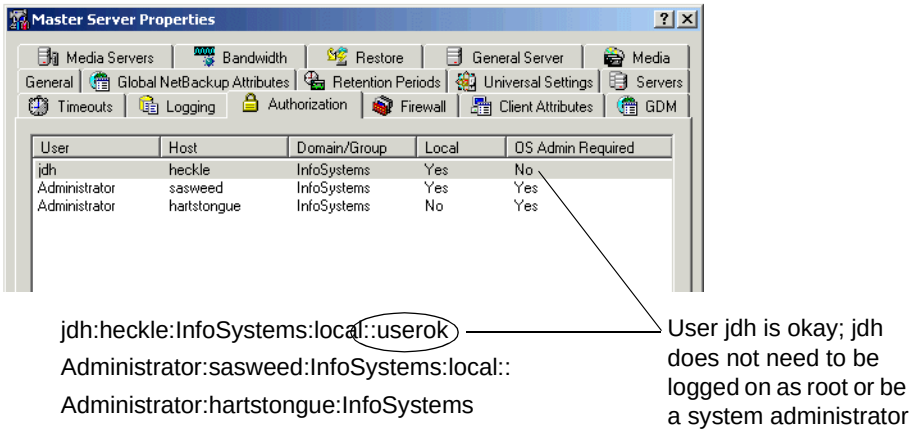
authorize.txt File Format

Use the following format for authorization entries in the `authorize.txt` file:

host_name`:`*user_name*`:`*domain_group_name*`[:local[operator:][userok]]]]`

The figure below compares Authorization property tab entries with the corresponding `authorize.txt` file.

Comparing Authorization Property Tab Entries and authorize.txt Entries



If the NetBackup Administration Console is UNIX:

- *host_name* is the remote NetBackup Administration Console name, or * for all hosts.
- *user_name* is the UNIX user name, or * for all users.
- *domain_group_name* is a netgroup name or a local group name, or * for all groups. For information about netgroups refer to the `netgroup` man page.

- `local` (if specified) indicates that the *domain_group_name* is a local group name.
- `operator` is not in use for this release.
- `userok` (if specified) indicates that the user does not need to be an OS administrator.

Use * in the *user_name* and *host_name* fields to authorize all users and/or hosts. For comments, use a # symbol.

If the NetBackup Administration Console is Windows:

- *user_name* is the Windows Administrator name, or * for all users.
- *host_name* is the remote NetBackup Administrative console host name, or * for all hosts.
- *domain_group_name* is the Windows domain and group name in the form *domain\group.* Or, use * to indicate all domains/groups.
- `local` (if specified) indicates the group is not a domain group, but is local to the host specified by *host_name*.
- `operator` is not in use for this release.
- `userok` (if specified) indicates that the user does not need to be an OS administrator.

For comments, use a # symbol.

Example authorize.txt File Entries

```
# Authorize 'root' with a local group name
# of 'admin' on the UNIX server
root:dog:admin:local
#
# Authorize all NT Administrators that are
#members of NETBACKUP\Domain Admins
*:*:NETBACKUP\Domain Admins
```

Library Files

The library files that are required for authentication depend on the platform. (See "methods.txt" on page 372.)

Commands

The following commands are used to configure and manage authentication. For more information on these commands, see Appendix A.

bpauthorize

Use `bpauthorize` to manage the `authorize.txt` files on remote machines for enhanced authorization. Or, make changes in the NetBackup Administration Console of the master server. (See “To create a list of authorized users” on page 395.)

bpauthsync

Run `bpauthsync` on the master server to set up enhanced authentication for one or more clients. `bpauthsync` ensures that the hashed and unhashed files contain the correct information.

Location of bpauthsync and bpauthorize commands

Platform	Path
UNIX	`/usr/openv/netbackup/bin/admincmd/`
Windows NT/2000	*install_path*`\NetBackup\bin\admincmd\`

vopie_util

Run on the client to manage the `hashed` and `unhashed` files. `vopie_util` generates the secret key for the local system and also the information that must be placed into the `hashed` file on systems that want to access this one.

Location of vopied_util command

Platform	Path
UNIX	`/usr/openv/bin/`
Windows NT/2000	*install_path*`\NetBackup\bin\`

Processes

vopied Daemon

The `vopied` daemon manages the authentication of nonroot users on Windows and UNIX clients and servers. By default, NetBackup configures the system to automatically start `vopied` when the system is started.

To start `vopied` directly, run `vopied` from the following directory on the client or server:

Location of vopied Daemon

Platform	Path
UNIX	`/usr/openv/bin/vopied`
Windows NT/2000	*install_path*`\NetBackup\bin\vopied`

vopie Files

The `vopie` processes use the following files during authentication.

hashed (public key) Files

The `hashed` files contain the authentication challenges that the local system presents to remote systems.

Location of hashed Files

Platform	Path
UNIX	`/usr/openv/var/auth/vopie/hashed/`*localhost*`/`*remotehost*.txt
Windows	*install_path*`\NetBackup\var\auth\vopie\hashed\`*localhost*`\`*remotehost*.txt
MacIntosh	`:System Folder:Preferences:NetBackup:var:auth:vopie:hashed:auth:`*localhost:remotehost*.txt

Where:

- *localhost* is the local system.
- *remotehost* contains the challenges for the remote system named *remotehost*.

There is a *remotehost*`.txt` file for each remote system that can be authenticated. Only root on the local system can read or write these files.

unhashed (secret key) Files

The `unhashed` files contains the secret key that NetBackup uses when it responds to challenges from remote systems.

Location of hashed Files

Platform	Path
UNIX	`/usr/openv/var/auth/vopie/unhashed/`*localhost*`/`*remotehost*.txt
Windows	*Install_path*`\NetBackup\var\auth\vopie\unhashed\`*localhost*`\`*remotehost*`.txt`
MacIntosh	`:System Folder:Preferences:NetBackup:var:auth:vopie:unhashed:auth:`*localhost*:*remotehost*.txt

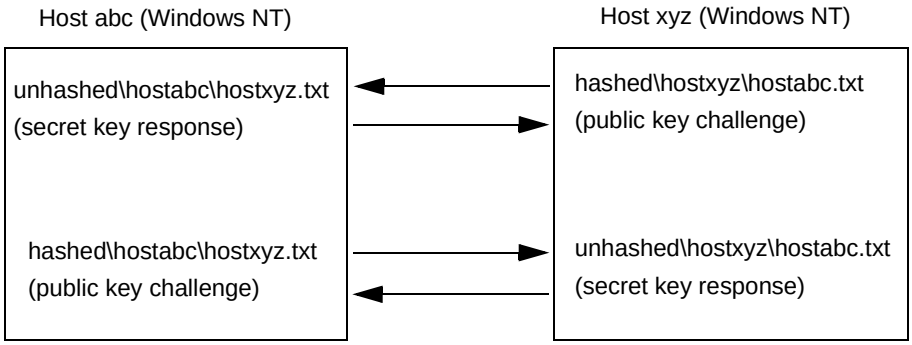
Where:

- *localhost* is the local system.
- *remotehost*.txt contains the responses for the remote system named *remotehost*.

There is a *remotehost*.`txt` file for each remote system that can request authentication. These files are created during installation and only root on the local system can read or write these files.

Caution Protect the `unhashed` files by allowing access only by the administrator on the local system. Also, do not NFS mount them on UNIX or place them on a network drive on Windows.

The `bpauthsync` command synchronizes the information between the `hashed` files on the local host with the `unhashed` files on remote systems. This enables the remote host to offer the correct response when it is challenged. The following figure illustrates this exchange between Windows NT systems.



temp File

On a Windows or UNIX system, the `vopie` daemon, `vopied`, creates a temporary file where it stores the challenges and responses required to authenticate nonroot users. This is necessary because nonroot users cannot access the files in the `hashed` and `unhashed` directories. The temporary files are valid for only one connection and are automatically deleted.

Location of Temporary Files

Platform	Path
UNIX	`/usr/openv/var/auth/vopie/temp/`*username*`/`*tempname*.txt
Windows	*install_path*`\NetBackup\var\auth\vopie\temp\`*username*`\`*tempname*.txt

Enhanced Authentication

The standard authentication that NetBackup uses is based on the network address of the connecting machine. NetBackup trusts that the connecting machine is who it says it is.

Enhanced authentication is additional authentication for NetBackup programs that communicate through sockets. It allows each side of a NetBackup connection to verify the host and user on the other side of the connection, taking place after a NetBackup connection has been established, but before any NetBackup transactions have taken place. For example, enhanced authentication could be enforced when a backup or restore operation is started from a client or during remote administration.

Enhanced authentication is performed through a series of challenge and responses that require the exchange of secret password information. Passwords are defined during installation and configuration so users do not have to enter passwords each time they start a backup, archive, or restore.

Note Enhanced authentication can be used without enhanced authorization.

There are two supported enhanced authentication methods:

- `vopie` – (VERITAS One-time Passwords In Everything)
  The `vopie` method authenticates user name, host names, and group / domain names.
- `noauth` authentication – (“No authorization” authorization)
  The `noauth` method exchanges user name, host names, and group / domain names, but makes no attempt to verify that the information is correct.

Using vopie Enhanced Authentication

`vopie` authenticates at two levels:

- At the host level – The hosts authenticate one another.
- At the user level – If the user attempting the connection is a non-root user on UNIX or a non-administrator on Windows, the user is authenticated as well.

▼ To use the vopie enhanced authentication method

1. Install NetBackup on each system requiring authentication.

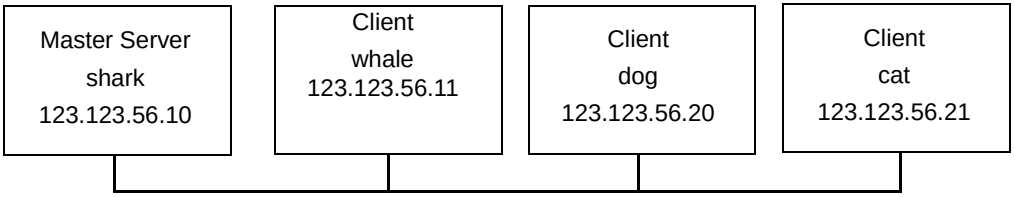
   The NetBackup install process installs the necessary files and commands. The administrator then uses commands to set up the files so they contain the proper authentication information.

2. Run:
   install_path`\NetBackup\bin\admincmd\bpauthsync` on the master server. (See“vopie Enhanced Authentication Examples” on page 384 to determine which options to use.)

   `bpauthsync` sets up authentication files on the NetBackup server and clients. (See “bpauthsync” on page 435.)

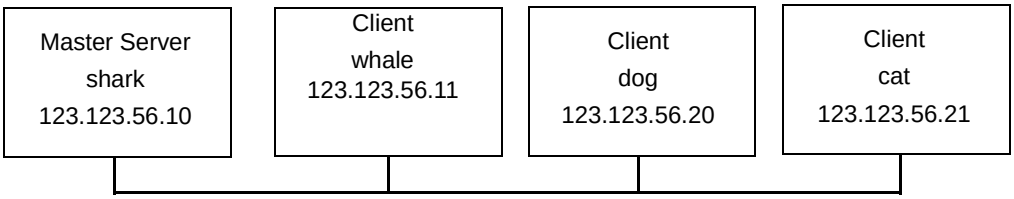
vopie Enhanced Authentication Examples

The examples in this section are based on the following configuration:



vopie Example 1: Typical Configuration

Assume that this is an initial installation and you want to configure `vopie` authentication for all systems in the figure below. NetBackup server and client software has already been installed.



1. Run the following command on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -vopie -servers -clients`

   This synchronizes the key files on all the systems.

2. On the master server, copy the `methods_allow.txt` to a temporary file. For example, `C:\tmp\ma.txt`.

3. To the temporary file, add an entry for each host that requires authentication:

```
vopie : shark
vopie : whale
vopie : dog
vopie : cat
```

4. Synchronize the `methods_allow.txt` files on the server and the clients by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -methods -methods_allow C:\tmp\ma.txt -servers -clients`

   The information in `C:\tmp\ma.txt` is written in the `methods_allow.txt` files on the servers and clients.

vopie Example 2: Disable Authentication for a Client

To disable authentication for client cat in the previous figure:

1. Push an empty `methods_allow.txt` file to the client by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -methods -methods_allow /dev/null -clients cat`

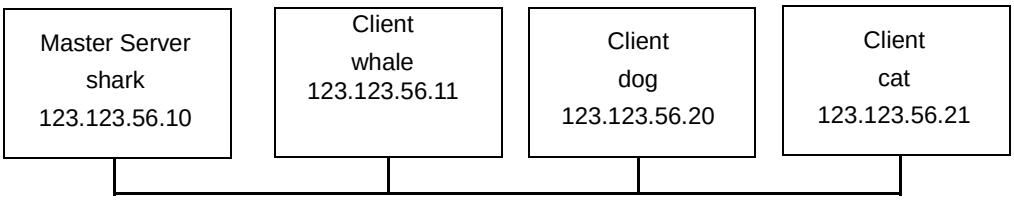
   This disables authentication on the client.

2. On the master server, remove the entry for cat from the *install_path*`\NetBackup\var\auth\methods_allow.txt` file.

   Authentication is no longer performed when communicating with this client.

vopie Example 3: Adding a Client

Assume that all systems below are configured for authentication, except for client cat.



To add authentication for client cat:

1. On the master server, copy the `methods_allow.txt` to a temporary file. For example, .

2. Add an entry for the new client to the temporary file:

   ```
   vopie : cat
   ```

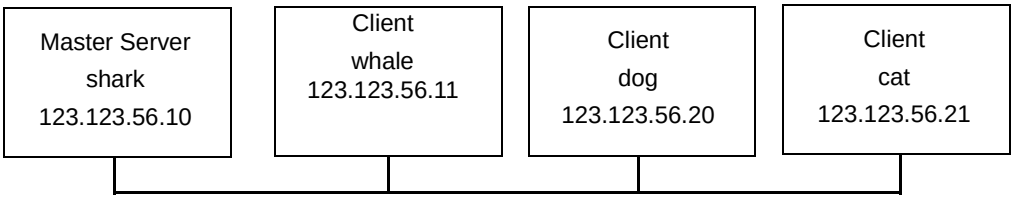
3. Synchronize the methods files on the server and the new client by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -vopie -methods -methods_allow C:\tmp\ma.txt -servers -clients cat`

   The information in is written in the `methods_allow.txt` files on the server and the client.

vopie Example 4: Restoring Authentication After Client Disk Crash

Assume that cat was configured for authentication and the disk failed.



To restore authentication so all files can be recovered:

1. On the master server, copy the current `methods_allow.txt` file to another file. For example, copy it to `C:\`*install_path*`\NetBackup\var\auth\methods_allow.txt.save`

2. Remove the entry for the failed client from `methods_allow.txt` on the master server.

   This disables authentication for the failed client so the servers can communicate with it during recovery.

3. Reinstall the operating system (Windows 2000, NT, or UNIX) and NetBackup on the failed client by following the instructions in the *Troubleshooting Guide*. However, do not restore any NetBackup or user files at this time.

4. On the master server, run the following command to synchronize and push the original methods to the failed client. The command is on two lines:

install_path`\NetBackup\bin\admincmd\bpauthsync -vopie -methods -servers -clients cat -methods_allow`

install_path`\NetBackup\var\auth\methods_allow.txt.save`

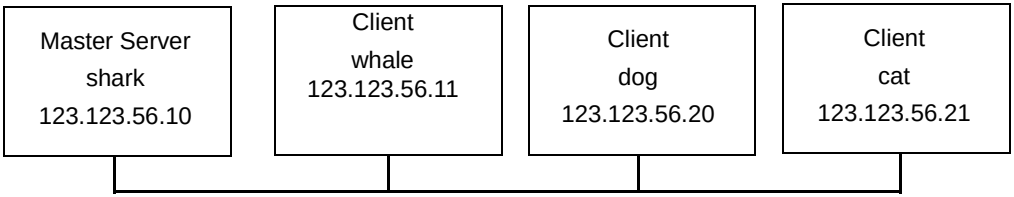
The information in `methods_allow.txt.save` is written in the `methods_allow.txt` files on the client. The original authentication methods are now restored.

Note Do not restore the files in the *install_path*`\NetBackup\var\auth` directory on the client or authentication will have to be resynchronized.

5. Complete the client recovery by restoring the original NetBackup and user files as explained in the *NetBackup Troubleshooting Guide for Windows*.

vopie Example 5: Restoring Authentication on NetBackup Server

Assume that authentication was configured on all servers and clients and the disk fails on the master server shark.



If the NetBackup catalog backup was written to a storage unit on the master server shark:

1. On the master server, recover the disk as explained in *NetBackup Troubleshooting Guide for Windows* and reinstall NetBackup.

2. Restore all files to the master server.

3. Synchronize all clients and servers by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -vopie -servers -clients`

Using noauth Rather than vopie Authentication

The `noauth` method exchanges user name, host names, and group / domain names, but makes no attempt to verify that the information is correct.

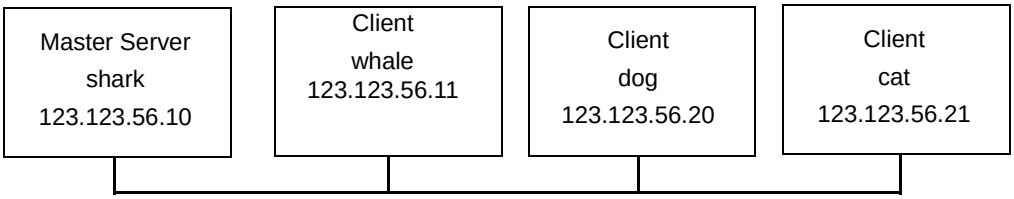
Configuring for the `noauth` method is similar to configuring for the `vopie` method with these exceptions:

- Do not run the `bpauthsync` command with the `-vopie` argument
- Use string `noauth` instead of `vopie` in the `methods_allow.txt` file

Note The `noauth` method is not supported for Sequent systems.

noauth Authentication Examples

The examples in this section are based on the following configuration:



noauth Example 1: Typical Configuration

Assume that this is an initial installation and you want to configure authentication for all systems. NetBackup server and client software has already been installed.

1. On the master server, copy the `methods_allow.txt` to a temporary file. For example, `C:\tmp\ma.txt`.

2. To the temporary file, add an entry for each host that requires `noauth` authentication:

```
noauth : shark
noauth : whale
noauth : dog
noauth : cat
```

3. Synchronize the `methods_allow.txt` files on the server and the clients by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -methods -methods_allow C:\tmp\ma.txt -servers -clients`

   The information in `C:\tmp\ma.txt` is written to `methods_allow.txt` on the servers and clients.

noauth Example 2: Authentication for a Client

To disable authentication for client cat:

1. Push an empty `methods_allow.txt` file to the client by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -methods -methods_allow /dev/null -clients cat`

   This disables authentication on the client.

2. On the master server, remove the entry for cat from the *install_path*`\NetBackup\var\auth\methods_allow.txt` file.

   Authentication is no longer performed when communicating with this client.

noauth Example 3: Adding a Client

Assume that all systems are configured for authentication, except for client cat.

To add authentication for client cat:

1. On the master server, copy the `methods_allow.txt` to a temporary file. For example, `C:\tmp\ma.txt`.

2. Add an entry for the new client to the temporary file:

   ```
   noauth : cat
   ```

3. Synchronize the `methods_allow.txt` files on the server and the new client by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -methods -methods_allow.txt C:\tmp\ma.txt -servers -clients cat`

   The information in `C:\tmp\ma.txt` is written to `methods_allow.txt` files on the server and the client.

noauth Example 4: Restoring Authentication After Client Disk Crash

Assume that client cat was configured for authentication and the disk failed.

To restore authentication so all files can be recovered:

1. On the master server, copy the current `methods_allow.txt` file to another file. For example, copy it to
   `C:\`*install_path*`\NetBackup\var\auth\methods_allow.txt.save`

2. Remove the entry for the failed client from `methods_allow.txt` on the master server.

   This disables authentication for the failed client so the servers can communicate with it during recovery.

3. Reinstall the operating system (Windows 2000, NT, or UNIX) and NetBackup on the failed client by following the instructions in the *NetBackup Troubleshooting Guide - Windows*. However, do not restore any NetBackup or user files at this time.

4. On the master server, run the following command to push the original methods to the failed client (the command is all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -methods -servers -clients cat -methods_allow`
   install_path`\NetBackup\var\auth\methods_allow.txt.save`

   The information in `methods_allow.txt.save` is written in `methods_allow.txt` on the the client. The original authentication methods are restored.

5. Complete the client recovery by restoring the original NetBackup and user files as explained in the *NetBackup Troubleshooting Guide - Windows*.

noauth Example 5: Restoring Authentication on NetBackup Server

Assume that authentication was configured on all servers and clients and the disk fails on master server shark.

If the NetBackup catalog backup was written to a storage unit on the master server shark:

1. On the master server, recover the disk as explained in the *NetBackup Troubleshooting Guide for Windows* and reinstall NetBackup.

2. Restore all files to the master server.

3. Synchronize all clients and servers by running the following on the master server (all on one line):

   install_path`\NetBackup\bin\admincmd\bpauthsync -servers -clients`

Troubleshooting Authentication

If you have problems with authentication, perform the following steps:

1. Look for status code 160 (authentication failed). If you see this status code, go to the *NetBackup Troubleshooting Guide for Windows* for corrective actions.

2. Create debug log directories for the processes involved in communication between NetBackup systems. These include:
   - On the server, create debug log directories for `bprd`, `bpdbm`, `bpcd`.
   - On the client, create debug log directories for `bpcd`, `bpbackup`, `bprestore`, `bplist`.

3. Retry the operation and check the logs.

Enhanced Authorization

The standard authorization that NetBackup runs is based on listing the connecting server in the server list, and the user having root or administrator privileges.

Enhanced authorization provides a platform-independent mechanism for selected users (or groups of users) to administer a NetBackup server from a remote NetBackup Administration Console.

The user(s) can be given privileges to act as a NetBackup administrator, while not having system administrator or UNIX root privileges. Using enhanced authorization, a user can be given the following roles:

- NetBackup administrator on a NetBackup server with administration privileges
- Non-administrator with no administrative privileges

Note Enhanced authorization can only be used with enhanced authentication.

Enhanced Authorization Process

The following describes the flow for a request from a remote NetBackup Administration Console to a NetBackup master server.

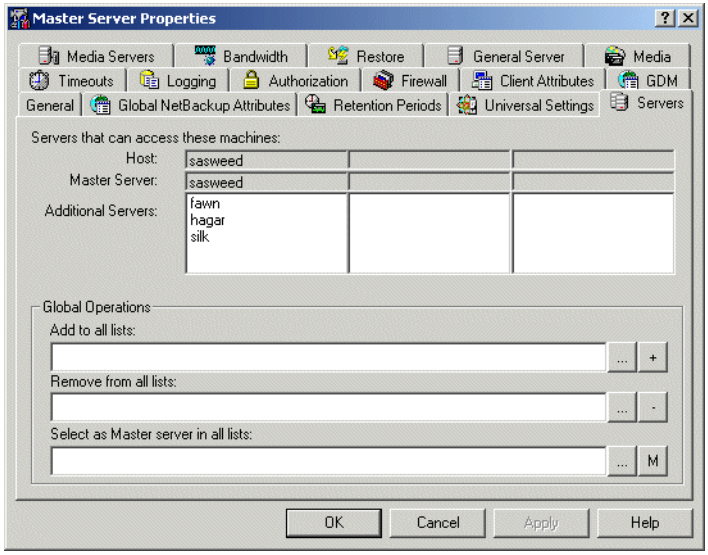
Gaining Access to a Server

When an administrator on a remote NetBackup Administration Console makes a request to a NetBackup server, and enhanced authentication is enabled between the two systems, the *user_name*, *host_name*, *domain_group_name*, and `local` flag are passed from the requesting NetBackup Administration Console to the NetBackup master server accepting the request.

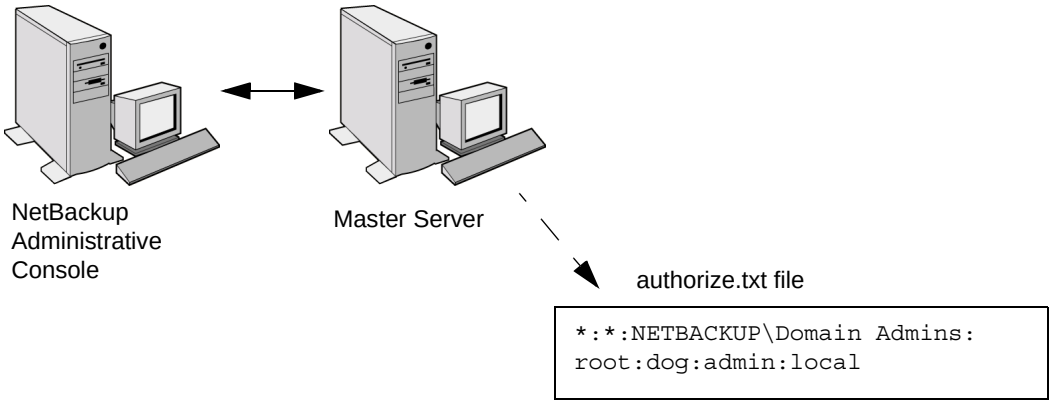
After passing authentication, the accepting NetBackup master server checks for the existence of the `authorize.txt` file and for an entry in the file that matches the information passed by requester.

If a match exists, the request is authorized (allowed). If the request is not authorized, the request can proceed only if the NetBackup Administrative Console making the request contains:

- On UNIX servers:
  `SERVER =` *server_name* entry in the `bp.conf` file of the accepting server.
- On Windows servers: The server must be among those listed under **Servers that can access these machines** on the **Servers** properties tab, as shown below. (See "Servers Tab" on page 254.):



If the server name is not in the server list, the request fails, indicating a `request from invalid server`. You also need an entry in the `vm.conf` file in order to use Media Manager applications (see the *Media Manager System Administrator's Guide*).

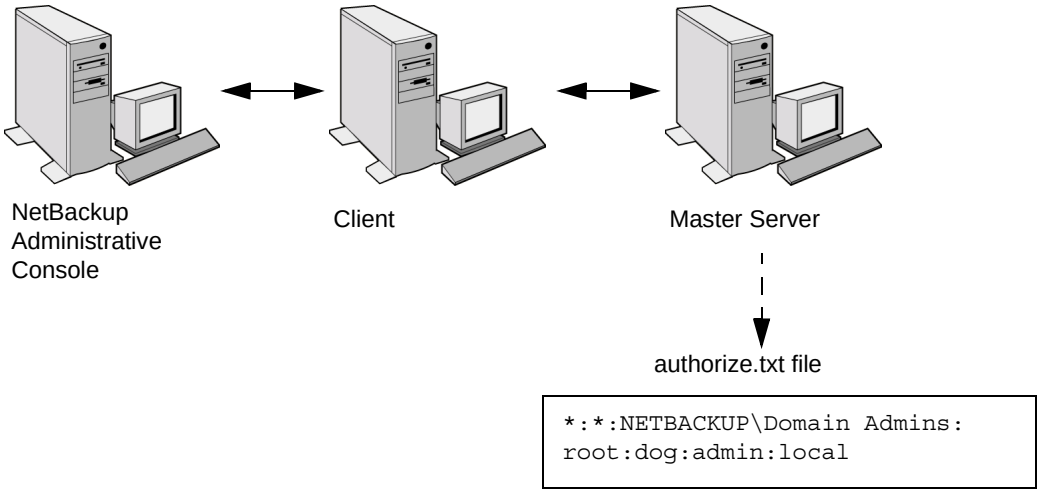


Gaining Access to a Client

Some requests, such as client configuration, are made directly to a client. These types of requests do not require an `authorize.txt` file on the client. The following describes the flow for a request from a remote NetBackup Administration Console to a NetBackup client.

When an administrator on a remote NetBackup Administration Console makes a request to a NetBackup client, and enhanced authentication is enabled between the two systems, the *user_name*, *host_name*, *domain_group_name*, and `local` flag are passed from the requesting NetBackup Administrative Console to the NetBackup client accepting the request.

If the requesting NetBackup Administration Console is not in the client's server list, the client requests authorization from its master server (the first server listed in the server list). The NetBackup Administrative Console authorization information is passed to the master server. The master server checks for the existence of the `authorize.txt` file and for an entry in the file that matches the information passed. If a match exists, authorization is granted, otherwise authorization is denied.



Configuring NetBackup Enhanced Authorization

The process of configuring NetBackup enhanced authorization can be broken down into four steps:

1. Add NetBackup servers to one another's server lists. (See "Adding a NetBackup Server to a Server List" on page 320.)

2. Enable NetBackup authentication. (See "Enabling NetBackup Enhanced Authentication" on page 394.)

3. Add an authorized user (creating an `authorize.txt` file). (See "Adding an Authorized User" on page 395.)

4. Optionally, specify the preferred group. (See "Using the Administrative Console to Specify Preferred Groups (optional)" on page 396.)

Enabling NetBackup Enhanced Authentication

To use enhanced authorization, enable NetBackup enhanced authentication between NetBackup Administration Consoles and the NetBackup servers to be administered. To perform administrative tasks on clients, such as client configuration, you must also enable NetBackup enhanced authentication between the clients and NetBackup Administration Consoles.

For more on authentication, see:

- "Configuring NetBackup Enhanced Authorization" on page 394
- "vmd Security" in the *Media Manager System Administrator's Guide.*

Adding an Authorized User

To enable enhanced authorization, create a list of authorized users.

▼ To create a list of authorized users

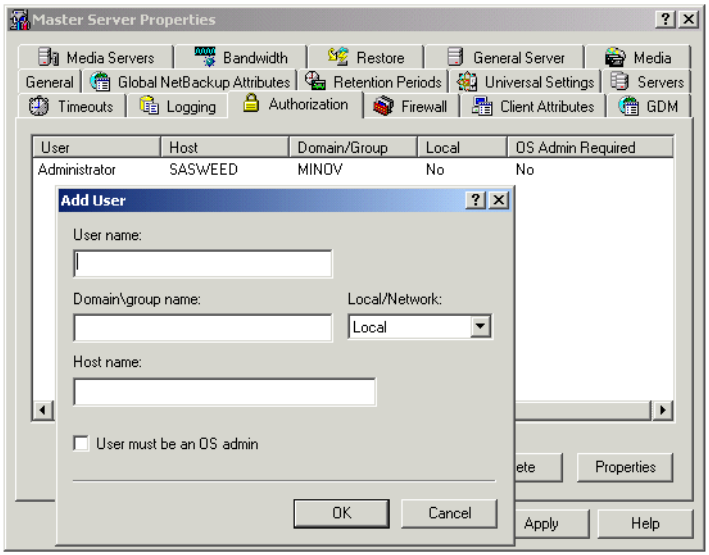
1. Expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server** (or **Media Servers**).

2. Double-click the Master or Media server where you'd like to add the authorized user.

3. In the **Properties** dialog, click the **Authorization** tab.

4. Click **New**. The **Add User** dialog appears.

5. Type the user name that will have access to this server. To allow any user, type: *



6. Type the domain or group name to which the user belongs. To allow any domain group, type: *

7. Select whether the domain is local or on a network.

8. Type the host name that will be accessing the selected master or media server. To allow any host, type: *

9. Select to allow users onto the machine to administrate NetBackup who are not system administrators or logged on as UNIX root.

10. Click **OK**.

Upon the addition of the first user to the list of authorized users, the `authorize.txt` is created. After the creation of `authorize.txt`, the server requires authorization from any NetBackup Administration Console that attempts remote administration.

Using the Administrative Console to Specify Preferred Groups (optional)

You can specify a preferred group of administrative users in the NetBackup Administrative Console. The preferred group entry is intended specifically for use with NetBackup enhanced authorization and determines the *domain_group_name* that is sent to the NetBackup server.

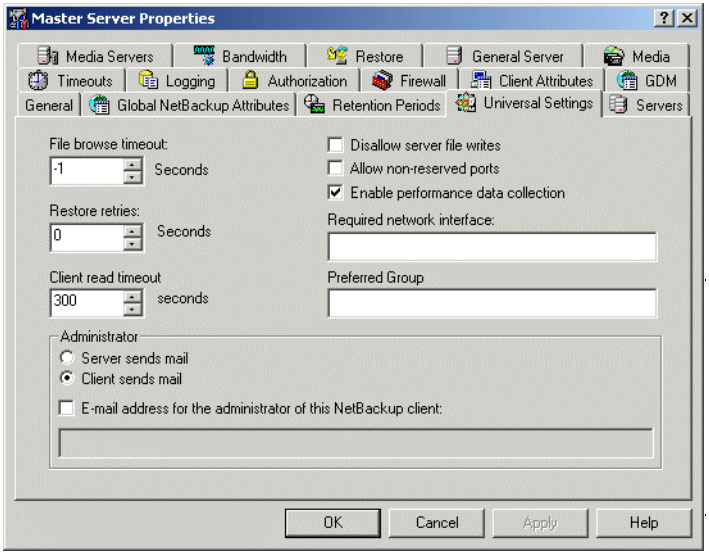
Some NetBackup processes also use the preferred group entry for Media Manager authorization. For more information on this, see "Media Manager Configuration File (vm.conf)" in the *NetBackup Media Manager System Administrator's Guide*.

▼ To specify a preferred group

1. Expand **Master Server** > **NetBackup Management** > **Host Properties** > **Master Server** (or **Media Servers**).

2. Double-click the Master or Media server where you'd like to specify a preferred group.

3. In the **Properties** dialog, select the **Universal Settings** tab.



Note To facilitate a platform-independent implementation, the string in the preferred group entry is case sensitive for both UNIX and Windows.

Adding a **Preferred Group** in the NetBackup Administration Console has the following effect on UNIX and Windows systems.

On UNIX

The `PREFERRED_GROUP` entry is added to the `bp.conf` file:

`PREFERRED_GROUP =` *netgroup name*

- If the `bp.conf` configuration file has a `PREFERRED_GROUP` entry, the `innetgr()` function is used to determine if the user is in the netgroup (for further details refer to the `innetgr` man page).
- If the `PREFERRED_GROUP` entry does not exist or the user is not a member of the netgroup, the local group name is obtained.

Note Netgroups are not supported for Sequent systems.

On Windows

The PREFERRED_GROUP NetBackup configuration is added to the KEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config registry key.

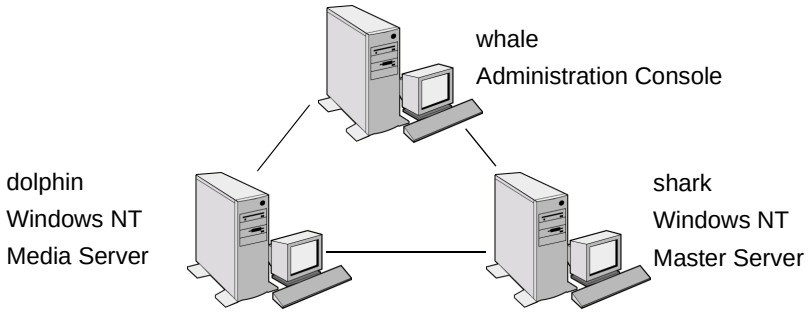
A check is made to determine if the user is a member of domain\group. This check is limited to NT global groups. In other words, if PREFERRED_GROUP is set to a domain local group, a match will not occur and the user's primary domain\group will be used.

If the PREFERRED_GROUP configuration option does not exist or the user is not a member of the domain\group, the user's primary domain\group is obtained. When the domain name is an empty string or is the name of the local machine, it is considered to be local.

4. Click **OK**.

Example Configuration

The following explains how to set up NetBackup enhanced authorization between the computers in the figure below.



1. Update the server lists and `vm.conf` files as follows:
   - On shark, add dolphin to the server list and `vm.conf` file.
   - On dolphin, add shark to the server list and `vm.conf` file.
   - On whale, add shark and dolphin to the server list.
2. Enable NetBackup enhanced authentication:
   a. On shark, run:

      ```
      bpauthsync -vopie -servers shark dolphin whale
      ```

   b. On shark, create a temporary file (`C:\tmp_file`) with the following values:

      ```
      vopie: shark
      vopie: dolphin
      vopie: whale
      ```

   c. On shark, run (all on one line):

      ```
      bpauthsync -methods_allow c:\tmp_file -servers shark dolphin
      whale
      ```

3. Create a global network group named:

   `MYDOMAIN\NetBackup Admins`

   Someone logging in as a member of this group will be able to be a NetBackup administrator.
4. Edit the `authorize.txt` files on shark and dolphin so they contain:

   `*:*:MYDOMAIN\NetBackup Admins`
5. On whale, set the preferred group to:

```
MYDOMAIN\NetBackup Admins
```

Additional Configuration 10

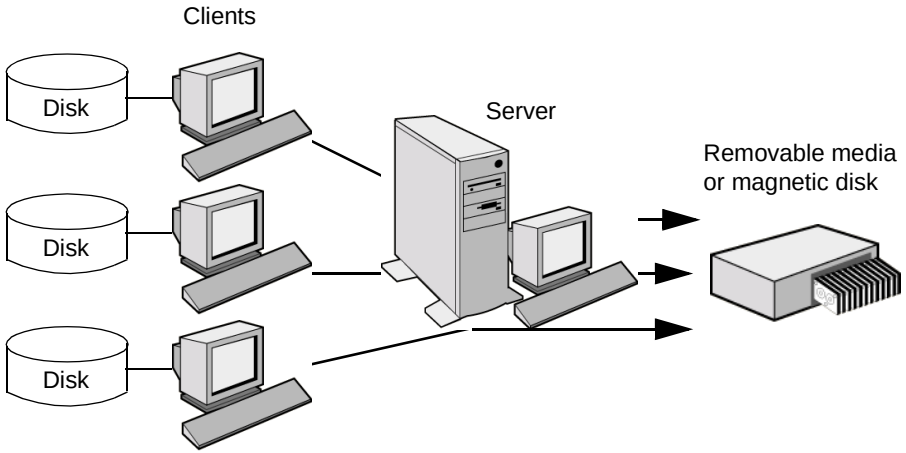
The previous chapters describe the setup that you must complete for all installations. This chapter explains settings that in many instances are optional either because the default is appropriate or a site does not use the feature. The topics included here are:

- Multiplexing
- Using Multiple NetBackup Servers
- Dynamic Host Name and IP Addressing
- Bandwidth Limiting
- Specifying the Locale of the NetBackup Installation

Multiplexing

NetBackup multiplexing sends concurrent backups from one or several clients to a single storage device (see figure below). NetBackup multiplexes the backups sequentially onto the media. Multiplexed and unmultiplexed backups can reside on the same volume. It is not necessary to create separate volume pools or media IDs.

No special action is required to restore a multiplexed backup. NetBackup finds the media and restores the requested backup.



When to Use Multiplexing

Multiplexing is generally used to reduce the amount of time required to complete backups. The following are situations where multiplexing can improve backup performance.

- Slow clients. This includes instances where NetBackup is using software compression, which normally reduces client performance.
- Multiple slow networks. The parallel data streams take advantage of whatever network capacity is available.
- Many short backups (for example, incrementals). In addition to providing parallel data streams, multiplexing reduces the time each job spends waiting for a device to become available, and therefore better utilizes the transfer rate of storage devices.

Multiplexing reduces performance on restores because it uses extra time to read the images.

Note To reduce the impact of multiplexing on restore times, set maximum fragment size for the storage units to a value other than zero.

How to Configure Multiplexing

Multiplexing must be set in two places in the NetBackup configuration:

- Storage unit
- Schedule

Note If you change these values, it does not take effect until the next time a schedule runs.

Maximum Multiplexing Per Drive for Storage Unit

The **Maximum Multiplexing Per Drive** setting for a storage unit specifies how many backups NetBackup can multiplex onto any single drive in the storage unit. You set this value for each storage unit. (See "Maximum Multiplexing per Drive" on page 32.) The number can range from 1 through 8, where 1 is the default and specifies no multiplexing.

Choose a value based on the ability of your central processing unit to handle parallel jobs. Because extra buffers are required, memory is also important. If the server cannot perform other tasks or runs out of memory or processes, reduce the **Maximum Multiplexing Per Drive** setting for the storage unit. Consider the following when estimating the load that multiplexing can potentially put on your central processing unit:

- The maximum number of concurrent-backup jobs that NetBackup is allowed to attempt, is equal to the sum of the concurrent-backup jobs that can run on the storage units.
- The maximum number of concurrent-backup jobs that can run on a single storage unit is equal to the Maximum Multiplexing per drive by the number of drives.

Media Multiplexing for a Schedule

In addition to the **Maximum Multiplexing Per Drive** setting for a storage unit, you specify a **Media Multiplexing** value for each schedule. (See "Media Multiplexing" on page 117.) This setting specifies the maximum number of backups from the schedule that you can multiplex onto any single drive in the configuration.

The Media multiplexing setting can range from 1 through 8, where 1 is the default and specifies no multiplexing. Regardless of the setting on a schedule, the maximum jobs that NetBackup starts never exceeds the storage unit's **Maximum Multiplexing Per Drive**. When adding jobs to drives, NetBackup attempts to add multiplex jobs to drives that are already using multiplexing. This leaves other drives available for non-multiplex jobs.

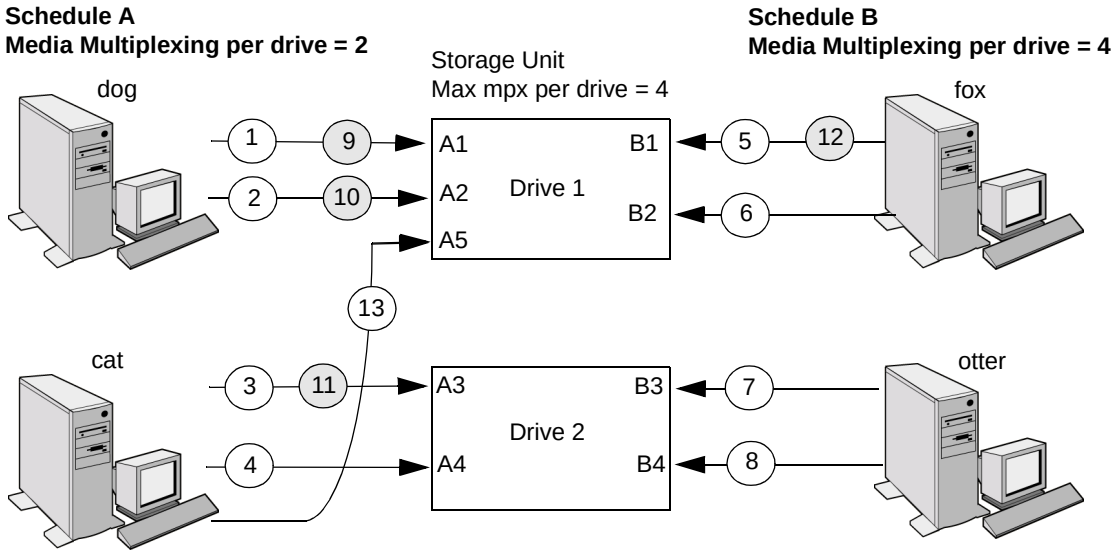
When NetBackup multiplexes jobs, it continues to add jobs to a drive until the number of jobs on the drive matches either of the following:

- This schedule's **Media Multiplexing** setting.

  If the limit is reached for a drive, NetBackup starts sending jobs to another drive. In the following figure, when the Schedule A limit is reached on Drive 1, NetBackup starts adding Schedule A jobs to Drive 2.

- The storage unit's **Maximum multiplexing per drive** setting. NetBackup can add jobs from more than one schedule to a drive.

  In the following figure, unshaded numbers denote job starting. Shaded numbers denote job completion. For example, ① denotes the start of job A1 on Drive 1. ⑨ denotes the completion of job A1 on Drive 1.



Assume schedule A begins first (note that the schedules can be in the same or different policies). Also, assume that Allow Multiple Data Streams is enabled, so a client can have multiple data streams.

(1)(2) Jobs A1 and A2 from client dog start on drive 1. Schedule A Media Multiplexing limit of 2 is reached for this drive.

(3)(4) Jobs A3 and A4 from client cat start on drive 2. Schedule A Media Multiplexing limit of 2 is reached for this drive.

(5)(6) Jobs B1 and B2 for client fox start on drive 1. Storage unit max mpx is reached for this drive.

(7)(8) Jobs B3 and B4 from client otter start on drive 2. All jobs are now running for schedule B. Storage Unit Max mpx is reached for drive 2.

(9)(10) Jobs A1 and A2 from client dog finish on drive 1. However, jobs B1 and B2 for client fox are still running, so Schedule A Media Multiplexing limit of 2 still prevents job A5 from starting on drive 1.

(11)(12) Job A3 from client cat finishes on drive 2 and job B1 from client fox finishes on drive 1. Job B2 is the only job currently running on drive 1.

(13) Job A5 from client cat starts on drive 1. This is the last job for schedule A. Schedule A Media Multiplexing limit of 2 prevents job A5 from starting on Drive 2. Therefore, job A5 starts on Drive 1. When adding jobs to drives, NetBackup attempts to add multiplex jobs to drives that are already using multiplexing. This leaves other drives available for non-multiplex jobs.

Note If the backup window closes before NetBackup can start all the jobs in a multiplexing set, NetBackup completes only the jobs that have actually started. For example, on the figure above, assume that the Activity Monitor shows A1 through A5 as queued and active. If only A1 and A2 actually start before the window closes, NetBackup does not perform the other jobs that are in the set. If the window closes before any jobs have started, then only the first queued and active job starts and completes. (A1 in this example.)

Other Configuration Settings to Consider Using Multiplexing

Limit Jobs per Policy

Set **Limit Jobs Per Policy** high enough to support the specified level of multiplexing. (See "Limit Jobs Per Policy" on page 62.)

Maximum Jobs per Client

The **Maximum Jobs Per Client** global attribute limits the number of backup jobs that can run concurrently on any NetBackup client. Usually, its setting does not affect multiplexing. However, to illustrate its effect, consider a case where there are jobs from different schedules on the same client and all are going to the same storage unit. In this case, it is possible for the maximum number of jobs permitted on the client to be reached before the multiplexing limit is reached for the storage unit. If this occurs, it prevents NetBackup from fully utilizing the storage unit's multiplexing capabilities.

Maximum Jobs this Client

You can also set the maximum number of jobs that are allowed on a specific client without affecting other clients. (See "Maximum Data Streams" on page 264.)

MPX Restore Delay

The NetBackup configuration option, **Delay On Multiplexed Restores**, applies to multiplexed restores. The option specifies how long (in seconds) the server waits for additional restore requests of files and (or) raw partitions that are in a set of multiplexed images on the same tape. The **Delay On Multiplexed Restores** option appears on the General Server properties dialog.

Demultiplexing

Demultiplexing speeds up future restores and is also useful for creating a copy for off-site storage.

To demultiplex a backup, select **Images** > **Duplicate** in the NetBackup Administration Console. This command lets you copy one multiplexed backup at a time from the source media to the target media. When duplication is complete, the target contains a single demultiplexed copy of each backup you duplicated (the target can also have other backups). If desired, you can make the duplicate copy the primary copy.

Note If you use the `bpduplicate` command instead of the NetBackup Administration Console, do not include the `-mpx` option on that command.

Example

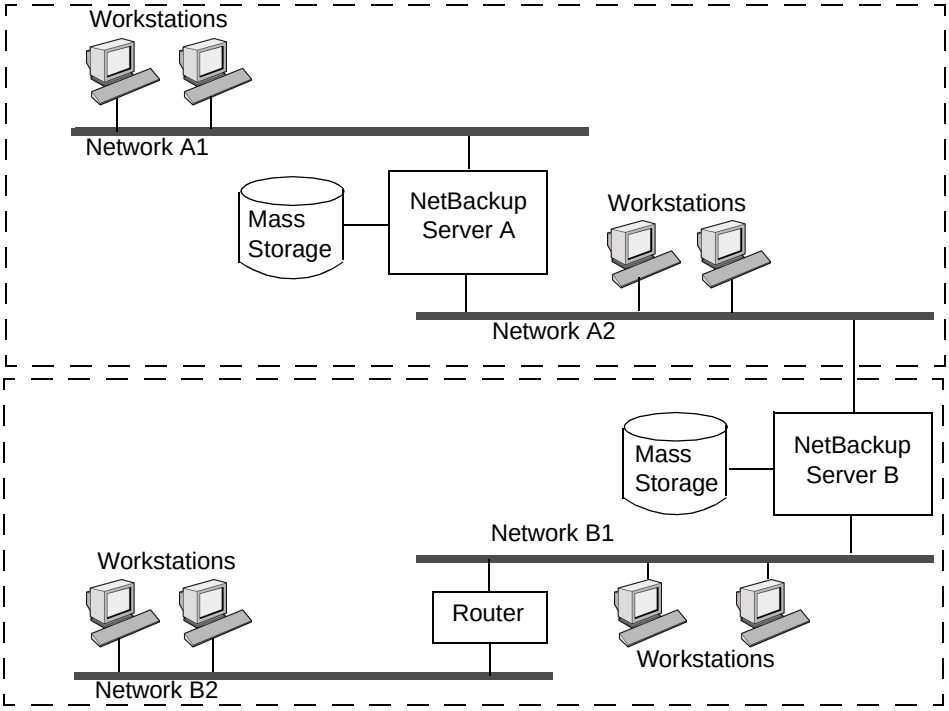
Assume you multiplexed clients A, B, and C to media ID MPX001. This can be done in a single duplicate operation.

The general procedure is as follows.

1. Select the clients and media ID MPX001. Ensure that the date and time range covers the period of the multiplexed backup.
2. Click **Search**. NetBackup lists the backups that were created for the clients on MPX001.
3. Clear the **MPX** box if it is checked. Otherwise the selected backups are duplicated as multiplexed backups and no demultiplexing occurs.
4. In the destination section, click **Images > Duplicate** and select the storage unit and volume pool.
5. Click **Duplicate** and check the progress log for results.

Using Multiple NetBackup Servers

A large site that has more than one master server can divide the clients between the servers as necessary to optimize the backup loads. The figure below shows a multiple-server configuration where the two sets of networks (A1/A2 and B1/B2) each have enough clients to justify separate servers. In this environment, the two NetBackup server configurations are completely independent..



Dynamic Host Name and IP Addressing

By default, a NetBackup server assumes that a NetBackup client name is the same as the network host name of the client machine. This makes it difficult to back up clients that have network host names that might change; examples of this are portable machines that plug into a LAN and obtain IP addresses from a DHCP server or remote machines that dial into a PPP server. NetBackup dynamic host name and IP addressing allows you to define NetBackup clients that do not have fixed IP addresses and host names.

Note If you use dynamic addressing, remember that the NetBackup servers still require fixed IP addresses and host names.

Note All clients configured to use dynamic addressing and host names must trust each other in a way similar to that provided by the NetBackup altnames feature.

The following steps are required to support configurations that use dynamic IP addressing for NetBackup. Read all sections of this topic prior to making any changes to your configuration.

1. Configure your network to use a dynamic IP addressing protocol like DHCP.

   NetBackup requires that IP addresses of clients have a network host name. Be sure to define network host names for the range of dynamic IP addresses in the `hosts` file and (or) DNS on your network.

2. Determine the NetBackup client names for the machines that have dynamic IP addresses and network host names.

   You will use these NetBackup client names in step 3 and step 6 of this procedure. Each NetBackup client must have a unique NetBackup client name. The NetBackup client name assigned to a client is permanent—do not change it.

3. Make changes on the master server:

   a. Create NetBackup policies with client lists that include the names from step 2.

   b. Create entries in the NetBackup client database for the client names from step 2.

      Create the entries by using the `bpclient` command.

4. Make changes on each dynamic NetBackup Windows client:

   a. Start the user interface on the client and click **NetBackup Client Properties** > **Configure**. On the **General** tab of the NetBackup Configuration dialog, change the **Client Name** so it is the correct NetBackup client name for the machine.

   b. In the registry, modify the NetBackup configuration option, `Announce_DHCP_Interval`, so it contains a value other than 0. This option is in the following registry key on the client:

      `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config`

5. Make changes on each dynamic NetBackup Macintosh client:

a. Modify the `bp.conf` file so it includes a `CLIENT_NAME` entry with the correct NetBackup client name for the machine.

b. Modify the `mac.conf` file so it includes a `DYNAMICNOTIFY` entry to periodically notify the NetBackup master server of the machine's NetBackup client name and current network host name.

6. Make changes on each dynamic NetBackup UNIX client:

a. Modify the `bp.conf` file to include a `CLIENT_NAME` entry with the correct NetBackup client name for the machine.

b. Configure the system to notify the master server of the machine's NetBackup client name and current network host name during startup. The `bpdynamicclient` command is used to notify the master server.

c. Configure the system to periodically notify the master server of the machine's NetBackup client name and current network host name.

Setting up Dynamic IP Addresses and Host Names

Configure your network to use a dynamic IP addressing protocol. A protocol like DHCP will have a server and several clients. For example, when a DHCP client starts up, it requests an IP address from the DHCP server. The server then assigns an IP address to the client from a range of predefined addresses.

NetBackup requires that the IP addresses of NetBackup clients have corresponding network host names. Ensure that each IP address that could be assigned to NetBackup clients has a network host name defined in the `host` file, NIS, and (or) DNS on your network.

As an example, suppose that you have 10 dynamic IP addresses and host names available. The dynamic IP addresses and host names might be:

```
123.123.123.70 dynamic00
123.123.123.71 dynamic01
123.123.123.72 dynamic02
123.123.123.72 dynamic03
.
.
.
123.123.123.79 dynamic09
```

Assign a unique NetBackup client name to each NetBackup client that might use one of these dynamic IP addresses. The NetBackup client name assigned to a client is permanent and should not be changed. The client name assigned to NetBackup clients with dynamic

IP addressing must not be the same as any network host names on your network. If the NetBackup client names are changed or are not unique, backup and restore results are unpredictable.

For example, suppose you have four machines that will share the IP addresses defined above. If you want these machines to be NetBackup clients, you might assign them these NetBackup client names as follows:

```
nbclient01
nbclient02
nbclient03
nbclient04
```

Configuring the NetBackup Server

On the master server, create your NetBackup backup policies as you would otherwise. For client name lists, use the NetBackup client names (for example, nbclient01) rather than the dynamic network host names (for example, `dynamic01`).

Next, create the client database on the master server. The client database consists of directories and files in the following directory:

install_path`\NetBackup\db\client`

You can create, update, list, and delete client entries with the `bpclient` command. The `bpclient` command is in the following directory:

install_path`\NetBackup\bin\admincmd`

- To create a dynamic client entry:

  `bpclient.exe -add -client` *client_name* `-dynamic_address 1`

  where *client_name* is the NetBackup client name. The `-dynamic_address 1` argument indicates that the client uses dynamic IP addressing. You can create entries with `-dynamic_address 0` for static IP addressing, but that is unnecessary and will adversely affect performance.

- To delete a client entry:

  `bpclient.exe -delete -client` *client_name*

- To list a client entry:

  `bpclient.exe -L -client` *client_name*

- To list all client entries:

  `bpclient.exe -L -All`

In our example, you can enter these commands to create the four clients:

`cd` *install_path*`\NetBackup\bin\admincmd`

```
bpclient -add -client nbclient01 -dynamic_address 1
bpclient -add -client nbclient02 -dynamic_address 1
bpclient -add -client nbclient03 -dynamic_address 1
bpclient -add -client nbclient04 -dynamic_address 1
```

To see what is currently in the client database, run `bpclient` as follows:

install_path`\NetBackup\bin\admincmd\bpclient -L -All`

The output is similar to the following:

```
Client Name: nbclient01
Current Host:
Hostname: *NULL*
IP Address: 0.0.0.0
Connect on non-reserved port: no
Dynamic Address: yes

Client Name: nbclient02
Current Host:
Hostname: *NULL*
IP Address: 0.0.0.0
Connect on non-reserved port: no
Dynamic Address: yes
.
.
.
```

After the NetBackup client notifies the NetBackup server of its NetBackup client name and network host name, the Current Host, Hostname, and IP Address fields will display the values for that NetBackup client.

Configuring a Dynamic Microsoft Windows Client

If it is not already installed, install NetBackup for Windows.

Start the NetBackup user interface on the client and click **Actions > Configure**. On the General tab of the NetBackup Configuration dialog, change the **Client Name** to specify the NetBackup client name for the Windows client. For example:

```
Client Name = nbclient06
```

On the Windows NetBackup server, set **Announce DHCP Interval** to specify how often (in minutes) to notify the NetBackup server of the NetBackup client name and network host name of the Windows client. (See “Announce DHCP Interval” on page 306.) For example, to notify the server every hour set this option to 60.

The server is not notified if the default value of 0 is used. For a DHCP client, a good value to use is one-half of the lease period.

On the client, stop and restart the NetBackup Client service to have the changes take effect.

Configuring a Dynamic Macintosh NetBackup Client

If not already installed, install NetBackup for Macintosh.

Edit the `bp.conf` document with a text editor such as SimpleText. The `bp.conf` document follows the folder path on the startup disk from `System` to `Preferences` to `NetBackup`. Use the `CLIENT_NAME` entry to specify the NetBackup client name for the Macintosh. For example:

```
CLIENT_NAME = nbclient02
```

Edit the `mac.conf` document with a text editor such as SimpleText. The `mac.conf` document follows the folder path on the startup disk from `System` to `Preferences` to `NetBackup`. Use the `DYNAMICNOTIFY` entry to specify how often (in seconds) to notify the NetBackup server of the NetBackup client name and network host name of the Macintosh. For example, notify the server every hour as follows:

```
dynamicnotify = 3600
```

The server is not notified if the default value of 0 is used. For a DHCP client, a good value to use is one-half of the lease period.

Restart the Macintosh.

Configuring a Dynamic UNIX NetBackup Client

If not already installed, install the NetBackup client software.

Edit the `/usr/openv/netbackup/bp.conf` file. Use the `CLIENT_NAME` entry to specify the NetBackup client name for the machine, as follows:

```
CLIENT_NAME = nbclient00
```

You must run the `bpdynamicclient` command once when the system first starts up. `bpdynamicclient` notifies the NetBackup server of the machine's NetBackup client name and current network host name. The `bpdynamicclient` command is in the directory:

```
/usr/openv/netbackup/bin
```

The format of the `bpdynamicclient` command is, as follows:

`bpdynamicclient -last_successful_hostname` *file_name*

When `bpdynamicclient` starts up, it checks for the existence of *file_name*. If *file_name* does exist, `bpdynamicclient` determines if the host name written in the file is the same as the current network host name of the machine. If the host names match,

bpdynamicclient exits and does not connect to the master server. If the host names do not match, bpdynamicclient connects to the master server and informs the server of its NetBackup client name and host name. If bpdynamicclient successfully informs the server, bpdynamicclient writes the current network host name into *file_name*. If bpdynamicclient cannot inform the server, bpdynamicclient deletes *file_name*.

Most UNIX systems provide a facility to define startup scripts. For example, on a Solaris system, you can create a script in the /etc/rc2.d directory:

```
# cat > /etc/rc2.d/S99nbdynamicclient <<EOF
#! /bin/sh

rm /usr/openv/netbackup/last_successful_hostname
/usr/openv/netbackup/bin/bpdynamicclient -last_successful_hostname
\
/usr/openv/netbackup/last_successful_hostname
EOF
# chmod 544 /etc/rc2.d/S99nbdynamicclient
```

Ensure that the dynamic client startup script is called after the machine obtains its IP address.

You must also create a root crontab entry to periodically call the bpdynamicclient command. For example, the following entry (one line) calls bpdynamicclient at seven minutes after each hour:

```
7 * * * * /usr/openv/netbackup/bin/bpdynamicclient -last_successful_hostname
/usr/openv/netbackup/last_successful_hostname
```

If you are using DHCP, a good interval to use between calls to bpdynamicclient is one-half of the lease period.

Bandwidth Limiting

Bandwidth limiting allows you to restrict the amount of network bandwidth consumed by one or more NetBackup clients on a network. The actual limiting occurs on the client side of the backup connection.

Bandwidth limiting only restricts bandwidth during backups. Restores are unaffected.

Read This First

- NetBackup does not currently support bandwidth limiting on NetBackup for Microsoft SQL-Server clients
- Bandwidth limiting has no effect on a local backup (where the server is also a client and data does not go over the network).

- Bandwidth limiting restricts maximum network usage and does not imply required bandwidth. For example, if you set the bandwidth limit for a client to 500 kilobytes per second, the client can use up to that limit. It does not mean, however, that the client requires 500 kilobytes per second.
- You cannot use bandwidth limiting to load-balance active backups by having NetBackup pick the most-available network segment. NetBackup does not pick the next client to run based on any configured bandwidth limits.

How Bandwidth Limiting Works

When a backup starts, NetBackup reads the bandwidth limit configuration and then determines the appropriate bandwidth value and passes it to the client. NetBackup computes the bandwidth limit based on the current set of active backups on the subnet (if any) and the new backup that is starting. Backups that start later are not considered. NetBackup also does not include local backups in its calculations.

The NetBackup client software enforces the bandwidth limit. Prior to each write of a buffer to the network, client software calculates the current value for kilobytes per second and adjusts its transfer rate if necessary.

As the number of active backups increase or decrease on a subnet, NetBackup dynamically adjusts the bandwidth limiting on that subnet. If additional backups are started, the NetBackup server instructs the other NetBackup clients running on that subnet to decrease their bandwidth setting. Similarly, bandwidth per client is increased if the number of clients decreases. Changes to the bandwidth value occur on a periodic basis rather than as backups stop and start. This can reduce the number of bandwidth value changes that are required.

Configuration

Configure bandwidth settings in **Master Server** > **NetBackup Management** > **Host Properties** > **Master Servers** > **Bandwidth**. (See “Bandwidth Tab” on page 269.)

Or, add one or more `LIMIT_BANDWIDTH` entries to the registry on the master server or the host property settings. These entries let you designate bandwidth values and the IP addresses of the clients and networks to which they apply.

Rules for IP Address Ranges

The IP address ranges can specify individual clients or entire subnets. The following are some specific rules on addresses:

- An IP address can have any one of the following forms:

- `a.b.c.d`

  Where `a`, `b`, `c`, and `d` are integers in the range 0-255.

- `128.net.host`

  Policy B address (16 bit host).

- `net.host`

  Policy A address (24 bit host).

- `a`

  A 32 bit integer, representing the full IP address in network byte order (that is, big endian, the most significant byte is first on the wire).

◆ You can enter IP addresses as decimal, octal or hexadecimal numbers. Numbers beginning with 0 are assumed to be octal, numbers beginning with 0x are hexadecimal and all others are assumed to be decimal.

◆ Neither the net nor the host part of an IP address can be zero.

◆ Only ordinary IP addresses are accepted (policy A, B & C, no multicast or reserved addresses).

◆ Do not create multiple entries that specify the same range of IP addresses. If you do, NetBackup uses the last one it finds. In the following example, NetBackup uses the second entry.

```
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 500
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 200
```

This rule also applies to multiple entries that specify an exact client address:

```
LIMIT_BANDWIDTH = 111.222.333.111 111.222.333.111 200
LIMIT_BANDWIDTH = 111.222.333.111 111.222.333.111 100
```

◆ Do not specify IP address ranges that overlap one another. Consider the following:

```
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 500
LIMIT_BANDWIDTH = 111.222.333.5 111.222.333.255 500
```

The ranges overlap, and bandwidth limiting results are unpredictable.

◆ You can specify a range of addresses in one entry and an address for a specific client in other entries.

If a client is covered by an entry that specifies its exact IP address and by another entry that specifies a range of IP addresses, NetBackup uses the bandwidth value in the entry with the exact IP address.

The following sets the bandwidth for a range of IP addresses:

```
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 500
```

The following sets the bandwidth for a specific address that is within the above range.

```
LIMIT_BANDWIDTH = 111.222.333.111 111.222.333.111 200
```

In this case, NetBackup uses the specific entry (bandwidth of 200) for the client whose address is 111.222.333.111. You can also use this capability to exclude specific clients from bandwidth limiting (see Example 3 below). The order in which the range and specific address entries appear in the registry is not significant.

Rules for Setting Bandwidth Values

When setting bandwidth values for individual clients, you must set it to either:

- 0 (no bandwidth limiting), or
- Less than or equal to any value set for the IP address range containing the IP address for the client.

  For example, the following is valid:

```
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 500
LIMIT_BANDWIDTH = 111.222.333.111 111.222.333.111 300
```

If you set the bandwidth higher for an individual client than it is for the range, NetBackup ignores that setting and uses the value for the range. In this case, the client gets its share of the bandwidth specified for the network.

If the bandwidth limit for an individual client is equal to or lower than the value for the range, the client uses one of the following, whichever is lower:

- Its share of the network bandwidth value
- Its individual bandwidth value

The bandwidth value that NetBackup uses for a client will always be at least one kilobyte per second.

Examples

Example 1

Configure a bandwidth limit of 500 kilobytes per second for all machines on the subnet 111.222.333 as follows:

```
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 500
```

Example 2

Configure a bandwidth limit of 700 kilobytes per second for a particular client (111.222.333.111) as follows:

```
LIMIT_BANDWIDTH = 111.222.333.111 111.222.333.111 700
```

Example 3

To disable bandwidth limiting for a client in a subnet that has a bandwidth limit, specify 0 for the kilobytes per second:

```
LIMIT_BANDWIDTH = 111.222.333.1 111.222.333.255 500
LIMIT_BANDWIDTH = 111.222.333.111 111.222.333.111 0
```

In this case, no limiting occurs for the client with IP address 111.222.333.111

Specifying the Locale of the NetBackup Installation

NetBackup applications can display a wide range of international date and time formats as determined by the locale of the installation. To help ensure consistency among the applications, NetBackup uses a single configurable source to define the locale conventions.

To Specify Locale of NetBackup Installation

Platform	Directions
Windows	To access the regional settings, double-click **Regional Settings** in the Windows Control Panel. This provides access to the predefined Number and Date/Time formats. See the Microsoft Help pages for further assistance.
Macintosh	Use the Date & Time Control Panel to change the values for the current date and current time, as well as to customize the date and time formats. See the Mac OS System Software manual pages for further assistance.
UNIX	The `/usr/openv/msg/.conf` file contains information on the supported locales. This file defines the date and time formats for each supported locale. The `.conf` file contains very specific instructions on how to add or modify the list of supported locales and formats. However, the format of the file is summarized here. The `.conf` file is divided into two parts, the `TL` lines and the `TM` lines.

To Specify Locale of NetBackup Installation (continued)

Platform	Directions
	TL Lines The third field of the `TL` lines defines the case-sensitive locales that the NetBackup applications support. The fourth and fifth fields define the date and time fields and associated separators for that supported locale is as follows: You can modify the existing formats to change the default output. For example, the `TL` line for the C locale is: `TL 1 C :`*hh*`:`*mn*`:`*ss*`/`*mm*`/`*dd*`/`*yyyy* An alternate specification the order of months, days, and years could be as follows: `TL 1 C :`*hh*`:`*mn*`:`*ss*` -`*yyyy*`-`*mm*`-`*dd* or: `TL 1 C :`*hh*`:`*mn*`:`*ss*`/`*dd*`/`*mm*`/`*yy* You can add more `TL` lines; see the comments in the `.conf` file. If the `.conf` file is not accessible, the default locales (`TL` lines) are: `TL 1 C :`*hh*`:`*mn*`:`*ss*` /`*mm*`/`*dd*`/`*yyyy* `TL 2 ov :`*hh*`:`*mn*`:`*ss*`/`*mm*`/`*dd*`/`*yyyy* Note that `C` and `ov` are synonymous.

	TM Lines
	The `TM` lines define a mapping from unrecognized locales to those supported by NetBackup, as defined by the `TL` lines.
	The third field of the `TM` lines define the unrecognized locale and the fifth field defines the supported equivalent identified in the `TL` lines.
	For example, use the following `TM` line to map the unrecognized locale *french* to the supported locale *fr*, the `TM` line is:
	`TM 6 french 2 fr`
	To map french to C
	`TM 6 french 1 C`
	To add more `TM` lines, see the specific instructions in the `.conf` file.
	If the `.conf` file is not accessible, there are no default `TM` lines as the default locale will be `C` (`ov`).

NetBackup Commands A

This section describes commands specific to the NetBackup product. Run these commands in an MS-DOS window to see the results.

The following are special conventions used in the command descriptions.

- Brackets [ ] mean that the enclosed command line component is optional.
- A vertical bar (or pipe) symbol | separates optional arguments from which the user can choose. For example, assume that a command has the following format:

  command [arg1 | arg2]

  Here, the user can choose either arg1 or arg2 (but not both).
- Italics indicate that the information is user supplied. For example, the user supplies *policy*, *schedule*, and *filename* in the following command:

  `bpbackup -p` *policy* `-s` *schedule filename*
- An ellipses (...) means that you can repeat the previous parameter. For example, consider the following command:

  `bpbackup` [`-S` *master_server* [,*master_server*,...]] *filename*

  Here, the `-S` option requires the first master server name. Additional names can be added, separated by commas and followed by a file name as in:

  `bpbackup -S mars,coyote,shark,minnow memofile.doc`

beconv

NAME

`beconv` - Convert Backup Exec on-disk catalogs to NetBackup on-disk catalogs.

SYNOPSIS

```
install_path\NetBackup\admincmd\beconv -all [-L output_file]
         [-non_interactive] [-auto_correct]

install_path\NetBackup\admincmd\beconv -rn robot_number [-L
         output_file] [-non_interactive]

install_path\NetBackup\admincmd\beconv -tbs [-rn robot_number]
         [-L output_file] [-non_interactive]

install_path\NetBackup\admincmd\beconv -m media_id [-h
         volume_database_name] [-L output_file] [-non_interactive]
         [-f]

install_path\NetBackup\admincmd\beconv -check_consistency

install_path\NetBackup\admincmd\beconv -show_mappings
```

DESCRIPTION

The `beconv` command converts Backup Exec on-disk catalogs to NetBackup catalogs. It also converts Backup Exec media records to NetBackup media manager records with the media being assigned to NetBackup. The media is kept in a frozen state so that NetBackup does not accidentally use it for backups.

The expiration date for Backup Exec images is the current date plus a retention level of 2 weeks. For example, if Backup Exec catalogs are converted on 7 August 2001, the expiration date for converted NetBackup catalogs will be 21 August 2001.

When the images expire, run `beconv` to regenerate the images.

OPTIONS

`-all` All media belonging to the Backup Exec server are converted and the corresponding images are generated.

`-auto_correct`
Use this option to take corrective actions (if any). Use it only when indicated during an earlier run of `beconv`.

`-check_consistency`
Use this option to check the consistency of media manager database.

With this option specified, no conversion takes place. In this mode, `beconv` searches for media manager records with ambiguous GUIDs and media ids in all the volume databases belonging to locally configured devices, then displays the list.

`-f`
: `-f` denotes the family to which the media belongs. `-f` converts all the media belonging to the same Backup Exec family. Use for backups which span more that one media.

`-h` *volume_database_host*
: Specifies the volume database host name where the media is actually present. If this is not specified, the local host name is taken.

`-L` *output_file*
: Specifies the name of a file in which to write progress information. The default is to not use a progress file.

`-m` *media_id*
: Specifies the media id of the Backup Exec media which needs to be converted.

`-non_interactive`
: Do not prompt for user input and carry on with the changes. Default is interactive mode, during which the user is prompted before any actual image generation.

`-rn` *robot_number*
: Specifies the NetBackup robot number for which the media need to be converted.

`-show_mappings`
: This option lists the current mappings between Backup Exec and NetBackup robots. With this option specified, no conversion takes place and only the mappings are displayed.

`-tbs`
: Trust By Slot. This mode is only for non-barcoded robotic media. In this mode, a match between a Backup Exec media record and a NetBackup media manager record is done on the basis of physical location of the media in the robot. In order for a match to be successful, physical inventory of the robot should be done prior to running `beconv` in this mode. The `-tbs` option can be combined with the `-rn` option to convert media for the specified robot only.

EXAMPLES

◆ Example 1

To run the catalog converter to convert all the media present on a Backup Exec server:

```
beconv -all
```

- Example 2

To run the catalog converter to convert only one media present on a Backup Exec server:

`beconv -m A00000 -h` *volume_database_host*

Where:

`A00000` is the media record corresponding to the Backup Exec media which needs to be converted.

volume_database_host is the machine where the NetBackup volume manager database resides.

bephyinv

NAME

bephyinv - Updates the media manager database, NetBackup media database and Backup Exec database for a set of Backup Exec media

SYNOPSIS

install_path\NetBackup\admincmd\bephyinv [-auto_correct] [-L *output_file*] [-V]

{

-rn *robot_number* |

{ -m *media_id* [-h *volume_database_host*] } |

{ -pn *pool_name* [-h *volume_database_host*] } |

{ -v *volume_group* [-h *volume_database_host*] } |

{ -rn *robot_number* -rc1 *robot_coord1* -number *number* }

}

DESCRIPTION

bephyinv allows fresh Backup Exec media (Backup Exec media which do not have on-disk Backup Exec catalogs present) to be imported into NetBackup. It is necessary to run bephyinv before running Step 1 of bpimport for such media.

bephyinv can also be used to update the Media Manager database in case Backup Exec media have been misplaced or manually been moved to a different slot.

bephyinv mounts the media, reads the tape header and updates the volume database for the media which was mounted.

bephyinv operates on Backup Exec media only; NetBackup media are ignored.

OPTIONS

-auto_correct
: If specified, bephyinv automatically expires media (only if found necessary) in order to keep the volume database consistent. By default, bephyinv never expires media.

-L *output_file*
: Specifies the name of a file in which to write progress information. The default is not to use a progress file.

`-h` *volume_database_host*
: Specifies the volume database which should be queried for the media id, pool name, or volume group in case the `-m`, `-pn`, or `-v` options are specified.

`-m` *media_id*
: Specifies the media id of the media manager record which needs to be inventoried. In case the `-h` option is not specified, *media_id* queries from the volume database of the local host.

`-number` *number*
: Specifies the number of slots starting from `robot_coord1` which need to be inventoried. Valid only when `-rn` and `-rc1` are also specified.

`-pn` *pool_name*
: Specifies the pool name of the media manager records which need to be inventoried. In case the `-h` option is not specified, *pool_name* queries from the volume database of the local host.

`-rc1` *robot_coord1*
: Specifies the starting slot of the media which needs to be inventoried. Valid only when `-rn` and `-number` are also specified.

`-rn` *robot_number*
: Specifies the Media Manager robot number where media will be inventoried. *robot_number* should correspond to a robot which has drives configured on the host on which `bephyinv` is being run.

  `Bephyinv` inventories each of the media, having *robot_number* in the volume database of *robot_number*.

`-V`
: Selects the verbose mode. When specified, the progress logs display more information.

`-v` *volume_group*
: Specifies the volume group of the media manager records which need to be inventoried. In case the `-h` option is not specified, *volume_group* queries from the volume database of the local host.

EXAMPLES

◆ Example 1

The user wants to inventory Backup Exec media which does not have on-disk Backup Exec catalogs present.

Before running `bephyinv`, the user creates a media manager record corresponding to the Backup Exec media. The user creates a media manager record, either by using `vmadd` or by placing the media in a robot and performing a NetBackup robotic inventory.

The user runs the following command:

`bephyinv -m` *media_id* `-h` *volume_database_host*

Where:

media_id is the newly created media manager media id of the Backup Exec media.

volume_database_host is the volume database host in which the media manager media id corresponding to the Backup Exec media has been created.

In case the media manager record indicates that the Backup Exec media is standalone (not-robotic), the user needs to manually assign the mount request to the drive in which the Backup Exec media has been placed:

`Vmoprcmd -assign` *drive_index* *mount_request_index*

Where:

Drive_index is the drive index of the standalone drive in which the Backup Exec media has been placed.

Mount_request_index is the mount request id corresponding to the Backup Exec media.

Note For NetBackup media, mount requests for standalone media are automatically assigned. For Backup Exec media, the mount request has to be assigned manually using either the device monitor or the media manager command, `vmoprcmd`.

Media Manager does not auto assign mount requests for standalone Backup Exec media.

◆ Example 2

The user has been restoring from Backup Exec media using NetBackup. However, the Backup Exec media are non-barcoded, and have been misplaced (their physical locations in a robot do not match with the logical locations specified in the media manager database).

The user runs the following command:

`bephyinv -rn` *robot_number*

Where:

Robot_number is the NetBackup robot number in which the Backup Exec media are placed.

Running `bephyinv` on a whole robot may be very time consuming since each of the media will be mounted and read. It may be quicker to run `bephyinv` on a range of slots if the user knows the range of slots in which the media may be placed.

The user runs the following command:

`bephyinv -rn` *robot_number* `-rc1 coord1 -number` *number*

Where:

Robot_number is the NetBackup robot number in which the Backup Exec media are placed.

Coord1 is the starting slot number.

Number is the number of slots (starting from coord1) which need to be inventoried.

bparchive

NAME

`bparchive` - Archive files to the NetBackup server

SYNOPSIS

install_path`\NetBackup\bin\bparchive [-p` *policy*`] [-s` *schedule*`] [-S` *master_server* `[,`*master_server*`,...]] [-t` *policy_type*`] [-L` *progress_log* `[-en]] [-w [`*hh*`:`*mm*`:`*ss*`]] [-help] [-k "`*keyword_phrase*`"] -f` *listfile* | *filenames*

DESCRIPTION

`bparchive` processes files that you list on the command line or in the file you specify with the `-f` *listfile* option. Any file path entered can be a file or directory name. If the list of files includes a directory, `bparchive` archives all files and subdirectories of that directory starting at the directory itself.

By default, you are returned to the system prompt after `bparchive` is successfully submitted. The command works in the background and does not return completion status directly to you. The `-w` option lets you change this behavior so `bparchive` works in the foreground and returns completion status after a specified time period.

`bparchive` writes its informative and error messages to a progress-log file. You must create this file prior to running the `bparchive` command and then specify it with the `-L` *progress_log* option. If `bparchive` cannot archive any of the requested files or directories, you can use the progress log to determine the reason for the failure.

If you create an *install_path*`\NetBackup\logs\bparchive\` directory with write access, `bparchive` creates an debug log file in this directory that you can use for troubleshooting.

The following restrictions apply to this command:

- To archive a file with the `bparchive` command, you must have permission to delete the file and the file must not be read-only. Otherwise, NetBackup saves the files but does not delete them from the disk.
- `bparchive` does not archive the "." or ".." directory entries, and does not archive disk-image backups.

OPTIONS

`-p` *policy* Names the policy to use for the user archive. If it is not specified, the NetBackup server uses the first policy it finds that includes the client and a user archive schedule.

`-s` *schedule*

Names the schedule to use for the user archive. If it is not specified, the NetBackup server uses the first user archive schedule it finds in the policy it is using (see the `-p` option).

`S` *master_server* `[,`*master_server*`,...]`

Specifies the name of the NetBackup master server. The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the user interface on the client and click Specify NetBackup Machines on the Actions menu.

`-t` *policy_type*

Specifies one of the following numbers corresponding to the policy type. The default for NT clients is `13`, for Apollo workstations the default is `3`, and for Netware clients the default is `10`. The default for all others is `0`:

`0` = Standard

`4` = Oracle

`6` = Informix-On-BAR

`7` = Sybase

`13` = MS-Windows-NT

`14` = OS/2

`15` = MS-SQL-Server

`16` = MS-Exchange-Server

`19` = NDMP

Note The following policy types apply only to NetBackup DataCenter.

`3` = Apollo-wbak

`11` = DataTools-SQL-BackTrack

`17` = SAP

`18` = DB2

`20` = FlashBackup

`21` = Split-Mirror

`22` = AFS

`-L` *progress_log* `[-en]`

Specifies the name of an existing file in which to write progress information.

For example: `c:\proglog`.

The default is to not use a progress log.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-w` [*hh:mm:ss*]

Causes NetBackup to wait for a completion status from the server before returning you to the system prompt.

The date and time format depend on the user's locale. See NOTES.

You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the archive is complete, the command exits with a timeout status. The archive, however, still completes on the server.

If you use `-w` without specifying the wait time or if you specify a value of 0, NetBackup waits indefinitely for the completion status.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-k` *keyword_phrase*

Specifies a keyword phrase that NetBackup associates with the image created by this archive operation. You can then restore the image by specifying the keyword phrase with the `-k` option on the `bprestore` command.

The keyword phrase is a textual description of the archive that is a maximum of 128 characters in length. All printable characters are permitted including space (" ") and period (."). Enclose the phrase in double quotes ("...") or single quotes ('...').

The default keyword phrase is the null (empty) string.

`-f` *listfile* Specifies a file (*listfile*) containing a list of files to be archived and can be used instead of the *filenames* option. In *listfile*, place each file path on a separate line.

The format required for the file list depends on whether the files have spaces or returns in the names.

To archive files that do not have spaces or returns in the names, use this format:

filepath

Where *filepath* is the path to the file you are archiving. For example:

```
c:\Programs
c:\winnt
c:\documents\old_memos
```

To archive files that have spaces or returns in the names, use this format:

filepathlen filepath

Where *filepath* is the path to the file you are archiving and *filepathlen* is the number of characters in the file path.

For example:

```
11 c:\Programs
8 c:\winnt
22 c:\documents\old memos
```

filenames

Names one or more files to be archived and can be used instead of the `-f` option.

Any files that you specify must be listed at the end, after all other options.

EXAMPLES

- Example 1

  To archive a single file, enter:

  ```
  bparchive c:\usr\user1\file1
  ```

- Example 2

  To archive files listed in a file named `archive_list`, enter:

  ```
  bparchive -f archive_list
  ```

- Example 3

  To associate the keyword phrase “Archive My Home Directory 02/02/02” to the archive of the directory `c:\home\kwc` and use a progress log named `c:\home\kwc\arch.log` enter the following (the backslash continues the command as if it were on one line):

  ```
  bparchive -k "Archive My Home Directory 01/01/97" -L
  c:\home\kwc\arch.log  c:\home\kwc
  ```

FILES

install_path`\NetBackup\logs\bparchive\*.log`

bpauthorize

NAME

`bpauthorize` - Manage the `authorize.txt` file on remote servers.

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpauthorize [-M` *nb_server*`] [-g` *user_if_host*`] [-debug] [-verbose] [-get_privileges]` *file*

install_path`\NetBackup\bin\admincmd\bpauthorize [-M` *nb_server*`] [-debug] [-verbose] -get_authorize` *file*

install_path`\NetBackup\bin\admincmd\bpauthorize [-M` *nb_server*`] [-debug] [-verbose] -set_authorize` *file*

DESCRIPTION

This command is available only on NetBackup master servers and sets up authentication files on NetBackup servers and clients according to the options that are specified on the command.

OPTIONS

`-debug` Issues debug messages to standard error.

`-g` *user_if_host*

When used with `-get_privileges`, indicates the job monitoring capabilities of the specified host:

```
MONITOR_OK = 0 | 1
```

Where `1` indicates that the host specified can use the more efficient job monitoring capabilities of NetBackup 4.5.

`-g` option is used internally by the Java interface (`jnbSA`).

`-get_privileges` *file*

Displays the privileges you have on the remote server.

If *file* specified, output is written to this file. By default, output is written to standard output.

If `-verbose` is not indicated, the output would look similar to the following example:

```
1 1 1 1 0
```

The privileges appear in the following order: (`-verbose` indicated)

```
IS_SERVER = 0 | 1
```

Where 1 indicates that the local host name is in the remote machine's SERVER list in `bp.conf`.

`IS_MEDIA_SERVER = 0 | 1`

Where 1 indicates that the local host name is in the remote machine's MEDIA_SERVER list in `bp.conf`.

`IS_ADMIN =0 | 1`

Where 1 indicates that the user is an administrator according to the `authorize.txt` file on the remote machine.

`IS_OPERATOR =0 | 1`

Where 1 indicates that the user is an operator according to the `authorize.txt` file on the remote machine.

AUTHENTICATION_REQUIRED = `0 | 1`

`1` = Authentication to the server is required

`0` = Authentication to the server is not required

Note If the server is a NetBackup version prior to 4.5, authentication required returns `1`.

`-get_authorize` *file*

Displays the contents of the `authorize.txt` file on the remote server.

If *file* specified, output is written to this file. By default, output is written to standard output.

`-M` *nb_server*

Indicates the remote server to check. The default is the master server.

`-set_authorize` *file*

Updates the contents of the `authorize.txt` file on the remote server.

If *file* is specified, input is read from this file. By default, input is read from standard input.

To use, first write the `authorize.txt` file from a NetBackup server to a temporary file:

`./bpauthorize -M` *nb_server* `-get_authorize /tmp/`*filename.txt*

Then, edit and save the file:

`vi /tmp/`*filename.txt*

Finally, use `-set_authorize` to update the `authorize.txt` file of the NetBackup server with the edited file:

`./bpauthorize -M` *nb_server* `-set_authorize /tmp/`*filename.txt*

`-verbose`

Select verbose mode to include more detailed descriptions when using `bpauthorize` with `-get_privileges` or `-get_authorize` options.

bpauthsync

NAME

`bpauthsync` - Synchronize authentication files on NetBackup servers and clients

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpauthsync [-verbose] [-methods] [-names] [-vopie] [-methods_allow` *path_name*`] [-methods_deny` *path_name*`] [-names_allow` *path_name* `] [-names_deny` *path_name*`] [-clients [`*client1 client2 ... clientN*`] ] [-servers [`*server1 server2 ... serverN*`] ]`

DESCRIPTION

This command is available only on NetBackup master servers and sets up authentication files on NetBackup servers and clients according to the options that are specified on the command.

OPTIONS

`-verbose`
Issue additional messages.

`-methods`
Push the `methods_allow.txt` and `methods_deny.txt` files to the specified clients and servers.

`-names` Push the `names_allow.txt` and `names_deny.txt` files to the specified clients and servers.

`-vopie` Synchronize the `VOPIE` key files between the specified servers and the specified clients.

Note If none of `-methods`, `-names`, and `-vopie` is specified, all three are assumed.

`-methods_allow` *path_name*
Specifies the local copy of the `methods_allow.txt` file to push to the servers and clients. If this option is not included, NetBackup uses the *install_path*`\NetBackup\var\auth\methods_allow.txt` file.

`-methods_deny` *path_name*
Specifies the local copy of the `methods_deny.txt` file to push to the servers and clients. If this option is not included, NetBackup uses the *install_path*`\NetBackup\var\auth\methods_deny.txt` file.

`-names_allow` *path_name*
Specifies the local copy of the `names_allow.txt` file to push to the servers and clients. If this option is not included, NetBackup uses the *install_path*`\NetBackup\var\auth\names_allow.txt` file.

`-names_deny` *path_name*
Specifies the local copy of the `names_deny.txt` file to push to the servers and clients. If this option not included, NetBackup uses the *install_path*`\NetBackup\var\auth\names_deny.txt` file.

`-clients [` *client1 client2 . . . clientN* `]`
Names the clients to update. If `-clients` is specified without listing any client names, all unique client names in the NetBackup catalog are updated. A client name can also be specified in this format:

name:*host*

Where *name* is the client name and *host* is the network host name of the client. This is useful for specifying NetBackup clients that use dynamic network addressing like DHCP.

`-servers [` *server1 server2 . . . serverN* `]`
Names the servers to update.

If `-servers` is specified but no server names are listed, all server names in the NetBackup configuration are updated.

Note The following cases also apply to using the `-clients` and `-servers` options:

If neither `-clients` nor `-servers` is used, all clients and all servers are updated.

If `-servers` is used but `-clients` is not, no clients are updated.

If `-servers` is not used but `-clients` is used along with `vopie` (either specifically or by default), the local server is updated.

If `-servers` is not used but `-clients` is used along with `-names` or `-methods`, no servers are updated.

FILES

install_path`\NetBackup\var\auth\methods.txt`

install_path`\NetBackup\var\auth\methods_allow.txt`

install_path`\NetBackup\var\auth\methods_deny.txt`

install_path`\NetBackup\var\auth\names_allow.txt`

install_path`\NetBackup\var\auth\names_deny.txt`

install_path`\NetBackup\var\auth\vopie\*`

SEE ALSO

`vopied`, `vopie_util`

bpbackup

NAME

bpbackup - Back up files to the NetBackup server

SYNOPSIS

install_path\NetBackup\bin\bpbackup [-p *policy*] [-s *schedule*] [-S *master_server* [,*master_server*,...]] [-t *policy_type*] [-L *progress_log* [-en]] [-w [*hh*:*mm*:*ss*]] [-help] [-k "*keyword_phrase*"] -f *listfile* | *filenames*

install_path\NetBackup\bin\bpbackup -p *policy* -i [-h *hostname*] [-s *schedule*] [-S *master_server* [,*master_server*,...]] [-t *policy_type*] [-w [*hh*:*mm*:*ss*]] [-k "*keyword_phrase*"]

DESCRIPTION

bpbackup starts either of the following processes:

On clients

Using the first form of the command above, bpbackup starts a user backup that is the equivalent to what is performed by using the interface on the client. This type of backup can be started from any NetBackup client in order to back up files from that client.

The bpbackup command processes the files that you list on the command line or in the file that you specify with the -f *listfile* option. A file path can be a file or directory name. If the named files include a directory, bpbackup backs up all files and subdirectories of that directory starting at the directory itself.

On master servers

Using the second form of the command shown above, bpbackup starts an immediate-manual backup of a client. This variation requires the -i option on the bpbackup command and is available only to the administrator on the master server. It is the equivalent of starting a manual backup from the NetBackup administrator's interface. Use the -h option to specify the host.

Since progress logs are written only on clients, and since this form of the bpbackup command is run from the master server only, the -L option is undefined.

The following restrictions apply to this command:

- You must be the owner of the file or an administrator to back up a file with bpbackup.
- You can back up files and directories owned by other users if you have the necessary permissions.

- bpbackup does not back up the "." or ".." directory entries.

By default, you are returned to the system prompt after bpbackup is successfully submitted. The command works in the background and does not return completion status directly to you. The -w option lets you change this behavior so the command works in the foreground and returns completion status after a specified time period.

bpbackup writes informative and error messages to a progress-log file if you create the file prior to running the bpbackup command and then specify the file with the -L *progress_log* option. If bpbackup cannot back up the requested files or directories, use the progress log to determine the reason for the failure.

If you create a directory named *install_path*\NetBackup\logs\bpbackup with write access, bpbackup creates a debug log file in this directory that can be used for troubleshooting.

OPTIONS

-p *policy* Names the policy to use for the backup.

If this option is not specified for a user backup, NetBackup uses the first policy it finds that includes the client and a user backup schedule.

The -p option is required for an immediate-manual backup (-i option).

-i Starts an immediate-manual backup. This is the equivalent of starting a manual backup from the NetBackup administrator interface. You must be the administrator on the master server to use the -i option.

-h *hostname*
It names the client host on which to run the backup. If it is not specified, NetBackup runs the backup on all clients in the policy.

-s *schedule*
Names the schedule to use for the backup. If it is not specified, the NetBackup server uses the first user backup schedule it finds for the client in the policy it is using (see the -p option).

-S *master_server* [, *master_server*, . . .]
Specifies the name(s) of the NetBackup master server(s). The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the user interface on the client and click Specify NetBackup Machines on the Actions menu.

-t *policy_type*
Specifies one of the following numbers corresponding to the policy type. The default for NT clients is 13, for Apollo workstations the default is 3, and for Netware clients the default is 10. The default for all others is 0:

0 = Standard

4 = Oracle

6 = Informix-On-BAR

7 = Sybase

13 = MS-Windows-NT

14 = OS/2

15 = MS-SQL-Server

16 = MS-Exchange-Server

19 = NDMP

Note The following policy types apply only to NetBackup DataCenter.

3 = Apollo-wbak

11 = DataTools-SQL-BackTrack

17 = SAP

18 = DB2

20 = FlashBackup

21 = Split-Mirror

22 = AFS

`-L` *progress_log* `[-en]`

Specifies the name of a file in which to write progress information. NetBackup creates the file if it doesn't exist.

For example: `c:\proglog`

The default is to not use a progress log.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-w` [*hh:mm:ss*]

Causes NetBackup to wait for a completion status from the server before returning you to the system prompt.

You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the backup is complete, the command exits with a timeout status. The backup, however, still completes on the server.

If you use `-w` without specifying a wait time or you specify a value of 0, NetBackup waits indefinitely for the completion status.

If you include `-i` with `-w`, NetBackup waits until all initiated jobs have completed before returning status. However, if more than one job starts, the status is unpredictable. If the multiple jobs are due to there being

more than one client and the policy does not have Allow Multiple Data Streams selected, you can include the `-h` option to restrict the operation to one client and obtain predictable status. However, if the policy has Allow Multiple Data Streams selected and there is more than one job from the selected client, the status is still unpredictable.

`-help`
Prints a command line usage message when `-help` is the only option on the command line.

`-k` *keyword_phrase*
Specifies a keyword phrase that NetBackup associates with the image being created by this backup operation. You can then restore the image by specifying the keyword phrase with the `-k` option on the `bprestore` command.

If you use the `-i` option with `-k`, NetBackup establishes an association between the keyword phrase and the backup policy and image.

The keyword phrase is a textual description of the backup that is a maximum of 128 characters in length. All printable characters are permitted including space (" ") and period (."). Enclose the phrase in double quotes ("...") or single quotes ('...').

The default keyword phrase is the null (empty) string.

`-f` *listfile*
Specifies a file (*listfile*) containing a list of files to be backed up. This option can be used instead of the *filenames* option, but cannot be used with the `-i` option. List each file on a separate line.

The format required for the file list depends on whether the files have spaces or returns in the names.

To back up files that do not have spaces or returns in the names, use this format:

filepath

Where *filepath* is the path to the file you are backing up. For example:

```
c:\Programs
c:\winnt
c:\documents\old_memos
```

To back up files that have spaces or returns in the names, use this format:

filepathlen filepath

Where *filepath* is the path to the file you are backing up and *filepathlen* is the number of characters in the file path.

For example:

```
11 c:\Programs
8 c:\winnt
```

```
22 c:\documents\old memos
```

filenames

Names one or more files to be backed up. This option can be used instead of the `-f` option, but cannot be used with the `-i` option. Any files that you specify must be listed at the end, following all other options.

EXAMPLES

- Example 1

  To perform a user backup of a single file, enter:

```
bpbackup c:\users\user1\file1
```

- Example 2

  The following command starts a user backup of the files that are listed in a file named `backup_list`.

```
bpbackup -f backup_list
```

- Example 3

  The following command (all on one line) starts an immediate-manual backup of the client host named diablo, in the policy named cis_co. The policy type is Standard policy and is in the configuration on the master server named hoss.

```
bpbackup -p cis_co -i -h diablo -S hoss -t 0
```

- Example 4

  The following command (all on one line, or using the backslash continuation character) associates the keyword phrase “Backup My Home Directory 01/01/0‘” to the user backup of the directory `c:\home\kwc`. The progress log is `c:\home\kwc\bkup.log`.

```
bpbackup -k "Backup My Home Directory 01/01/97" -L
c:\home\kwc\bkup.log  c:\home\kwc
```

- Example 5

  The following command (all on one line) associates the keyword phrase “Policy Win NT 01/01/01” to the immediate-manual backup of the client host named slater in the policy named win_nt_policy.

```
bpbackup -k "Policy Win NT 01/01/97" -i -h slater -p win_nt_policy
-t 13
```

FILES

install_path`\NetBackup\logs\bpbackup\*.log`

bpbackupdb

NAME

bpbackupdb - Back up NetBackup image catalogs

SYNOPSIS

install_path\NetBackup\bin\admincmd\bpbackupdb [-dpath *disk_path*] [-nodbpaths] [-v] [*path* . . .] [*host_name* :] [DB=*database_name*] [/*table_name*]

install_path\NetBackup\bin\admincmd\bpbackupdb [-tpath *tape_device_path* [-rv *recorded_vsn*]] [-nodbpaths] [-v] [*path* . .] [*host_name* :] [DB=*database_name*] [/*table_name*]

install_path\NetBackup\bin\admincmd\bpbackupdb [-opath *optical_device_path* [-rv *recorded_vsn*]] [-nodbpaths] [-v] [*path* . . .] [*host_name* :] [DB=*database_name*] [/*table_name*]

DESCRIPTION

bpbackupdb initiates a backup of one or more NetBackup image catalogs specified on the bpbackupdb command line. bpbackupdb also backs up the default set of NetBackup catalogs, unless the command line contains -nodbpaths. If the command line specifies a destination, the backup is stored there.

Otherwise, the backup is stored at the default location for backups of the NetBackup internal databases, which are called catalogs.

You can specify the default set of catalogs and the backup destination:

- The default paths to the NetBackup image catalogs are part of the NetBackup configuration. bpbackupdb uses the set of configured NetBackup catalog paths as the default value for the path option.
- The NetBackup configuration includes two destinations (media IDs or disk pathnames) for NetBackup catalog backups. bpbackupdb uses the less-recently used of the two destinations as its default value for the backup destination.

The *NetBackup System Administrator's Guide* explains how to configure and display these values.

This command requires administrator privileges.

Only one copy of bpbackupdb can run at a time. The bpbackupdb command fails if it determines that a NetBackup catalog backup is already running. If bpbackupdb fails because other backups are in progress, retry when no other NetBackup activity is occurring.

If bpbackupdb fails with the message "cannot find Internet service bpcd/tcp," then the service/protocol pair bpcd, tcp is not among the set of services defined on the local system. On Windows, look for a bpcd/tcp entry in the *install_path*\system32\drivers\etc\services file.

The *NetBackup System Administrator's Guide* provides additional information on backing up NetBackup catalogs. The NetBackup utility bprecover recovers catalogs that bpbackupdb has backed up. The NetBackup troubleshooting guide (Windows version) provides information on restoring the NetBackup catalogs if a disaster recovery is required.

OPTIONS

You can either specify a list of NetBackup image catalogs with the following options or default to the catalogs specified in the NetBackup configuration:

-dpath *disk_path*

-tpath *tape_device_path*

-opath *optical_device_path*

-tpath specifies a tape raw device path as the destination for the backup.

-opath specifies an optical raw device path as the destination for the backup.

-dpath Specifies a raw disk path as the destination for the backup. If the media for the catalog backup is non-robotic, a mount request occurs and the catalog backup waits until the mount request is either granted or denied. The MEDIA_MOUNT_TIMEOUT attribute does not apply to this request.

The NetBackup Device Manager service and NetBackup Volume Manager service need not be active when you use the -dpath option.

If -tpath or -opath is used, the device name can be an NDMP device name. The syntax for an NDMP device name is *client*:*drivename*. An NDMP device name can contain / but it cannot contain /ndmp.

-rv *recorded_vsn*

This is the recorded volume serial number (RVSN). This option is meaningful if either -tpath or -opath is used. Media Manager uses the RVSN for removable media to verify that the correct platter is mounted. The RVSN is the same value as the media ID. The RVSN's string length is between one and six characters and the string can be either uppercase or lowercase.

-help Prints a command line usage message when -help is the only option on the command line.

`-nodbpaths`

Do not back up the configured NetBackup catalogs. If this option is present, you must specify at least one catalog path on the command line. If this option is absent, `bpbackupdb` backs up the catalogs configured by NetBackup for catalog backups, as well as any catalog listed by the *path* option.

`-v`

Selects verbose mode. This option causes `bpbackupdb` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\netbackup\logs\admin` directory defined).

path...

Back up these NetBackup catalogs. This is a list of absolute pathnames.

To back up a NetBackup catalog on the master server, specify the catalog backup path as an absolute pathname, for instance, *install_path*`\Volmgr\database`.

If the backup path contains special characters, such as blank(" "), the pathname must be enclosed in quotes ("). Use a blank to separate two pathnames, not a comma. The complete list of pathnames to be backed up must also be enclosed in quotes. See Example 3.

To back up a NetBackup catalog on a media server other than the master server (this configuration is supported only by NetBackup DataCenter), specify the catalog backup path as *hostname*:*pathname*. For instance, *hostname*:*install_path*`\Volmgr\database`.

There must be at least one path specified if `-nodbpaths` is present.

EXAMPLES

Examples 1 and 2 assume that NetBackup has been configured so that `bpbackupdb` can use the default values for catalogs and destination. Example 3 uses the *path...* option to specify the catalogs to back up.

- Example 1

  The following example backs up the NetBackup catalogs

  ```
  bpbackupdb
  ```

  - If the backup succeeds, the NetBackup mail administrator receives email containing the details of the backup.
  - If the backup fails, the NetBackup mail administrator receives email containing the reason for the failure.

- Example 2

  The following example backs up the NetBackup catalogs to the tape device `\\.\Tape1`.

```
bpbackupdb -tpath \\.\Tape1
```

- Example 3

This example backs up the catalogs specified in the *path...* option in addition to the configured NetBackup catalogs.

```
bpbackupdb ""C:\catalog A" "C:\catalog B""
```

EXIT STATUS

An exit status of 0 means that the backup ran successfully.

Any exit status other than 0 means that an error occurred.

DIAGNOSTICS

If `bpbackupdb` succeeds, it logs one of the following messages:

NB database backup to path *destination* SUCCEEDED

NB database backup to media id *destination* SUCCEEDED

NB database backup SUCCEEDED

If `bpbackupdb` fails, it logs one of the following messages:

NB database backup to path *destination* FAILED

NB database backup to media id *destination* FAILED

NB database backup FAILED

`bpbackupdb` also sends mail to the NetBackup administrator reporting the results of the backup.

FILES

install_path`\NetBackup\db\*`

install_path`\NetBackup\logs\admin\log.`*mmddyy*

install_path`\Volmgr\database\*`

SEE ALSO

`bprecover`

bpchangeprimary

NAME

`bpchangeprimary` - Promote a copy of a backup to be the primary copy

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpchangeprimary`
`-copy` *number* | `-pool` *volume_pool* | `-group` *volume_group* `[-id` *backup_id*`]`
`[-M` *master_server*`]`

install_path`\NetBackup\bin\admincmd\bpchangeprimary`
`-copy` *number* | `-pool` *volume_pool* | `-group` *volume_group*
`[-sl` *schedule_name*`]` `[-pn` *policy_name*`]`
`[-st` *schedule_type*`]` `[-pt` *policy_type*`]`
`[-cl` *client_name*`]`
`[-kw` *keyword*`]`
`[-sd` *mm/dd/yyyy* `[HH:MM:SS]]` `[-ed` *mm/dd/yyyy* `[HH:MM:SS]]`
`[-M` *master_server*`]`

DESCRIPTION

The `bpchangeprimary` command lets you change which copy is the primary copy for a set of backup images. You can choose the copy to be promoted to primary by specifying a copy number, volume pool, or volume group. You can apply several optional criteria to identify the backup images to be affected.

The primary copy of a backup is the copy used by a restore process. Ensure that the primary copy is accessible for restore. For instance, if one copy of a backup has been sent offsite, change the primary copy to be the copy that remains onsite.

The `bpchangeprimary` command runs a `bpimagelist` command with the optional criteria and finds all backups matching that criteria. After the backups are identified, a `bpimage` command is run for each backup matching the copy or pool or group specification.

If you use the `-copy` option, the specified copy number becomes the primary copy. If you use the `-group` or `-pool` option, the process identifies all media IDs that belong to the specified volume group or volume pool and changes to primary, all copies that reside on those media.

OPTIONS

One of the following three options is required; using one precludes use of the others.

`-copy` *number*
: Specifies that *copy_number* is the number of the backup copy you want to promote to primary.

`-pool` *volume_pool*
: Specifies that the copy that is on media belonging to *volume_pool* should be promoted to primary.

`-group` *volume_group*
: Specifies that the copy that is on media belonging to *volume_group* should be promoted to primary.

Combinations of one or more of the following criteria can be applied to specify which copies will be made primary. None of the following options are required.

`-cl` *client_name*
: Specifies that backups of *client_name* will be affected. For those backup images, the copy that corresponds to the specified `-pool`, `-group`, or `-copy` option will be promoted to primary. The default is all clients.

`-sd` *mm/dd/yy* [*hh*:*mm*:*ss*]

`-ed` *mm/dd/yy* [*hh*:*mm*:*ss*]
: Specifies the start date (`-sd`) or end date (`-ed`) of the backup images for which the primary copy will be changed.

The default start date is January 1, 1970, effectively causing a search for all images. If you run `bpchangeprimary` without using the `-sd` option, you are prompted for confirmation that you want to change the primary copy for backups created after January 1, 1970.

The default end date is the current date and time.

The `locale` setting for the system affects the way you specify dates and times. See NOTES. The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07.

`-id` *backup_id*
: Specifies the backup id of the backup image for which the primary copy will be changed. For that backup image, the copy that corresponds to the specified `-pool`, `-group`, or `-copy` option will be changed.

If you specify this option, you can specify an alternate master server (using the `-M` option). You must specify one of `-pool`, `-group`, or `-copy`. No other options are used with `-id`.

`-kw` *keyword_phrase*
: Specifies a keyword phrase for NetBackup to use when identifying backup images for which the primary copy will be changed.

`-M` *master_server*

Specifies that backups belonging to *master_server* will be affected. For those backup images, the copy that corresponds to the specified `-pool`, `-group`, or `-copy` option will be promoted to primary.

If you use this option, then any other options you specify determine which backup images on the specified master server will be affected. The *master_server* must allow access by the system issuing the `bpchangeprimary` command. The default is the master server for the system running the `bpchangeprimary` command.

`-pn` *policy_name*

Specifies the name of the backup policy of the backups for which the primary copy will be changed. The default is all policies.

`-pt` *policy_type*

Specifies the type of the backup policies of the backups for which the primary copy will be changed. The default is all policy types.

The *policy_type* is one of the following character strings:

```
Informix-On-BAR
MS-Exchange-Server
MS-SQL-Server
MS-Windows-NT
NetWare
Oracle
OS/2
Standard
Sybase
NDMP
```

The following policy types apply only to NetBackup DataCenter.

```
AFS
Apollo-wbak
Auspex-FastBackup
DataTools-SQL-BackTrack
DB2
FlashBackup
SAP
Split-Mirror
```

`-sl` *schedule_name*

Specifies the *schedule name* (label) for the selection of the backup images for which the primary copy will be changed.

By default, the `bpchangeprimary` command uses all schedules.

`-st` *schedule_type*

Specifies the schedule type for the selection of the backup images for which the primary copy will be changed.

By default, the `bpchangeprimary` command uses any schedule type. Valid vales are as follows:

`FULL` (full backup)
`NCR` (differential-incremental backup)
`CINC` (cumulative-incremental backup)
`UBAK` (user backup)
`UARC` (user archive)
`NOT_ARCHIVE` (all backups except user archive)

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the output for the `-sd` and `-ed` options:

```
[-sd mm/dd/yyyy HH:MM:SS] [-ed mm/dd/yyyy HH:MM:SS]
```

Notice the month / day / year and hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales.

EXAMPLES

The following command will promote all copies on media belonging to the volume pool, SUN, created after 08 / 01 / 2001 to be the primary copy.

```
bpchangeprimary -pool SUN -sd 08/01/2001
```

The following command will promote copy 2 of all backups of client, oak, created after 01 / 01 / 2001 to be the primary copy:

```
bpchangeprimary -copy 2 -cl oak -sd 01/01/2001
```

The following command will promote copy 4 of all backups that were created by the backup policy, Offsite, after 08 / 01 / 2001 to be the primary copy:

```
bpchangeprimary -copy 4 -pn Offsite -sd 08/01/2001
```

bpclient

NAME

`bpclient` - Manage client entries on a master server

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpclient [-All] [-M` *master_server*`] [-L|-H]`

install_path`\NetBackup\bin\admincmd\bpclient -client` *client_name* `[-M` *master_server*`] [-L|-H]`

install_path`\NetBackup\bin\admincmd\bpclient -client` *client_name* `[-M` *master_server*`] -add|-update options [-connect_nr_port 0|1] [-no_callback 0|1][-dynamic_address 0|1][-current_host` *host_name* `[:`*ip_address*`]|:`*ip_address*`][-free_browse 0|1|2][-list_restore 0|1|2|3][-max_jobs [1-99]]`

install_path`\NetBackup\bin\admincmd\bpclient -client` *client_name* `[-M` *master_server*`] -delete`

OPTIONS

`-add` Add a new client entry.

`-All` List all client entries. Only client entries added explicitly using the `bpclient` command are displayed.

`-client` *client_name*
Where *client_name* is the name of the client to list or update.

`-connect_nr_port 0|1`

`0` = Connect to the client's `bpcd` using a reserved (less than 1024) port number (default).

`1` = Connect to the client's `bpcd` using a non-reserved port number. If you select this option, enable **Allow Nonreserved Ports** for the selected client. (See the Universal Settings dialog under **Host Properties** > **Clients**.)

`-current_host` *host_name*`[:`*ip_address*`]|:`*ip_address*
The host name/IP address of the client. This is only meaningful in the situation where the option `-dynamic_address 1` is used. Usually, you do not have to enter a `-current_host` value. The client normally contacts the master server to set the host name/IP address.

`-delete` Delete an existing client entry.

`-dynamic_address 0|1`

`0` = The client name is assumed to be a valid host name for the client (default).

`1` = The client is assumed to have a dynamic host name (such as DHCP).

`-free_browse 0|1|2`

`-free_browse` is a method that allows users to get around the checking that the server does when browsing images (owner/group). By default, normal users are not allowed to browse into scheduled backups on NT.

`0` = Allow

`1` = Deny

`2` = Use

By default, both the client and the server should be set up to `0` (allow). In order to free browsing to occur, either the client or the server must be setup to `2` (use) and neither can be setup for `1` (deny).

`-H` List host specific client information.

`-L` List all client information.

`-M` *master_server*

Name of the master server containing the client entries. The first server name in the local configuration is the default master server.

`-no_callback 0|1`

`0` = When connecting to the client's `bpcd`, the client connects back to the server on a random port number (default).

`1` = When connecting to client's `bpcd`, the client connects back to the server on the `vnetd` port number.

`-list_restore 0|1|2|3`

`-list_restore` can be set up on the server to disallow list and/or restore requests from a particular client. The value that is found in the client database overrides the `bp.conf` file setting.

`0` = Not specified (default)

`1` = Allow both list and restore requests

`2` = Allow list requests only

`3` = Deny both list and restore requests

`-max_jobs number [1-99]`

Specify the maximum number of jobs allowed to run concurrently on this client, up to 99.

`-update` Update an existing client entry.

bpconfig

NAME

`bpconfig` - Modify or display the global configuration attributes for NetBackup

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpconfig [-cd` *seconds*`] [-ha` *hours*`] [-kl` *days*`] [-kt` *days*`] [-ma` *address*`] [-mdtm` *drives*`] [-mj` *number*`] [-period` *hours*`] [-prep` *hours*`] [-to` *seconds*`] [-max_copies` *2...10*`] [-tries` *times*`] [-wi` *minutes*`] [-v] [-M` *master_server*`, . . .]`

install_path`\NetBackup\bin\admincmd\bpconfig [-L | -l | -U] [-v] [-M` *master_server*`, . . .]`

DESCRIPTION

`bpconfig` modifies or displays the NetBackup global configuration attributes. These attributes affect operations for all policies and clients. With the exception of the NetBackup administrator's email address, the default values for these attributes should be adequate for most installations. The section on NetBackup Global Attributes, in the *NetBackup System Administrator's Guide* describes the implications of setting the attribute values.

- The first form of `bpconfig` modifies one or more of the NetBackup global configuration attributes. At least one option that changes a NetBackup global configuration attribute must be on the command line.
- The second form of `bpconfig` displays the current settings of the NetBackup global configuration attributes. See the section DISPLAY FORMATS for more detail on the displays.

Errors are sent to `stderr`. A log of the command's activity is sent to the NetBackup admin log file for the current day.

This command requires administrator privileges.

OPTIONS

`-cd` *seconds*

The number of seconds that is the Compress-image-Database time interval. When seconds is a positive integer, an image will be compressed after this number of seconds has elapsed since the creation of the image. On Windows NT, NetBackup uses NTFS file compression only if the database is in an NTFS partition. Otherwise, it is not compressed.

The effect of compression is that less disk space is needed for the image database. However, when browsing the image database for restoring, the images need to be decompressed before they can be searched. While browsing for a restore, the compressed images will not be found. To decompress the images, you must use bpimage(1m).

The default is 0, which means no compression is done.

`-cd` *drives*

The maximum drives for this master, the maximum number of drives for this master and remote media server cluster that the master server should consider available when scheduling backups. An appropriate value for this attribute is the physical number of drives, counting shared drives only once, in the master and media server cluster. *drives* must be less than or equal to the number permitted by the version of NetBackup that is installed on the server (that is, 2 for NetBackup BusinesServer and unlimited for NetBackup DataCenter). *drives* is a non-negative integer. The default is 0 (unlimited).

`-ha` *hours*

The number of *hours* ago that is the beginning of the time range for selecting NetBackup report entries. The end of the time range is the current time. For instance, if *hours* ago is 24 and if you request a Backup Status report at 10:00 a.m., the report includes all backups run from 10:00 a.m. yesterday until 10:00 a.m. today. This value is used to calculate the time range for general reports and media reports. General reports include Backup Status, Client Backups, Problems, and All Log Entries. Media reports include Media List, Media Summary, Media Contents, Images on Media, and Media Log Entries. Hours Ago is a positive integer. The default value is 24 hours.

`-kl` *days*

The number of days to keep logs. This determines how long the NetBackup master server keeps its Error database and debug logs. NetBackup derives its Backup Status, Problems, All Log Entries, and Media Log Entries reports from the Error database, so this value limits the period that these reports can cover. The default is 28 days.

Note This attribute has no effect on remote media servers or clients (remote media servers apply only to NetBackup DataCenter).

`-kt` *days*

The number of days to Keep True-image-recovery (TIR) data. This determines how long to keep TIR information for those policies that have specified that TIR information is to be collected. The default is 1 day.

`-L` The list type is long. See the section DISPLAY FORMATS for more detail.

`-l`
The list type is short. This is the default if the command line has no list-type option (for instance, if you enter "`bpconfig`" and a carriage return). See the section DISPLAY FORMATS for more detail.

`-M` *master_server,...*
A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-ma` *address*
The mail address for the NetBackup administrator. This is the email address to which NetBackup sends notification of failed automatic backups, administrator-directed manual backup operations, and automatic database backups. The default is NULL (no email address).

If no address is provided, the current setting of the Admin Mail Address is cleared. This means that notification no longer will be sent by email to the NetBackup administrator.

`-max_copies` *2...10*
Specify the maximum number of copies per backup. Copies can range from between 2 and 10. The default is 2.

`-mhto` *seconds*
The multihosted-media-mount timeout, the length of time, in seconds, that NetBackup waits for a shared medium to be mounted, positioned, and become ready on backups and restores. Use this timeout to eliminate excessive waits when a shared medium is being used by another server. The default is 0, which means no timeout (unlimited wait time).

MultiHosted Drives is a separately-priced feature of NetBackup. For more information, see Multihosted Drives (Drive Sharing) in the Media Manager Reference Topics section of the *Media Manager System Administrator's Guide*.

`-mj` *number*
Specifies the maximum jobs per client. This is the maximum number of jobs that a client may perform concurrently. number must be a positive integer. The default is 1.

`-period` *hours*
The time interval associated with the configured number of tries for a backup (see `-tries`). This is the period, in hours, during which NetBackup will attempt a backup job for a client / policy / schedule combination for as many tries as configured. hours must be a positive integer. The default is 12 hours.

Note This attribute does not apply to user-directed backups and archives.

`-prep` *hours*

The preprocessing interval. This is the minimum time in hours between client queries to discover new paths if NetBackup is using auto-discover-streaming mode. For additional information, see the "Setting the Preprocess Interval for Auto Discovery" section in the topic on File-List Directives for Multiple Data Streams in the *NetBackup System Administrator's Guide*.

The default Preprocessing Interval value is 4 hours. If the preprocessing interval is changed, it can be changed back to the default by specifying `-prep -1`.

The preprocessing interval can be set for immediate preprocessing by specifying `0` as the preprocess interval for auto discovery on the `bpconfig` command line.

The maximum Preprocessing Interval is 48 hours.

`-to` *seconds*

This is the media-mount timeout, the length of time, in seconds, that NetBackup waits for the requested media to be mounted, positioned, and become ready on backups and restores. Use this timeout to eliminate excessive waits when it is necessary to manually mount media (for example, when robotic media is out of the robot or off site).

The default is 0, which means no timeout (unlimited wait time). If seconds is not 0, its value must be 300 (5 minutes) or greater.

`-tries` *times*

The number of retries for a backup, during the configured time period (see `-period`). NetBackup tries to run a backup job for a given client / policy / schedule combination this many times in the configured period. This allows you to limit the number of backup attempts should repeated failures occur.

Note This attribute does not apply to user-directed backups and archives.

Usually the number of tries should be greater than 0. Specifying 0 for the number of tries is legal but stops all scheduled backups. The default is 2 tries. If defaults are used for both `-tries` and `-period`, NetBackup will attempt the backup 2 times in 12 hours.

`-U` The list type is user. See the section DISPLAY FORMATS for more detail.

`-v`

Select verbose mode for logging. This is only meaningful when running with debug logging turned on (the *install_path*`\NetBackup\logs\admin` directory is defined).

`-wi` *minutes*

This is the wakeup Interval, the length in time in minutes that the scheduler waits before checking if any automatic backups are scheduled to begin. A long wakeup interval can cause the scheduler to miss too much of the backup window to complete its backups. The default is 10 minutes.

DISPLAY FORMATS

`bpconfig` uses three different formats to display the current values of the NetBackup global configuration attributes.

- User Display Format (`-U`)

  If the command line contains `-U`, the display format is user. The user display format is the format used by `bpadm` and the NetBackup graphical-user interfaces. This option produces a listing with one global attribute per line. Each line has the form *global attribute descriptor*: *value*. This listing is similar to the `-L` format, except that the global attribute descriptors are more explicit:

  Admin Mail Address

  Wakeup Interval

  Max Simultaneous Jobs / Client

  Backup Tries (x tries in y hours)

  Keep Error / Debug Logs

  Max drives this master

  Keep TrueImageRecovery Info

  Compress Image DB Files

  Media Mount Timeout

  Multihost Media Mount Timeout

  Display Reports

  Preprocess Interval

- Long Format (`-L`)

  If the command line contains `-L`, the display format is long. This option produces a listing with one global attribute per line, in the format *global attribute descriptor*: *value*. The fields in this display are as follows:

Mail Admin

Wakeup Interval

Max Jobs / Client

Backup Tries (x in y hours)

Keep Logs

Max drives / master

Compress DB Files

Media Mnt Timeout

Multihost Timeout

Postprocess Image

Display Reports

Keep TIR Info

Prep Interval

- Short Format (`-l`)

  If the `bpconfig` command line contains `-l` or contains no list-format option, the display format is short. This produces a terse listing. This option can be useful for scripts or programs that rework the listing into a customized report format. The listing layout is a single line containing the values for all global attributes. The attributes appear in the following order, separated by blanks. For those attributes that are expressed in units of time, the time units follow the attributes in parentheses:

  NetBackup administrator email address

  Wakeup interval (minutes)

  Time period (hours)

  Maximum simultaneous jobs per client

  Tries per period

  Keep logs (days)

  Maximum drives this master

  Compress image database interval (seconds; 0 denotes no compression)

  Media mount timeout (seconds; 0 denotes unlimited)

  Multihosted-media-mount timeout (seconds; 0 denotes unlimited)

  Postprocess images flag (0 denotes deferred, otherwise immediate)

  Display reports from <x> hours ago (hours)

Keep TIR information (days)

Preprocessing interval (hours)

- Example of How the Formats Differ

  Here is an example of how the display formats differ. `bpconfig` runs with each of the three display formats on a NetBackup installation. The NetBackup global attributes are the same for the three displays.

  The first display format, `-U`, looks like this:

```
bpconfig -U
Admin Mail Address:
Wakeup Interval:              1 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                 2 time(s) in 12 hour(s)
Keep Error/Debug Logs:        28 days
Max drives this master:       0
Keep TrueImageRecovery Info:  1 days
Compress Image DB Files:      (not enabled)
Media Mount Timeout:          0 minutes (unlimited)
Multihost Media Mount Timeout:0 minutes (unlimited)
Display Reports:              24 hours ago
Preprocess Interval:          0 hours
Maximum Backup Copies:    10
```

  The second display format, `-L`, looks like this:

```
bpconfig -L
Mail Admin:          *NULL*
Wakeup Interval:     1 minutes
Max Jobs/Client:     1
Backup Tries:        2 in 12 hours
Keep Logs:           28 days
Max drives/master:   0
Compress DB Files:   (not enabled)
Media Mnt Timeout:   0 minutes (unlimited)
Multihost Timeout:   0 minutes(unlimited)
Postprocess Image:   immediately
Display Reports:     24 hours ago
Keep TIR Info:       1 days
Prep Interval:       0 hours
Maximum Backup Copies: 10
```

  The third display format, `-l`, looks like this:

```
bpconfig -l
*NULL* 1 12 1 2 28 0 0 0 0 1 24 1 0
```

  The display fields for the `-l` display are interpreted as follows:

NetBackup administrator email address has not been set

Wakeup interval is 1 minute

Time period is 12 hours

Maximum simultaneous jobs per client is 1

Tries per period is 2

Keep logs for 28 days

Maximum drives this master is 0

Compress image database interval is 0 seconds; 0 denotes no compression

Media mount timeout is 0seconds; 0 denotes unlimited

Multihosted-media-mount timeout is 0 seconds; 0 denotes unlimited

Postprocess images flag is 1 (immediate)

Display reports from 24 hours ago

Keep TIR information for 1 day

Preprocessing interval is 0 hours

EXAMPLES

- Example 1

  While running on the master server kiwi, display the global attribute settings on the master server plum:

```
bpconfig -U -M plum

Admin Mail Address:           ichabod@null.null.com
Wakeup Interval:              10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                 1 time(s) in 8 hour(s)
Keep Error/Debug Logs:        6 days
Max drives this master:       0
Keep TrueImageRecovery Info:  1 days
Compress Image DB Files:      (not enabled)
Media Mount Timeout:          30 minutes
Multihost Media Mount Timeout:0 minutes (unlimited)
Display Reports:              24 hours ago
Preprocess Interval:          0 hours
Maximum Backup Copies:    10
```

- Example 2

Set the Compress-image-database interval to 604800 seconds, so that NetBackup compresses images more than 7 days old:

```
bpconfig -cd 604800
bpconfig -U

Admin Mail Address:
Wakeup Interval:              10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                 2 time(s) in 12 hour(s)
Keep Error/Debug Logs:        28 days
Max drives this master:       0
Keep TrueImageRecovery Info:  2 days
Compress Image DB Files:      older than 7 day(s)
Media Mount Timeout:          0 minutes (unlimited)
Multihost Media Mount Timeout:0 minutes (unlimited)
Display Reports:              24 hours ago
Preprocess Interval:          0 hours
Maximum Backup Copies:         10
```

- Example 3

  Set the Media Mount Timeout to 1800 seconds.

```
bpconfig -to 1800
bpconfig -U

Admin Mail Address:           sasquatch@wapati.edu
Wakeup Interval:              10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                 1 time(s) in 12 hour(s)
Keep Error/Debug Logs:        3 days
Max drives this master:       0
Keep TrueImageRecovery Info:  24 days
Compress Image DB Files:      (not enabled)
Media Mount Timeout:          30 minutes
Multihost Media Mount Timeout:0 minutes (unlimited)
Display Reports:              24 hours ago
Preprocess Interval:          0 hours
Maximum Backup Copies:         10
```

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bpconfig: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\config\behavior`

SEE ALSO

`bpimage`

See the *NetBackup Media Manager System Administrator's Guide* for information on MultiHosted Drives.

bpdbjobs

NAME

`bpdbjobs` - Interact with the NetBackup jobs database

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpdbjobs [-report] [-M` *master_server*`] [-file` *pathname*`] [-append] [-vault | -lvault | -all_columns]`

install_path`\NetBackup\bin\admincmd\bpdbjobs -summary [-M` *master_server*`] [-file` *pathname*`] [-append] [-U | -L | -all_columns]`

install_path`\NetBackup\bin\admincmd\bpdbjobs -delete [-M` *master_server*`]` *job1,job2,...jobn*

install_path`\NetBackup\bin\admincmd\bpdbjobs -cancel [-M` *master_server*`]` *job1,job2,...jobn*

install_path`\NetBackup\bin\admincmd\bpdbjobs -cancel_all [-M` *master_server*`]`

install_path`\NetBackup\bin\admincmd\bpdbjobs -clean [-M` *master_server*`] [-keep_hours` *hours* `| -keep_days` *days*`] [-keep_successful_hours` *hours* `| -keep_successful_days` *days*`]`

install_path`\NetBackup\bin\admincmd\bpdbjobs -version`

install_path`\NetBackup\bin\admincmd\bpdbjobs -help`

DESCRIPTION

`bpdbjobs` interacts with the jobs database and is useful in scripts or as a command line administration tool. Use `bpdbjobs` to print the entire jobs database, print a summary, delete done jobs, cancel uncompleted jobs, and clean old jobs.

This command requires administrator privileges.

OPTIONS

`-all_columns`
: Summary displays all columns.

`-append`
: Appends the output to the file specified by the `-file` option. If no `-file` option is provided, the output goes to `stdout`.

`-cancel` Causes `bpdbjobs` to cleanly cancel active jobs with a Status 150, displayed in the Activity Monitor. For example:

```
bpdbjobs -cancel 11328
bpdbjobs -cancel 11328,11329,11330
```

`-cancel_all`
Causes `bpdbjobs` to cleanly cancel all uncomplete jobs with a Status 150, displayed in the Activity Monitor. For example:

```
bpdbjobs -cancel_all
```

`-clean` Causes `bpdbjobs` to delete done jobs that are older than a specified time period. Use with the `-keep_hours` or `-keep_days`, or `-keep_successful_hours` or `-keep_successful_days` parameters to specify a retention period. For example,

`bpdbjobs` -clean -keep_hours 30

`-delete` Causes completed jobs that are displayed in the Activity Monitor to be deleted.

Multiple jobids can be deleted in one command. For example:

```
bpdbjobs -delete 11328
bpdbjobs -delete 11328,11329,11330
```

`-file` *pathname*
Names a file to which the output of `bpdbjobs` will be written. If no `-file` option is provided, the output goes to `stdout`.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-keep_days` *days*
Use with the `-clean` option to specify how many days `bpdbjobs` keeps done jobs. Values outside of 1 to 30 range are ignored. Default is 3 days.

`-keep_hours` *hours*
Use with the `-clean` option to specify how many hours `bpdbjobs` keeps done jobs. Values outside of 3 to 720 range are ignored. Default is 72 hours.

`-keep_successful_days` *days*
Use with the `-clean` option to specify how many days `bpdbjobs` keeps successful done jobs. Values outside of 1 to 30 range are ignored. Default is 3 days.

This value must be less than the `-keep_days` value.

`-keep_successful_hours` *hours*

Use with the `-clean` option to specify how many hours `bpdbjobs` keeps successful done jobs. Values outside of 3 to 720 range are ignored. Default is 72 hours.

This value must be less than the `-keep_hours` value.

`-L` Report in long format.

`-lvault` Displays additional columns specific to Vault jobs.

`-M` *master_server*

Applies to an environment where there are multiple masters servers.

Use the `-M` option to:

Summarize jobs for a specific master server.

Delete jobid(s) for a specific master server.

Cancel jobid(s) for a specific master server.

Cancel all active jobids for a specific master server.

`-report` Provides a report of data stored in the Activity Monitor. If no option is specified with `bpdbjobs`, `-report` is the default option.

`-summary [-U | -L | -all_columns]`

Causes a summary line to be printed to `stdout` of all jobs stored in `NBU/jobs`.

Parameters `-U` and `-L` format the output of the command.

Use the `-file` option to write the output to a given directory/filename. For example:

```
bpdbjobs -summary -U -file /tmp/summary.out
```

`-U` Report in user format. This is the report format used by NetBackup report-generating tools such as the NetBackup-Java Reports application.

`-vault` Displays additional columns specific to Vault jobs.

`-version`

Causes `bpdbjobs` to print the version string, then halt. Any other switches are ignored.

FILES

install_path`\NetBackup\logs\bpdbjobs\*`

install_path`\NetBackup\db\config\behavior`

bpduplicate

NAME

`bpduplicate` - Create a copy of backups created by NetBackup.

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpduplicate -npc` *new_primary_copy* `-backupid` *backup_id* `[-local] [-client` *name*`]`

install_path`\NetBackup\bin\admincmd\bpduplicate [-number_copies` *number*`] [-dstunit` *destination_storage_unit_label*`[,`*copy2*`,...,`*copyn*`] [-dp` *destination_pool_name*`[,`*copy2*`,...,`*copyn*`] [-p | -pb | -PD | -PM] [-Bidfile` *file_name*`] [-v] [-local] [-client` *name*`] [-st` *sched_type*`] [-sl` *sched_label*`] [-L` *output_file* `[-en]] [-shost` *source_host*`] [-policy` *name*`] [-s` *mm/dd/yyyy hh:mm:ss*`] [-e` *mm/dd/yy hh:mm:ss*`] [-pt` *policy_type*`] [-hoursago` *hours*`] [[-cn` *copy_number*`] | [-primary]][-M` *master_server*`] [-altreadhost` *hostname*`] [-backupid` *backup_id*`] [-id` *media_id*`] [-rl` *retention_level*`[,`*rl-copy2*`,...,`*rl-copyn*`]] [-fail_on_error` `0|1[,..., 0|1]] [-mpx] [-set_primary` *copy_index*`]`

DESCRIPTION

The `bpduplicate` command allows a copy of a backup to be created. The `bpduplicate` command can also change the primary copy in order to enable restoring from a duplicated backup. The primary copy is used to satisfy restore requests and is initially the original copy.

Multiplexed duplications can be created by using the `-mpx` option. Refer to the discussion of the `-mpx` option for more information.

The duplicated backup has a separate expiration date from the original. Initially, the expiration date of the copy is set to the expiration date of the original. You can change the expiration date of the copy or the original by using the `bpexpdate` command.

Use `bpduplicate` to create up to 10 copies of unexpired backups.

OPTIONS

`-altreadhost` *hostname*

Specify an alternate host from which to read the media. The default is that `bpduplicate` reads the source media from the host that performed the backup.

`-backupid` *backup_id*
Specifies the backup ID of a single backup to duplicate or for which to change the primary copy.

`-Bidfile` *file_name*
file_name specifies a file that contains a list of backup IDs to be duplicated. List one backup ID per line in the file. If this parameter is specified, other selection criteria is ignored.

`-client` *name*
Specifies the name of the client that produced the originals and is used as search criteria for backups to duplicate. The default is all clients.

When specified with the `-npc` option in order to change the primary copy, this indicates that NetBackup will first search for the backup ID belonging to the specified client. This is useful if the client name has changed.

`-cn` *copy_number* | `-primary`
Determines the copy number to duplicate. Valid values are 1 through 10. The default is 1.

`-primary` indicates to `bpduplicate` to search or duplicate the primary copy.

`-dp` *destination_poolname [,copy2,...,copyn]*
Specifies the volume pool for the duplicates. NetBackup does not verify that the media ID selected for the duplicate copy is not the same media ID where the original resides. Therefore, to avoid the possibility of a deadlock, specify a different volume pool than where the original media ID resides. The default pool name is NB_duplicates.

Specify a pool for each copy specified.

`-dstunit` *destination_storage_unit_label [,copy2,...,copyn]*
Specifies the destination storage unit. This parameter is required to duplicate backups. Do not specify this option to preview backups to be duplicated (`-p`, `-pb`, `-PM`, or `-PD` options) or to change the primary copy (`-npc` option). This option does not have a default.

Specify a storage unit for each copy specified.

`-e` *mm/dd/yy* `[`*hh*`[:`*mm*`[:`*ss*`]]]`

`-s` *mm/dd/yy* `[`*hh*`[:`*mm*`[:`*ss*`]]]`
Specifies the end (`-e`) or start (`-s`) of the range of dates and times that include all backups to duplicate.The default end date is the current date and time. The default start time is 24 hours prior to the current data and time.

`-fail_on_error 0|1[,0|1,...,0|1]`

Specifies whether to fail the other duplications if the copy fails, where:

0 = Do not fail the other copies

1 = Fail other copies

Specify one for each copy specified.

`-hoursago` *hours*

Specifies number of hours prior to the current time to search for backups. Do not use with the `-s` option. The default is the previous midnight.

`-id` *media_id*

Search the image catalog for backups to duplicate that are on this media ID. If the original is fragmented between different media IDs, NetBackup duplicates only the backups that exist on the specified media ID. Backups that span media are duplicated, but not any other backups on the spanned media ID.

`-L` *output_file* `[-en]`

Specifies the name of a file in which to write progress information. The default is to not use a progress file.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-local`

When `bpduplicate` is initiated from a host other than master server and the `-local` option is *not* used (default), `bpduplicate` starts a remote copy of the command on the master server.

The remote copy allows the command to be terminated from the **Activity Monitor**.

Use the `-local` option to prevent the creation of a remote copy on the master server and to run the `bpduplicate` only from the host where it was initiated.

If the `-local` option is used, `bpduplicate` cannot be canceled from the **Activity Monitor**.

`-M` *master_server*

Specifies the master server that manages the media catalog that has the media ID. If this option is not specified, the default is one of the following:

For NetBackup BusinesServer:

NetBackup BusinesServer supports only one server (the master) with no remote media servers. Therefore, the default in this case is always the NetBackup BusinesServer master where you run the command.

For NetBackup DataCenter:

If the command is run on a master server, then that server is the default.

If the command is run on a media server that is not the master, then the master for that media server is the default.

`-mpx` Specifies that when duplicating multiplexed backups, NetBackup will create multiplexed backups on the destination media. This reduces the time to duplicate multiplexed backups.

Multiplexed duplication is not supported for:

- Non-multiplexed backups
- Backups from disk type storage units
- Backups to disk type storage units
- FlashBackup or NDMP backups

If backups in the above categories are encountered during duplication, NetBackup duplicates them first and uses non-multiplexed duplication. Then, the multiplexed backups are duplicated by using multiplexed duplication.

If all the backups in a multiplexed group are not duplicated, the duplicated multiplexed group will have a different layout of fragments. (A multiplexed group is a set of backups that were multiplexed together during a single multiplexing session.)

If this option is not specified, all backups are duplicated using non-multiplexed duplication.

For more information on multiplexing, see the *NetBackup System Administrator's Guide.*

`-npc` *new_primary_copy*

Allows the primary copy to be changed. The value can be `1` through `10`. The `-backupid` option must be specified with this option.

`-number_copies` *number*

Specifies the number of copies to be created. Without the Inline Tape Copy option or NetBackup Vault extension installed, the value can only be set to 1. The default is 1.

Use with `-dstunit`, `-dp`, `-fail_on_error`, and `-r1`:

`-number_copies 2 -dstunit` *stunit-copy1 , stunit-copy2*

`-number_copies 2 -dp pool1,pool2`

`-p` Previews backups to be duplicated according the option settings, but does not perform the duplication. Displays the media IDs, server name, backups that are not candidates for duplication (and why), and information about the backups to be duplicated.

`-pb` Previews the duplication but does not perform the duplication. Similar to the `-p` option, but does not display information about the backups.

`-PD` Same as the `-PM` option, except the backups are sorted and displayed by date and time (newest to oldest).

`-PM` Displays information on the backups to be duplicated according to the option settings, but does not perform the duplication. This format first displays the backup IDs that cannot be duplicated and why (for example, because the backup already has two copies). It then displays the following information about the backup: date and time of the backup, policy, schedule, backup ID, host, media ID or path, copy number, and whether the copy is the primary copy (0 or 1):

1 = Primary copy

0 = Not primary copy

`-policy` *name*
Search for backups to duplicate in the specified policy. The default is all policies.

`-pt` *policy_type*
Search for backups created by the specified policy type. The default is any policy type.

Valid values are:

```
Informix-On-BAR
Oracle
Macintosh
MS-Exchange-Server
MS-Windows-NT
MS-SQL-Server
NDMP
Netware
OS/2
Standard
Sybase
```

Note The following policy types apply only to NetBackup DataCenter.

```
AFS
Apollo-wbak
DataTools-SQL-BackTrack
DB2
```

FlashBackup

SAP

Split-Mirror

`-rl` *retention_level* `[`*,rl-copy2*`, . . . ,`*rl-copyn*`]`

Provides a retention level for each copy specified.

If no retention levels are specified, the expiration date of the original copy is used for each copy. If a retention period is indicated, the expiration date for the copy is the backup date plus the retention period.

For example, if a backup was created on November 14, 2001, and its retention period is one week, the new copy's expiration date is November 21, 2001.

A value of `-1` indicates that the original expiration date is used for the copy.

`-set_primary` *copy_index*

Specify a new copy to become the primary copy.

copy_index is one of the following:

`0` = Do not change the primary copy (default)

`1` = First new copy will be the primary copy

`2` = Second new copy will be the primary copy

`3` = Third new copy will be the primary copy, and so on.

copy_index cannot be greater than the `bpduplicate -number_copies` value.

If the copy specified to be the primary copy fails, but other copies are successful, the primary copy will not change from its current value.

`-shost` *source_host*

Specifies that only the backups created on the specified backup server are considered for duplication. The default is to consider all backups regardless of the backup server.

`-sl` *sched_label*

Search for backups to duplicate that were created by the specified schedule. The default is all schedules.

`-st` *sched_type*

Search for backups to duplicate that were created by the specified schedule type. The default is any schedule type.

Valid values are:

`FULL` (full backup)

`INCR` (differential-incremental backup)

	`CINC` (cumulative-incremental backup) `UBAK` (user backup) `UARC` (user archive) `NOT_ARCHIVE` (all backups except user archive)
`-v`	Selects verbose mode. When specified, the debug and progress logs include more information.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the output for the `-s` and `-e` options:

```
[-s mm/dd/yyyy HH:MM:SS] [-e mm/dd/yyyy HH:MM:SS]
```

Notice the month / day / year and hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales.

EXAMPLES

- Example 1

  The following command (all on one line) lists backups with a copy number of 1, that were backed up by the policy named stdpolicy, and created between July 1, 2001, and August 1, 2001.

```
bpduplicate -PM -cn 1 -policy stdpolicy -s 07/01/01 -e 08/01/01
```

- Example 2

  The following command (all on one line, or using a backslash continuation character) duplicates copy 1 of the backups listed in file `C:\tmp\bidfile`. The destination storage unit is unit1 and the destination pool is dup_pool. Progress information is written to `C:\tmp\bpdup.ls`.

```
bpduplicate -dstunit unit1 -Bidfile C:\tmp\bidfile \
-L C:\tmp\bpdup.ls -dp dup_pool -cn 1
```

- Example 3

  The following command (all on one line, or using a backslash continuation character) is the same as the prior example, except multiplexed backups are duplicated using multiplexed duplication.

```
bpduplicate -dstunit unit1 -Bidfile C:\tmp\bidfile \
-mpx -L C:\tmp\bpdup.ls -dp dup_pool -cn 1
```

FILES

install_path`\NetBackup\db\images\*`

install_path`\NetBackup\logs\admin\*`

bperror

NAME

`bperror` - Display NetBackup status and troubleshooting information or entries from the NetBackup error catalog.

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bperror {-S | -statuscode` *status_code*`} [-r|-recommendation] [-p | -platform Unx | NTx] [-v]`

install_path`\NetBackup\bin\admincmd\bperror [-all | -problems |-media | {-backstat [-by_statcode]}] [-L | -l | -U] [-columns` *ncols*`] [-d` *mm/dd/yyyy hh:mm:ss* `| -hoursago` *hours*`] [-e` *mm/dd/yyyy hh:mm:ss*`] [-client` *client_name*`] [-server` *server_name*`] [-jobid` *job_id*`] [-M` *master_server*`, ...] [-v]`

install_path`\NetBackup\bin\admincmd\bperror [-s {`*severity*`[+]}|`*severity*` ...] [-t` *type* `...] [-L | -l|-U] [-columns` *ncols*`] [-d` *mm/dd/yyyy hh:mm:ss* `| -hoursago` *hours*`] [-e` *mm/dd/yyyy hh:mm:ss*`] [-client` *client_name*`] [-server` *server_name*`] [-jobid` *job_id*`] [-M` *master_server*`, ...] [-v]`

DESCRIPTION

`bperror` displays information from either the same source as the online troubleshooter (in the Activity Monitor or Reports applications) or from the NetBackup error catalog. `bperror` provides the following types of displays:

- A display of the message that corresponds to a status code and, optionally, a recommendation on how to troubleshoot the problem. In this case, the display results come from the same source as the online troubleshooter for the local system.
- A display of the error catalog entries that satisfy the command-line options. For instance, `bperror` can display all the problem entries for the previous day.
- A display of the error catalog entries that correspond to a particular message severity and/or message type.

For information on details of the displays, see DISPLAY FORMATS later in this command description.

`bperror` writes its debug log information to the *install_path*`\NetBackup\logs\admin` directory. You can use the information in this directory for troubleshooting.

The output of bperror goes to standard output.

Only the administrator can run this command.

OPTIONS

`-all`

`-backstat [-by_statcode]`

`-media`

`-problems`

These options specify the type and severity of log messages to display. The default type is ALL. The default severity is ALL.

For `-all`: The type is ALL, and severity is ALL. Running `bperror` with this option and `-U` produces an All Log Entries report.

For `-backstat`: The type is BACKSTAT, and severity is ALL. If `-by_statcode` is present, the display contains one entry for each unique status code. Line 1 of the entry contains the status code and the corresponding message text. Line 2 of the entry contains the list of clients for which this status code occurred. `-by_statcode` is only valid when the command line contains both `-backstat` and `-U`. Running bperror with this option and `-U` produces a Backup Status report.

For `-media`: The type is MEDIADEV, and severity is ALL. Running `bperror` with this option and `-U` produces a Media Logs report.

For `-problems`: The type is ALL, and severity is the union of WARNING, ERROR, and CRITICAL. Running `bperror` with this option and `-U` produces a Problems report.

`-client` *client_name*

Specifies the name of a NetBackup client. This name must be as it appears in the NetBackup catalog. By default, `bperror` searches for all clients.

`-columns` *ncols*

For the `-L` and `-U` reports, `-columns` provides an approximate upper bound on the maximum line length. `bperror` does not attempt to produce lines exactly *ncols* characters in length.

`-columns` does not apply to the -l report.

ncols must be at least 40. The default is 80.

`-d` *mm/dd/yy* [*hh*:*mm*:*ss*]

`-e` *mm/dd/yy* [*hh*:*mm*:*ss*]

Specifies the start and end date range for the listing.

`-d` specifies a start date and time for the listing. The resulting list shows only images in back ups or archives that occurred at or after the specified date and time. Use the following format:

mm/dd/yy [*hh*[:*mm*[:*ss*]]]

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is 24 hours before the current date and time.

The method you use to specify the date and time is dependent on the `locale` setting for your system. See NOTES.

`-e` specifies an end date and time for the listing. The resulting list shows only files from backups or archives that occurred at or before the specified date and time. Use the same format as for the start date. The default is the current date and Time. The end date must be greater than or equal to the start date.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-hoursago` *hours*
Specifies a start time of this many hours ago. This is equivalent to specifying a start time (`-d`) of the current time minus hours. Hours is an integer. The default is 24, meaning a start time of 24 hours before the current time.

`-jobid` *job_id*
Specifies a NetBackup job ID. By default, `bperror` searches for all job IDs.

`-L` Report in long format.

`-l` Report in short format. This produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format. This is the default list type.

`-M` *master_server*
A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-p Unx | NTx`

`-platform Unx | NTx`
Display the message that applies to the platform (UNIX or Windows) for the specified status code. The default is to display the message for the platform on which `bperror` is running. The `-S` or `-statuscode` option must be specified when using this option.

`-r | -recommendation`

Display the recommended action for the specified status code from the troubleshooting guide. The default is not to display the recommended action. The `-S` or `-statuscode` option must be specified when using this option.

`-S` *status_code*

`-statuscode` *status_code*

Display the message that corresponds to the status code. There is no default for this option.

`-s` *severity*

`-s` *severity*+

Specifies the severity of log messages to display. The defined values are `ALL`, `DEBUG`, `INFO`, `WARNING`, `ERROR`, and `CRITICAL`.

There are two ways to specify severity. The first way is a list of one or more severity values. For instance, "`-s INFO ERROR`" displays the messages with either severity `INFO` or severity `ERROR`. The delimiter between the elements in the list must be a blank (" "). The second way is a single severity value with "+" appended, meaning this severity or greater. For instance "`-s WARNING+`" displays the messages with severity values `WARNING`, `ERROR`, and `CRITICAL`.

The default is `ALL`. The severity value can be in either upper or lower case.

`-server` *server_name*

Specifies the name of a NetBackup server. This name must be as it appears in the NetBackup catalog. The display is limited to messages logged for this server, which also satisfy the other criteria specified by `bperror` options. For instance, if `-server plum` and `-hoursago 2` are `bperror` options, the display contains messages logged for the media server plum in the past two hours.

The server name must match the server name recorded in the log messages. For instance, if the logs record the server name as `plum.null.null.com`, specifying `-server plum` will not display the logs, but `-server plum.null.com` will.

The query goes to the error catalog residing on the master server (either the local master server or the master server specified by -M). The master server must allow access by the system running bperror.

The default is to display log messages for all media servers known to the master server(s).

`-t` *type*

Specifies the type of log messages to display. The defined values are `ALL`, `BACKSTAT`, `MEDIADEV`, `GENERAL`, `BACKUP`, `ARCHIVE`, `RETRIEVE`, and `SECURITY`. The default is `ALL`. The type value can be in either upper or lower case. The type value is entered as a list of one or more values. For instance, "`-t BACKSTAT MEDIADEV`" displays the messages with either type `BACKSTAT` or type `MEDIADEV`. The delimiter between the elements in the list must be a blank (" ").

`-U` Report in user format. This is the report format used by NetBackup report-generating tools such as the NetBackup-Java Reports application.

`-v` Selects verbose mode. This option causes `bperror` to log additional information for debugging purposes. The information goes into the NetBackup-administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined). The default is not to be verbose.

DISPLAY FORMATS

STATUS CODE DISPLAY (for example, `bperror -S` *status_code*):

`bperror` queries the NetBackup online troubleshooter on the local system for the message that corresponds to the status code. `bperror` displays the message text on one line and an explanation on a second line.

If `-r` or `-recommendation` is an option, `bperror` also queries for the troubleshooting recommendation that corresponds to the status code. `bperror` displays the recommendation following the status message, on one or more lines.

ERROR CATALOG DISPLAY (for example, `bperror -all`; `bperror -s` *severity*):

`bperror` queries the NetBackup error catalog on either the local master server or the master servers in the `-M` option list. The display consists of the results returned from querying the error catalog on the master server(s). The results are limited to catalog entries that satisfy all the `bperror` options. For instance, if the `bperror` command line contains options for client, start time, and end time, then `bperror` reports only the jobs run for that client between the start and end times. For the display variant that shows individual message entries from the error catalog, the display can appear in long (`-L`), user (`-U`), or short (`-l`) format. For the display variant that categorizes by status code, the display can appear in user (`-U`) format only. The display content for each of these formats is as follows:

- Error catalog display, individual message entries, long format (for example, `bperror -media -L`). This report produces several lines per log entry, with the following contents:

  Line 1: Date and time

V:NetBackup version

S:Server

C:Client

J:Job ID

(U:Job group ID and an unused field) If multi-streaming is enabled for a policy, the job group ID is the job ID of the first job that spawned a collection of multi-streaming backups; if multi-streaming is disabled for the policy, the job group ID is always zero.

Line 2: Severity (severity name and severity code in hexadecimal)

Type (type name and type code in hexadecimal)

Who (name of the entity that added the log entry)

Line 3: Text (beginning of the log message text, continued on succeeding lines if necessary)

- Error catalog display, individual message entries, user format (for example., `bperror -media -U`). The user format produces a header line showing column names, and then one or more lines per log entry, with the following contents:

  Line 1: Date and time

  Server

  Client

  Text (beginning of the log message text, continued on succeeding lines if necessary)

- Error catalog display, individual message entries, short format (for example., `bperror -media -l`). The short format produces a single line per log entry, with the following contents:

  Line 1: Time (internal system representation)

  NetBackup version

  Type code (decimal)

  Severity code (decimal)

  Server

  Job ID

  Job Group ID

  An unused field

  Client

Who

Text (the entire log message text, with no truncation of the line length)

- Error catalog display categorized by status code. This display reports only each unique status code, instead of listing every log entry for that status code (for example, `bperror -backstat -by_statcode -U`). This produces two or more lines per status code, with the following contents:

  Line 1: Status code

  Text (the beginning of the log message text, continued on succeeding lines if necessary)

  Line 2: The list of clients for which this status occurred.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the part of the `bperror` usage output:

```
USAGE: bperror ...
            [-d mm/dd/yyyy hh:mm:ss|-hoursago hours]
            [-e mm/dd/yyyy hh:mm:ss] [-client client_name] ...
```

Notice the month/day/year and hours:minutes:seconds requirements for the `-d` and `-e` options. These are for a locale setting of C and can be different for other locales.

EXAMPLES

- Example 1

  Here `bperror` displays the error for a job that failed because the NetBackup encryption package was not installed. Status code 9 is the NetBackup status code for this failure. The second run of `bperror` displays the action recommended for NetBackup status code 9.

```
bperror -d 12/23/2001 16:00:00 -e 12/23/2001 17:00:00 -t backstat -U
STATUS    CLIENT    POLICY    SCHED    SERVER    TIME COMPLETED
9         plum      dhcrypt   user     plum      12/23/2001 16:38:09

      (an extension package is needed, but was not installed)

bperror -S 9 -r

      an extension package is needed but was not installed

      A NetBackup extension product is required in order to perform the
      requested operation.
```

```
   Install the required extension product.
```

- Example 2

  Here bperror reports, in User format, the problems that have occurred in the previous 24 hours.

```
   bperror -U -problems
TIME            SERVER CLIENT - TEXT
   11/23/2001 16:07:39 raisin - no storage units configured
   11/23/2001 16:07:39 raisin -  scheduler exiting - failed reading
   storage unit database information (217)
   11/23/2001 16:17:38 raisin -  no storage units configured
   11/23/2001 16:17:38 raisin -  scheduler exiting - failed reading
   storage unit database information (217)
   11/23/2001 16:26:17 raisin -  WARNING:  NetBackup database backup
   is currently disabled
   11/23/2001 18:11:03 raisin nut  bpcd on nut exited with status 59:
   access to the client was not allowed
   11/23/2001 18:11:20 raisin -  WARNING:  NetBackup database backup
   is currently disabled
```

- Example 3

  The following example displays status for type backstat for jobs run in the previous 24 hours. The option -by_statcode produces a display organized by status code.

  The display shows that one or more jobs for each of the clients chives, guava, plum, and raisin completed successfully (the status code is 0). In addition, one or more jobs for client nut failed because nut did not allow access by the master or media server (the status code is 59).

```
bperror -U -backstat -by_statcode
 0   the requested operation was successfully completed
   chives guava plum raisin
 59   access to the client was not allowed
   nut
```

- Example 4

  The following example identifies and retrieves the results for a particular user job. It first lists the log entries with job Ids other than zero. It then runs a User-format report on the job of interest.

```
bperror -hoursago 2000 -L | grep 'S:' | egrep 'J\:[1-9]'
   12/21/2001 17:24:14 V1 S:plum C:plum J:1 (U:0,0)
```

```
12/23/2001 16:31:04 V1 S:plum C:plum J:1 (U:0,0)

12/23/2001 16:31:06 V1 S:plum C:plum J:1 (U:0,0)

12/23/2001 16:38:04 V1 S:plum C:plum J:3 (U:0,0)

12/23/2001 16:38:07 V1 S:plum C:plum J:3 (U:0,0)

12/23/2001 16:38:08 V1 S:plum C:plum J:3 (U:0,0)

12/23/2001 16:38:09 V1 S:plum C:plum J:3 (U:0,0)

01/07/2000 13:12:31 V1 S:plum C:plum J:34 (U:0,0)

01/07/2000 13:12:36 V1 S:plum C:plum J:34 (U:0,0)

01/07/2000 13:12:40 V1 S:plum C:plum J:34 (U:0,0)

01/07/2000 13:12:41 V1 S:plum C:plum J:34 (U:0,0)


bperror -d 1/7/2000 -jobid 34 -U
 TIME            SERVER CLIENT - TEXT

01/07/2000 13:12:31 plum plum  started backup job for client plum,
policy jdhcrypt, schedule user on storage unit jdhcrypt

01/07/2000 13:12:36 plum plum  begin writing backup id
plum_0947272350, copy 1,fragment 1

01/07/2000 13:12:40 plum plum  successfully wrote backup id
plum_0947272350,copy 1, fragment 1, 32 Kbytes at 11.057 Kbytes/sec

01/07/2000 13:12:41 plum plum  CLIENT plum  POLICY jdhcrypt  SCHED
user EXIT STATUS 0 (the requested operation was successfully
completed)
```

- Example 5

  The following example shows the media entries in the error catalog for the past 2000 hours.

```
bperror -hoursago 2000 -media -U

TTIME            SERVER CLIENT - TEXT

12/23/2001 16:31:04 plum plum  media manager terminated during
mount of media id A00000, possible media mount timeout

12/24/2001 04:31:20 plum -  media id A00000 removed from media
manager database (manual deassign)
```

- Example 6

  The following example tallies and reports the total number of bytes backed up in the past 24 hours.

```
bperror -all -hoursago 24 | grep "successfully wrote backup id" |
awk '{bytes= bytes + $20} END {print "backed up",bytes," Kbytes of
data"}'
```

```
backed up 64  Kbytes of data
```

- Example 7

  The following example reports the performance, in Kbytes per second, for each of today's backups:

```
bperror -all | grep Kbytes
```

```
0912013673 1 4 4 hat 0 0 0 hat bptm successfully wrote backup id
hat_0912013584, copy 1, fragment 1, 32256 Kbytes at 891.222
Kbytes/sec
```

```
0912014210 1 4 4 hat 0 0 0 hat bptm successfully wrote backup id
hat_0912014132, copy 1, fragment 1, 32256 Kbytes at 1576.848
Kbytes/sec
```

```
0912016068 1 4 4 hat 0 0 0 hat bptm successfully wrote backup id
hat_0912015780, copy 1, fragment 1, 603136 Kbytes at 2645.960
Kbytes/sec
```

- Example 8

  Here `bperror` displays the status message and the recommended action for status code 0:

```
bperror -S 0 -r
```

```
the requested operation was successfully completed
```

```
There were no problems detected with the requested operation.
```

```
None, unless this was a database backup performed through a
database  extension product (for example, NetBackup for Oracle or
NetBackup for  SQL Server). In those instances, code 0 means the
backup script that  started the backup ran without error. However,
you must check other  status as explained in the related NetBackup
manual to see if the  database was successfully backed up.
```

FILES

install_path`\NetBackup\logs\admin\log.`*mmddyy*

install_path`\NetBackup\db\error\`*log files*

install_path`\NetBackup\bin\NbwTroub.dll`

install_path`\NetBackup\msg\.conf`

bpexpdate

NAME

`bpexpdate` - Change the expiration date of backups in the image catalog and media in the media catalog.

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpexpdate -m` *media_id* `-d` *mm/dd/yyyy hh/mm/ss* `0|infinity [-host` *name*`] [-force] [-M` *master_server*`, . . . ,` *master_server*`]`

install_path`\NetBackup\bin\admincmd\bpexpdate -deassignempty [-m` *media_id*`] [-host` *name*`] [-force] [-M` *master_server*`, . . . ,` *master_server*`]`

install_path`\NetBackup\bin\admincmd\bpexpdate -backupid` *backup_id* `-d` *mm/dd/yyyy hh/mm/ss* `0|infinity [-client` *name*`] [-copy` *number*`] [-force] [-M` *master_server*`, . . . ,` *master_server*`]`

install_path`\NetBackup\bin\admincmd\bpexpdate -recalculate [-backupid` *backup_id*`] [-copy` *number*`] -d` *mm/dd/yyyy hh/mm/ss* `0|infinity] [-client` *name*`] [-policy` *name*`] [-ret` *retention_level*`] [-sched` *type*`] [-M` *master_server*`, . . . ,` *master_server*`]`

DESCRIPTION

NetBackup maintains internal databases with backup image and media information. These internal databases are called catalogs. Both an image record in the image catalog and a media ID in the media catalog contain an expiration date. The expiration date is the date and time when NetBackup removes the record for a backup or media ID from the corresponding catalog.

The `bpexpdate` command allows the expiration date and time of backups to be changed in the NetBackup image catalog. It is also used to change the expiration of removable media in the NetBackup media catalog. If the date is set to zero, `bpexpdate` immediately expires backups from the image catalog or media from the media catalog. When a media ID is removed from the NetBackup media catalog, it is also deassigned in the Media Manager volume database, regardless of the media's prior state (FROZEN, SUSPENDED, and so on).

Changing the expiration can be done on a media ID basis or on an individual backup ID basis. Changing the expiration date of a media ID also causes the expiration date of all backups on the media to be changed. `bpexpdate` also provides options to deassign media from the media catalog if they no longer contain valid backups and to recalculate the expiration date based on the configured or a supplied retention level.

The different formats of the command are described below.

- `m`

  Changes the expiration date or removes the media ID from the media catalog and associated backups from the NetBackup catalog. A separate expiration date is maintained in the image catalog for each copy of a backup. When this format is used, only the expiration of the copy on the media is affected. If the media ID is removed from the media catalog by specifying a zero date, the media ID is also deassigned in the Media Manager volume database.

- `deassignempty`

  Searches the catalog for removable media that no longer contain valid backups, removes it from the media catalog, and deassigns the media IDs in the Media Manager catalog. The media is then available to be used again. You can use the NetBackup Images on Media report to determine if there are assigned media that no longer contain valid backups.

- `backupid`

  Changes the expiration of a single backup. If the date is zero, the backup is removed from the image catalog. If the backup is on removable media and the expiration date given by the `-d` option is greater than the current expiration of the media ID, the expiration date of the media ID in the media catalog is also changed. The change affects all copies of a backup, unless the `-copy` option is used. The `-copy` option causes only the specified copy to be affected.

- `recalculate`

  Allows the expiration date of backups to be changed based on the specified retention level or you can specify a new expiration date. When the expiration is changed according to retention level, the new date is calculated based on the creation date of the backup plus the value of the retention level. The expiration can be changed for a single backup, or for all backups for a particular client, policy, or schedule type.

  If the backup is on removable media, the expiration date of the media ID in the media catalog is changed, providing the expiration date on this command is greater than the current expiration of the media ID.

OPTIONS

`-client` *name*

Specifies the client name for the `-backupid` and `-recalculate` operations.

For the `backupid` operation, this option causes NetBackup to first search for the backup ID for the specified client, which is useful if the client name has changed.

For the `recalculate` operation, this option causes NetBackup to recalculate the expiration date based on the retention level for all the specified client backups.

`-copy` *number*

Expires or changes the expiration date of the specified copy number and is valid only with the `-backupid` and `-recalculate` options. Valid values are `1` through 10.

If the primary copy is expired, the other copy becomes the primary copy. If this option is not specified, the expiration affects both copies of the backup.

`-d` *date_time*

Specifies the expiration date and time. *date_time* can be any one of the following:

mm / *dd* / *yy hh*:*mm*:*ss*

or

`0`

or

`infinity`

If `0` is specified, the backup or media is expired immediately. If `infinity` is specified the backup is never expired.

`-deassignempty`

Expires removable media from the media catalog when that media no longer contains valid backups and also deassigns the media ID in the Media Manager catalog.

`-force` Prior to running the specified operation, `bpexpdate` queries before starting the operation. This option forces `bpexpdate` to carry out the operation without querying the user.

`-host` *name*

Note For NetBackup BusinesServer this option is not required because there is only one server (the master), so if you do use the option specify the host name of that server.

Specifies the host name of the server where the media catalog resides. This option is required only if the master has remote media servers and the volume was not written on the server where you run the `bpexpdate` command. In this case, the media ID is in the NetBackup media catalog on the server where the media was written and you must specify the name of that server on the `bpexpdate` command.

For example, assume you have a master server named whale and a media server named eel. You run the following `bpexpdate` command on whale in order to manually remove media ID BU0001 from the media catalog , and all corresponding backups from the image catalog:

```
bpexpdate -m BU0001 -d 0 -host eel
```

You can use the NetBackup Media List report to determine which server's media catalog has the volume.

`-m` *media_id*

Specifies the media ID that is affected by the expiration date change. The expiration dates of the backups on the media ID are also changed. The `-d` option must be included with this option.

This option can also be used when the `-deassignempty` option is specified to check if valid backups exist on this particular media ID. In this case, do not include the `-d` option.

The media ID must be six or less characters and must be in the NetBackup media catalog.

`-M` *master_server , . . . , master_server*

Specifies the master server that manages the media catalog that has the media ID. If this option is not specified, the default is one of the following:

For NetBackup BusinesServer:

NetBackup BusinesServer supports only one server (the master) with no remote media servers. Therefore, the default in this case is always the master server where you run the command.

For NetBackup DataCenter:

If the command is run on a master server, then that server is the default.

If the command is run on a media server that is not the master, then the master for that media server is the default.

`-policy` *name*

Specifies the policy name and is valid with the `-recalculate` option. When specified, the expiration is recalculated based on the retention level for all backups created in this policy.

`-recalculate`

Recalculates the expiration of backups based on the retention level or you can specify a new expiration date. Other options can be included in order to change the expiration for a single backup, or for all backups for a specific client name, policy name, or schedule type. Either the `-d` or `-ret` option must be specified with this option.

`-ret` *retention_level*

Specifies the retention level to use when recalculating expiration dates and is valid with the `-recalculate` option. Levels range from 0 to 24. The new expiration date is determined by adding the configured retention level value to the backup's creation date. Either the `-backupid` or `-policy` option must be specified with this option.

`-sched` *type*

Specifies the schedule type and is valid with the `-recalculate` option. When specified, the expiration is recalculated based on the retention level for all backups created with this schedule type. Enter a numeric value for type as follows:

`0` = Full

`1` = Differential Incremental

`2` = User Backup

`3` = User Archive

`4` = Cumulative Incremental

The `-policy` option must be specified with `-sched`.

NOTES

- The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

  If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the output for the `-d` option:

  ```
  -d <mm/dd/yyyy HH:MM:SS | 0 | infinity>
  ```

  Notice the month / day / year and hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales. See the `locale`(1) man page for detailed information.

- Some options in large environments can take a significant amount of time to complete. Changes that cause backups or media to expire are irrevocable; importing backups and (or) recovering previous versions of the catalogs can be required if mistakes are made using this command.

- The `bpexpdate` command itself does not necessarily make modifications to the catalogs. Therefore, aborting the command will not produce the desired or expected result.

EXAMPLES

- Example 1

The following command, run on the master server, removes media ID BU0002 from the media catalog, and deassigns the media ID in the Media Manager catalog. It also expires associated image records in the image catalog.

```
bpexpdate -m BU0002 -d 0
```

- Example 2

  The following command changes the expiration of copy 2 of backupid eel_0904219764. The expiration of copy 1 of the backup is not affected.

  ```
  bpexpdate -backupid eel_0904219764 -d 12/20/2001 08:00:00 -copy 2
  ```

- Example 3

  The following command removes the backup from the image catalog. Since the `-copy` option is not specified, all copies are removed.

  ```
  bpexpdate -backupid eel_0904219764 -d 0
  ```

- Example 4

  The following command checks for all media in host cat's media catalog that are still assigned but no longer contain valid backups. If any such media are found, the command removes them from the media catalog and deassigns them in the Media Manager catalog.

  ```
  bpexpdate -deassignempty -host cat
  ```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\media\*`

install_path`\NetBackup\db\images\*`

bpimagelist

NAME

`bpimagelist` - Queries the NetBackup catalog and produces a report on the status of the NetBackup images.

SYNOPSIS

install_path`\NetBackup\bin\bpimagelist -l | -L | -U | -idonly [-d` *mm/dd/yy hh:mm:ss* `| -hoursago` *hours* `] [-e` *mm/dd/yy hh:mm:ss*`] [-keyword "`*keyword phrase*`"] [-client` *client_name*`] [-backupid` *backup_id*`] [-option` *option_name*`] [-policy` *policy_name*`] [-pt` *policy_type*`] [-rl` *retention_level*`] [-sl` *sched_label*`] [-st` *sched_type*`] [-M` *master_server*`, . . .] [-v]`

install_path`\NetBackup\bin\bpimagelist -media [-l | -L | -U | -idonly] [-d` *mm/dd/yy hh:mm:ss* `| -hoursago` *hours*`] [-e` *mm/dd/yy hh:mm:ss*`] [-server` *server_name*`] [-keyword "`*keyword phrase*`"] [-client` *client_name*`] [-option` *option_name*`] [-policy` *policy_name*`] [-pt` *policy_type*`] [-rl` *retention_level*`] [-sl` *sched_label*`] [-st` *sched_type*`] [-M` *master_server*`, . . .] [-v]`

DESCRIPTION

`bpimagelist` queries the NetBackup catalog and produces a report on the status of the NetBackup images. It will produce one of two types of reports:

- Report images satisfying a set of criteria (if `-media` is absent)
- Report on removable media satisfying a set of criteria (if `-media` is present).

`bpimagelist` shows a list of previously archived or backed up files according to the options that you specify. You can choose the file or directory and the time period that you want the listing to cover. Directories can be recursively displayed to a specified depth.

The list shows only the files that you have read access to. You also must have read access to all directories in the file paths or you must own the directories. You can list files that were backed up or archived by another client if you are validated to do so by the NetBackup administrator.

`bpimagelist` writes its debug log information to the *install_path*`\NetBackup\logs\admin` directory. You can use the information in this directory for troubleshooting.

The output of `bpimagelist` goes to standard output.

This command requires administrator privileges.

OPTIONS

Report-type options

`-media`
Specifies that the listing reports on removable media satisfying a set of criteria. If `-media` is not present, the report is on images, not media, satisfying a set of criteria.

Report-format options:

`-U` Report in User mode. The report is formatted, it includes a banner listing the column titles, and the status is a descriptive term instead of a number.

`-L` Report in Long mode. For instance, for the Media List report, the report lists the information for each media ID as a series of *attribute* = *value* pairs, and the density value is provided as both a descriptive term and a number.

`-l` Report in Short mode. This produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format.

`-idonly` Produce an abbreviated listing. For an image listing, the listing contains the creation time, backup ID, and schedule type of each image. For instance, if the listing criterion is a window of time image listing contains, for each image created in this window, only the creation time, backup ID, and schedule type of the image.

For a media listing, the listing contains only the applicable media IDs. For instance, if the listing criterion is a window of time, the listing contains only the media IDs written in this window.

The following options represent the criteria that determine which images or media are selected for the report. Where images are discussed in these options, media can be substituted if this is a media report.

`-hoursago` *hours*
Include images written up to this many hours ago. This is equivalent to specifying a start time (`-d`) of the current time minus *hours*. *hours* must be 1 or greater.

`-option` *option_name*
Specifies a criterion for finding images to list. *option_name* is one of the following character strings, in either upper-or lower-case:

`INCLUDE_PRE_IMPORT` - Include images that have completed phase one of an import. Refer to the `bpimport` command description or the *NetBackup System Administrator's Guide* for more information.

`ONLY_PRE_IMPORT` - Include only images that have completed phase one of an import.

`INCLUDE_TIR` - Include images that were created by true-image-recovery backups. Refer to the `bpcpinfo` command description or the *NetBackup System Administrator's Guide* for more information on this topic.

`ONLY_TIR` - Include only images that were created by true-image-recovery backups.

The default is that there are no restrictions on the images selected.

`-backupid` *backup_id*

Specifies a backup ID to use for finding applicable images (applies only to image listing).

`-client` *client_name*

Specifies a client name to use for finding backups or archives to list. This name must be as it appears in the NetBackup catalog. By default, `bpimagelist` searches for all clients.

`-server` *server_name*

Specifies the name of a NetBackup server or `ALL`. This option applies to the media report (`-media`). If `-server` specifies a server name, the media in the report are only the media which reside on that server and which also satisfy the other criteria specified by `bpimagelist`. For instance, if `-hoursago 2` is specified, the media must contain an image created in the past two hours.

The query goes to the image catalog residing on the local master server. The master server must allow access by the system running `bpimagelist`.

The default is to report all media in the image catalog on the local master server. This is equivalent to specifying `-server ALL`.

`-M` *master_server*, . . .

A list of alternative master servers. This is a comma-delimited list of hostnames. If this option is present, each master server in the list runs the `bpimagelist` command. If an error occurs for any master server, processing stops at that point.

The report is the composite of the information returned by all the master servers in this list. `bpimagelist` queries each of these master servers. The master server returns image or media information from the image catalogs. Each master server must allow access by the system issuing the `bpimagelist` command.

The default is the master server for the system running `bpimagelist`.

`-pt` *policy_type*

Specifies a policy type. By default, `bpimagelist` searches for all policy types. *policy_type* is one of the following character strings:

```
Informix-On-BAR
MS-Exchange-Server
MS-SQL-Server
MS-Windows-NT
NetWare
Oracle
OS/2
Standard
Sybase
NDMP
```

Note The following policy types apply only to NetBackup DataCenter.

```
AFS
Apollo-wbak
DataTools-SQL-BackTrack
DB2
FlashBackup
SAP
Split-Mirror
```

`-rl` *retention_level*

Specifies the *retention_level*. The *retention_level* is an integer between 0 and 24. By default, `bpimagelist` searches for all retention levels.

`-d` *mm/dd/yy* [*hh*:*mm*:*ss*]

`-e` *mm/dd/yy* [*hh*:*mm*:*ss*]

Specifies the start and end date range for the listing.

`-d` specifies a start date and time for the listing. The resulting list shows only images in backups or archives that occurred at or after the specified date and time. Use the following format:

mm/dd/yy [*hh*[:*mm*[:*ss*]]]

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the previous midnight.

The local setting for the system affects the way you must specify dates and times. See NOTES.

`-e` specifies an end date and time for the listing.

The resulting list shows only files from backups or archives that occurred at or before the specified date and time. Use the same format as for the start date. The default is the current date and time.

`-keyword "`*keyword_phrase*`"`
Specifies a keyword phrase for NetBackup to use when searching. The phrase must match the one that has been previously associated with the image. For instance, the `-k` option of the `bpbackup` or `bparchive` command associates a keyword with the image when the image is created.

`-sl` *sched_label*
Specifies a schedule label for the image selection. The default is all schedules.

`-st` *sched_type*
Specifies a schedule type for the image selection. The default is any schedule type. Valid values are:

`FULL` (full backup)

`INCR` (differential-incremental backup)

`CINC` (cumulative-incremental backup)

`UBAK` (user backup)

`UARC` (user archive)

`NOT_ARCHIVE` (all backups except user archive)

`-policy` *name*

Searches for backups to import in the specified policy. The default is all policies.

Other options:

`-help` Prints a command line usage message when it is the only option on the command line.

`-v` Selects verbose mode. This option causes `bpimagelist` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined).

EXAMPLES

◆ Example 1

The first example shows the last time each media ID available to a server had a backup image written today:

```
bpimagelist -media -U
```

```
Media ID   Last Written     Server
--------   --------------   ----------
IBM000     01/06/2001 01:06   hat
```

```
AEK800      01/06/2001 03:01   hat
C0015       01/06/2001 02:01   hat
```

- Example 2

  The following example shows the last time the media IDs available to the server had a backup image written during the specified time:

```
bpimagelist -media -d 01/05/2001 18:00:46 -e 01/06/2001 23:59:59
-U

Media ID   Last Written     Server
--------   --------------   ----------
IBM000     01/06/2001 01:06   hat
AEK800     01/06/2001 03:01   hat
C0015      01/06/2001 02:01   hat
143191     01/05/2001 23:00   hat
```

  The following example lists all images written today:

```
C:\VERITAS\NetBackup\bin\admincmd\bpimagelist -U
Backed Up       Expires     Files       KB  C  Sched Type Policy
--------------  -------- -------- --------  -  ------------
------------
01/27/2001 01:08  02/03/2001     1122   202624  N  Full Backup
3590Grau
01/27/2001 01:01  02/03/2001     1122   202624  N  Full Backup
IBM3590policy
01/27/2001 03:01  02/03/2001      531  1055104  N  Full Backup
DELLpolicy
01/27/2001 02:01  02/03/2001      961    31776  N  Full Backup
QUALpolicy
01/27/2001 01:08  02/03/2001     2063   603328  N  Full Backup
IBM3590policy
01/27/2001 01:01  02/03/2001     2063   603328  N  Full Backup
3590Grau
```

- Example 3

  The following example lists media written information for 01/05/2001:

```
bpimagelist -media -d 01/05/2001 -e 01/05/2001 -U
Media ID   Last Written     Server
--------   --------------   ----------
IBM000     01/05/2001 01:13   hat
143191     01/05/2001 23:00   hat
AEK800     01/05/2001 03:07   hat
C0015      01/05/2001 02:06   hat
```

FILES

install_path`\NetBackup\logs\admin\log.`*mmddyy*

install_path`\NetBackup\db\images`

SEE ALSO

`bparchive`, `bpbackup`, `bprestore`

bpimmedia

NAME

`bpimmedia` - Display information about the NetBackup images on media

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpimmedia [-l | -L] [-policy` *policy_name*`] [-client` *client_name*`] [-d` *mm/dd/yyyy hh:mm:ss*`] [-e` *mm/dd/yyyy hh:mm:ss*`] [-mediaid` *vsn* | *path_name*`] [-mtype` *image_type*`] [-option` *option_name*`] [-rl` *retlevel*`] [-sl` *sched_label*`] [-t` *sched_type*`] [-verbose] [-M` *master_server,...*`]`

install_path`\NetBackup\bin\admincmd\bpimmedia -spangroups [-mediaid` *vsn*`] [-U] [-cn` *copy_number*`]`

DESCRIPTION

`bpimmedia` queries the NetBackup image catalog and reports on the NetBackup images. `bpimmedia` produces two reports:

- An Images-on-Media report
- A Spangroups report

The first form of `bpimmedia` in the SYNOPSIS displays a set of NetBackup images in the Images-on-Media report. The Images-on-Media report lists the contents of media as recorded in the NetBackup image catalog. You can generate this report for any medium (including disk), filtering the report contents according to client, media ID or path, and so on. Refer to the section on NetBackup Reports in the *NetBackup System Administrator's Guide* for more information, including details about the fields in the Images on Media report. The Images on Media report does not show information for media used in backups of the NetBackup catalogs.

The second form of `bpimmedia` in the SYNOPSIS uses the `-spangroups` option to list media id groups that are *related* because images span from one volume to another. The output lists, for each media server in the cluster, the media ids that have spanning images. The `-spangroups` form of `bpimmedia` must be run on the NetBackup master server that administers the volumes. (See the Spanning Media topic in the *NetBackup System Administrator's Guide*.) Only removable media types are processed.

`bpimmedia` sends its error messages to stderr. `bpimmedia` sends a log of its activity to the NetBackup admin log file for the current day.

This command requires administrator privileges.

OPTIONS

`-policy` *policy_name*
Policy name. By default, `bpimmedia` searches for images for all policies.

`-client` *client_name*
Client name. This name must be as it appears in the NetBackup catalog. By default, `bpimmedia` searches for all clients.

`-cn` Copy number (1 or 2) of a backup ID. The default is copy 1. This option is used only in combination with `-spangroups`.

`-d` *mm/dd/yyyy* [*hh*:*mm*:*ss*]

`-e` *mm/dd/yyyy* [*hh*:*mm*:*ss*]
The start and end date. These specify the time range during which an image must have been created to be included in the report.

The locale setting for your system affects the way you specify dates and times. See NOTES.

`-d` specifies a start date and time. The resulting list shows only images from backups or archives that occurred at or after the specified date and time. Use the following format:

mm/dd/yyyy [*hh*[:*mm*[:*ss*]]]

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the previous midnight.

`-e` specifies an end date and time. The resulting list shows only images from backups or archives that occurred at or before the specified date and time. Use the same format as for the start date. The default is the current date and time.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-L` The list type is long. See the section DISPLAY FORMATS for more detail.

`-l` The list type is short. This is the default if the command line has no list-type option (for instance, if you enter `bpimmedia` and a carriage return). See the section DISPLAY FORMATS for more detail.

`-M` *master_server,...*
A list of alternative master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-mediaid` *vsn* | *pathname*

This is either a VSN or an absolute pathname. If the media ID is a VSN, it is a one- to six-character string. If the media ID is a pathname, it is the absolute pathname of the filesystem for a disk storage unit.

When `-mediaid` is specified, the Images-on-Media report displays only images stored on this VSN or pathname. By default, the report displays images stored on all media IDs and pathnames.

For the Spangroups report (`-spangroups`), `-mediaid` can only be followed by a VSN. If `-mediaid` is omitted when `-spangroups` is present, `bpimmedia` displays all media in all spanning groups.

`-mtype`

Image type. The defined values, and their interpretations, are

`0` = Regular backup (scheduled or user-directed backup)

`1` = Pre-imported backup (phase 1 completed)

`2` = Imported backup

`-option` *option_name*

Specifies a criterion for finding images to list. option_name is one of the following character strings, in either upper-or lower-case:

`INCLUDE_PRE_IMPORT` - Include images that have completed phase one of an import. Refer to the `bpimpor` command description or the *NetBackup System Administrator's Guide* for more information.

`ONLY_PRE_IMPORT` - Include only images that have completed phase one of an import.

The default is `INCLUDE_PRE_IMPORT`.

`-rl` *retention_level*

The retention_level. The retention_level is an integer between 0 and 24. By default, `bpimmedia` searches for all retention levels.

`-sl` *sched_label*

The schedule label. By default, `bpimmedia` searches for images for all schedule labels.

`-spangroups`

Specifies that `bpimmedia` should create a Spangroups report. The default is to create an Images-on-Media report.

`-t` *sched_type*

Specifies a schedule type for the image selection. The default is any schedule type. Valid values, in either upper- or lower-case, are:

`FULL` (full backup)

`INCR` (differential-incremental backup)

`CINC` (cumulative-incremental backup)

UBAK (user backup)

UARC (user archive)

-U The list type is user. This option is used only in combination with -spangroups. See the section DISPLAY FORMATS for more detail.

-verbose

Select verbose mode for logging. This is only meaningful when running with debug logging turned on (the *install_path*\NetBackup\logs\admin directory is defined).

DISPLAY FORMATS

IMAGES-ON-MEDIA REPORT

For the Images-on-Media report, there are two formats, short (-l or default) and long (-L).

- Long Display Format (-L)

  If the command line contains -L, the display format is long. The -L display format contains a multi-line entry for each backup image. The number of lines for an entry is n+1, where n is the number of fragments for the image. The fields for an entry are listed in the table below. The first line of the entry contains the fields Backup_ID...Expires. Then, for each fragment in the image, there is a line containing the fields Copy_Media ID. The report has a two-line header. The first header line lists the field names for line 1 of each entry. The second header line lists the field names for the lines that contain fragment information.

  See bpduplicate for more information on the terms *copy number* and *primary copy*.

  Fields and meanings for the -L format are as follows:

  Line 1

  Backup-ID - Unique identifier for the backup that produced this image

  Policy - Policy name (may be truncated if long)

  Type - Schedule type (FULL, etc.)

  RL - Retention level (0..24)

  Files - Number of files in the backup

  C - Compression (Y or N)

  E - Encryption (Y or N)

  T - Image type

  R is Regular (scheduled or user-directed backup)

  P is Pre-imported backup (phase 1 completed)

I is Imported backup

PC - Primary copy, 1 or 2. Designates which copy of the backup NetBackup chooses when restoring.

Expires - Expiration date of the first copy to expire, which is indicated by the Expires field of the fragment which is described below

Line 2_n+1

Copy - Copy number of this fragment

Frag - Fragment number, or IDX for a true-image-restore (TIR) fragment

KB - Size of the fragment, in kilobytes. This value does not include the size of tape headers between backups. A fragment size of 0 is possible for a multiplexed backup.

Type - Media type (Rmed for removable media; Disk otherwise)

Density - Density of the device that produced the backup (applies only to removable media)

Fnum - File number; this is the n-th backup on this medium (applies only to removable media)

Off - The byte offset on the medium where the backup begins (applies only to optical disk; ignore this value for tapes and magnetic disk)

Host - Server whose catalog contains this image

DWO - Device Written On; device where the backup was written. The DWO matches the drive index as configured in Media Manager (applies only to removable media).

MPX - Flag indicating whether this copy is multiplexed, Y or N (applies only when fragment number is 1)

Expires - Expiration date of this copy (applies only when fragment number is 1)

MediaID - Media ID or absolute path where the image is stored

Example of Long display format:

```
bpimmedia -L -policy regr1_guava -t FULL
Backup-ID        Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag  KB Type Density FNum Off Host DWO MPX Expires          MediaID
-----------------------------------------------------------------------
guava_0949949902 regr1_guav FULL  3   25      N  N  R  1   12:58 03/09/2000
 1   1    256 RMed dlt     13   0   plum 0   Y   12:58 03/09/2000 A00002
```

- Short Display Format (`-l`)

If the `bpconfig` command line contains `-l` or contains no list-format option, the display format is short. This produces a terse listing. This option can be useful for scripts or programs that rework the listing into a customized report format. The `-l` display format contains a multi-line entry for each backup image. The number of lines for an entry is n+1, where n is the number of fragments for the image. The layout of an entry is a first line, containing information about the image, followed by a line containing information about each fragment of the image. The attributes appear in the following order, separated by blanks.

Fields and Meanings for the `-l` format are as follows:

Line 1

IMAGE - Identifies the start of an image entry

Client - Client for the backup that produced this image

Version - Image-version level

Backup-ID - Unique identifier for the backup that produced this image

Policy - Policy name

Policy type - 0 denotes Standard, etc. Run bpimmedia -L or refer to bpbackup(1m) to interpret the policy-type value as a policy-type name.

Schedule - Schedule name

Type - Schedule type (full, etc.)

RL - Retention level (0..24)

Files - Number of files

Expires - Expiration date of the first copy to expire, which is indicated by the Expires field of the fragment which is described below (system time); 0 denotes an image “in progress” or failed.

C - Compression; 1 (yes) or 0(no)

E - Encryption; 1 (yes) or 0(no)

Line 2_n+1

FRAG - Identifies a fragment line in an image entry

Copy - Copy number of this fragment

Frag - Fragment number, or -1 for a TIR fragment

KB - Size of the fragment, in kilobytes

(Internal) Internal value, not documented

Type - Media type (2 for removable media; 0 for disk)

Density - Density value (applies only to removable media) Run `bpimmedia -L` or `bpmedialist -mlist -L -ev` *mediaid* to interpret the density value as a density label.

Fnum - File number; this is the n-th backup on this medium (applies only to removable media)

MediaID - Media ID or absolute path where the image is stored

Host - Server whose catalog contains this image

Block size - Number of kilobytes per block for this medium

Off - Offset

Media dateTime this medium was allocated (system time)

DWO - Device Written On (applies only to removable media)

(Internal) - Internal value, not documented

(Internal) - Internal value, not documented

Expires - Expiration date of this copy in system time (applies only when fragment number is 1)

MPX - Flag indicating whether this copy is multiplexed, 1(yes) or 0(no) (applies only when fragment number is 1)

Example of the short display format:

```
bpimmedia -l -policy regr1_guava -t FULL
IMAGE guava 3 guava_0949949902 regr1_guava 0 full 0 3 25 952628302 0 0
FRAG 1 1 10256 512 2 13 13 A00002 plum 65536 0 949616279 0 0 *NULL* 952628302 1
```

SPANGROUPS REPORT

For the Spangroups report, there are two formats: user (`-U` option) and short (the default). Both formats list, for each server, the server name, and the group data for that server. For each group of media that share spanned backup images, the media Ids are listed. When -mediaid appears on the command line, only the server and media group related to that media ID are displayed.

The user (`-U`) display format looks like this:

```
bpimmedia -spangroups -U
```

```
Related media groups containing spanned backup images, server plum:
Group:
  A00002  A00003
Group:
  400032
```

The short display format looks like this

```
bpimmedia -spangroups
```

```
SERVER plum
GROUP A00002 A00003
GROUP 400032
```

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. The following is part of the usage statement for `bpimmedia` that shows the `-d` and `-e` options:

```
[-d mm/dd/yy hh:mm:ss] [-e mm/dd/yy hh:mm:ss]
```

Notice the month / day / year and hours:minutes:seconds requirements for the `-d` and `-e` options. These are for a locale setting of C and can be different for other locales.**EXAMPLES**

- Example 1

  List the images for policy c_NDMP. This request runs on a NetBackup media server. The report is based on the image catalog on the media server's master server, almond.

```
bpimmedia -L -policy c_NDMP

Backup-ID        Policy  Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires MediaID
-----------------------------------------------------------------------------------------

t_0929653085    c_NDMP  FULL  3   5909    N  N  R  1   15:58 07/18/2001
 1 IDX      844 RMed dlt     2         0         almond     3                      CB7514
 1   1     9136 RMed dlt     1         0         almond     3   N   15:58 07/18/2001 CB7514
```

- Example 2

  The following example displays the tapes required to restore a particular file. If the `bpimmedia` command line provides the criteria to identify an individual backup, the output shows which media were used for the backup.

  In this case, the command line provides the client, the date of the backup and the schedule type. The output shows that tape A00002 on the server plum contains the backup.

```
bpimmedia -L -client guava -d 2/7/2000 -t UBAK

Backup-ID            Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires     MediaID
-----------------------------------------------------------------------------------------
```

```
guava_0949949686     regr1_guav UBAK  3   25      N  N  R  1   12:54 03/09/2000
 1   1    10256 RMed dlt     11        0         plum       0   Y   12:54 03/09/2000 A00002
```

- Example 3

  List, in long format, all the backups in the image catalog on the master server guava.

```
bpimmedia -L -M guava
```

```
Backup-ID            Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires   MediaID
-----------------------------------------------------------------------------------------
guava_0949599942     test-policy FULL  1   15      N  N  R  1   11:45 02/17/2000
 1   1      224 Disk -       -         -         guava      -   N   11:45 02/17/20
/var/qatest/storage_unit//guava_0949599942_C1_F1
```

- Example 4

  List, in long format, the backups on media ID CB7514.

```
bpimmedia -L -mediaid CB7514

Backup-ID            Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires   MediaID
-----------------------------------------------------------------------------------------
toaster1_0929679294  tort_policy FULL  3   5898    N  N  R  1   23:14 07/18/2001
 1 IDX      839 RMed dlt     4         0         almond     6                  CB7514
 1   1    27154 RMed dlt     3         0         almond     6   N   23:14 07/18/2001 CB7514

toaster1_0929653085  NDMP_policy FULL  3   5909    N  N  R  1   15:58 07/18/2001
 1 IDX      844 RMed dlt     2         0         almond     3                  CB7514
 1   1     9136 RMed dlt     1         0         almond     3   N   15:58 07/18/2001 CB7514
```

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bpimmedia: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\images`

SEE ALSO

`bpbackup`, `bpduplicate`, `bpimport`

bpimport

NAME

`bpimport` - Import NetBackup and Backup Exec backups that are expired or are from another NetBackup or Backup Exec server

SYNOPSIS

install_path`\NetBackup\admincmd\bpimport -create_db_info -id` *media_id* `[-server` *name*`] [-L` *output_file* `[-en]] [-passwd] [-local]`

install_path`\NetBackup\admincmd\bpimport [-l] [-p] [-pb] [-PD] [-PM] [-v] [-local] [-client` *name*`] [-Bidfile` *file_name*`] [-backup_copy` *backup_copy_value*`] [-M` *master_server*`] [-st` *sched_type*`] [-sl` *sched_label*`] [-L` *output_file* `[-en]] [-policy` *name*`] [-s` *startdate*`] [-e` *enddate*`] [-pt` *policy_type*`] [-hoursago` *hours*`] [-cn` *copy_number*`] [-backupid` *backup_id*`] [-id` *media_id*`]`

DESCRIPTION

The `bpimport` command allows backups to be imported. This command is useful for importing backups that have expired or are from another NetBackup server.

The import operation consists of two steps:

- Step 1 is performed with the first form of the command shown above (`-create_db_info` option) and recreates catalog entries for the backups that are on the specified media.
- Step 2 is performed with the second form of the command shown above and imports the backups from the media.

The expiration date for imported backups is the current date plus the retention period. For example, if a backup is imported on 14 November 2001 and its retention level is one week, its new expiration date is 21 November 2001.

You can import a backup only if all copies of it are expired. For more information on importing backups, see the *NetBackup System Administrator's Guide*.

OPTIONS

`-backup_copy` *n*
Where *n* is 3, indicates that the import is for Fastrax.

`-backupid` *backup_id*
Specifies the backup ID of a single backup to import.

`-Bidfile` *file_name*

file_name specifies a file that contains a list of backup IDs to be imported. List one backup ID per line in the file. If this option is included, other selection criteria is ignored.

`-client` *name*

The host name of the client for which the backups were performed. The default is all clients.

`-cn` *copy_number*

Specifies the source copy number of the backups to import. Valid values are 1 through 10. The default is all copies.

`-create_db_info`

This option recreates catalog entries for the backups that are on the specified media. It skips backups that are already in the catalog. This option only creates information about backups that are candidates for import, and does not perform the import operation. The `bpimport` command must be run with this option prior to importing any backups.

The `-id` parameter is required with this option.

`-e` *enddate*

`-s` *startdate*

Specifies the end (`-e`) or start (`-s`) of the range of dates and times that include all backups to import. The date and time syntax is as follows:

mm / *dd* / *yy* [*hh*[: *mm*[: *ss*]]]

The default for the end date is the current date and time; the default for the start date is 24 hours prior to the current date and time.

`-hoursago` *hours*

Specifies number of hours to search prior to the current time for backups. Do not use with the `-s` option. The default is the previous midnight.

`-id` *media_id*

For step 1 (`-create_db_info`), this option specifies the media ID that has the backups you are going to import. This option is required with `-create_db_info`.

For step 2, this option designates a specific media ID from which to import backups. The default is all media IDs that were processed by step 1 of the import operation.

A backup ID that begins on a media ID that was not processed by step 1 is not imported. A backup that ends on a media ID that was not processed by step 1 will be incomplete.

`-L` *output_file* `[-en]`

Specifies the name of a file in which to write progress information. The default is to not use a progress file.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-l` Produces output in the progress log that lists each file imported.

`-local` When `bpimport` is initiated from a host other than master server and the `-local` option is *not* used (default), `bpimport` starts a remote copy of the command on the master server.

The remote copy allows the command to be terminated from the Activity Monitor.

Use the `-local` option to prevent the creation of a remote copy on the master server and to run the `bpimport` only from the host where it was initiated.

If the `-local` option is used, `bpimport` cannot be canceled from the Activity Monitor.

`-M` *master_server*

Note For NetBackup BusinesServer, this option is not required because there is only one server, the master. If you do use this option in this case, specify the NetBackup BusinesServer master where you run the command.

Specifies the master server that manages the media catalog that has the media ID. If this option is not specified, the default is one of the following:

If the command is run on a master server, then that server is the default.

If the command is run on a media server that is not the master, then the master for that media server is the default.

`-p` Previews backups to be imported according to the option settings, but does not perform the import. Displays the media IDs, server name, and information about the backups to be imported.

`-passwd` Use with the Backup Exec tape reader option to catalog password protected Backup Exec media. When `-passwd` is specified, `bpimport` prompts the user for a password. The password given is then compared with the password on the media. If the password matches, the job proceeds. If the password does not match, the job fails.

Use `-passwd` only when Backup Exec media are being imported and the Backup Exec media are password-protected. Backup Exec media can only be imported on a Windows media server.

`-pb` Previews the backups to import but does not perform the import. Similar to the `-p` option, but does not display the backups.

`-PD` Same as the `-PM` option, except the backups are sorted by date and time (newest to oldest).

`-PM` Displays information on the backups to be imported according to the option settings, but does not perform the import. It displays the following information about the backup: date and time of the backup, policy, schedule, backup ID, host, and media ID.

`-policy` *name*
Search for backups to import in the specified policy. The default is all policies.

`-pt` *policy_type*
Search for backups created by the specified policy type. The default is any policy type.

Valid values are:

```
Informix-On-BAR
MS-Exchange-Server
MS-SQL-Server
MS-Windows-NT
NDMP
NetWare
Oracle
OS/2
Standard
Sybase
```

Note The following policy types apply only to NetBackup DataCenter.

```
AFS
DataTools-SQL-BackTrack
DB2
FlashBackup
SAP
Split-Mirror
```

`-server` *name*

Note For NetBackup BusinesServer there is only one server (the master). When using BusinesServer, specify the name of that server.

Specifies the name of the media server. The volume database for this server must have a record of the media ID that contains the backups to be imported. The default is the media server where the command is run.

`-sl` *sched_label*
Search for backups to import which were created by the specified schedule. The default is all schedules.

`-st` *sched_type*
Search for backups to import which were created by the specified schedule type. The default is any schedule type.

Valid values are:

`FULL` (full backup)

`INCR` (differential-incremental backup)

`CINC` (cumulative-incremental backup)

`UBAK` (user backup)

`UARC` (user archive)

`NOT_ARCHIVE` (all backups except user archive)

`-v` Selects verbose mode. When specified, the debug and progress logs display more information.

EXAMPLES

- Example 1

  The following command (all on one line) creates catalog information for backups on media ID A00000. The media host hostname is cat. The progress file is `/tmp/bpimport.ls`.

```
bpimport -create_db_info -id A00000 -server cat -L \tmp\bpimport.ls
```

- Example 2

  The following command (all on one line) displays information about the backups that are candidates for import. The backups displayed would have been created between 11/01/2000 and 11/10/2000. The `bpimport` command with the `-create_db_info` option must be run prior to this command.

```
bpimport -PM -s 11/01/2000 -e 11/10/2000
```

- Example 3

The following command imports the backups specified in the `/tmp/import/images` file. The progress is entered in the `/tmp/bpimport.ls` file.

```
bpimport -Bidfile \tmp\import\image -L \tmp\bpimport.ls
```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\images\*`

bplabel

NAME

`bplabel` - Write a NetBackup label on tape media

SYNOPSIS

install_path`\netbackup\bin\admincmd\bplabel -m` *media_ID* `-d` *density* `[-o] [-p` *volume_pool_name*`] [-n` *drive_name* `| -u` *device_number*`]`

DESCRIPTION

`bplabel` writes a NetBackup label on the specified media. Labeling is required only for media that were last used for NetBackup catalog backups or by a non-NetBackup application. You can also use it to assign specific media IDs. The NetBackup Device Manager service (`ltid`) must be active for `bplabel` to succeed. You must also manually assign the drive by using the NetBackup Device Monitor unless you include the `-u` option on the `bplabel` command.

Caution Ensure that the media does not contain required backups. After the media is relabeled, any backups that were on it cannot be restored.

The following are some facts about using this command:

- The `-ev` and `-d` options are required.
- The `-p` option is required if the *evsn* (media ID) is not in the NetBackup volume pool.
- If the data already on the media is in a recognized format and the `-o` option is not specified, `bplabel` prompts you to confirm the overwrite. Data format recognition works only if the first block on a variable length media is less than or equal to 32 kilobytes.
- Use the `bplabel` command only for tapes.

OPTIONS

`-m` *media_ID*

A required option that specifies the external volume serial number that is written to the tape label as a media ID . You can enter the evsn in either uppercase or lowercase. Internally, it is always converted to uppercase. The evsn must be six or fewer alphanumeric characters.

`-d` *density*

A required option that specifies the density of the tape drive on which the media is mounted. The tape mount request must be performed on a drive type that satisfies the `-d` option.

Note Do not use capital letters when entering the density. Incorrect density syntax causes the command to fail and an “Invalid Density Drive Type” message to appear.

The valid densities are as follows:

`4mm` (4-mm cartridge)

`8mm` (8-mm cartridge)

`dlt` (dlt cartridge)

`dlt2` (dlt cartridge alternate)

`qscsi` (1/4 in cartridge)

Note The following densities are supported only by NetBackup DataCenter servers.

`dtf` (dtf cartridge)

`hcart` (1/2 Inch cartridge)

`hcart2` (1/2 Inch cartridge alternate)

`-o` Unconditionally overwrites the selected media ID. If this option is not specified, `bplabel` prompts for permission to overwrite media that meets any of the following conditions:

Contains a NetBackup media header.

Is NetBackup catalog backup media.

Is in TAR, CPIO, DBR, AOS/VS, or ANSI format.

`-p` *volume_pool_name*
This option is required if the media ID is defined in the Media Manager volume database but is not in the NetBackup volume pool. *volume_pool_name* must specify the correct pool.

`-u` *device_number*
Unconditionally assigns the standalone drive specified by *device_number*. The drive must contain media and be ready. By using this option, manual operator assignment is not required. The number for the drive can be obtained from the Media Manager configuration.

`-n` *drive_name*
Unconditionally assigns the standalone drive specified by *drive_name*. The drive must contain media and be ready. By using this option, manual operator assignment is not required. The name for the drive can be obtained from the Media Manager configuration.

bplist

NAME

`bplist` - Lists backed up and archived files on the NetBackup server

SYNOPSIS

install_path`\NetBackup\bin\bplist [-A | -B] [-C` *client*`] [-S` *master_server*`] [-t` *policy_type*`] [-k` *policy*`] [-F] [-R [n]] [-b | -c | -u] [-l] [-r] [-flops` *file_options*`] [-Listseconds] [-T] [-unix_files] [-nt_files] [-s` *mm/dd/yy* `[`*hh:mm:ss*`]] [-e` *mm/dd/yy* `[`*hh:mm:ss*`]] [I] [PI] [-help] [-keyword "`*keyword_phrase*`"] [`*filename*`]`

DESCRIPTION

`bplist` shows a list of previously archived or backed up files according to the options that you specify. You can choose the file or directory and the time period that you want the listing to cover. Directories can be recursively displayed to a specified depth.

The list shows only the files that you have read access to. You also must own or have read access to all directories in the file paths. You can list files that were backed up or archived by another client only if you are validated to do so by the NetBackup administrator.

If you create directory *install_path*`\NetBackup\logs\bplist\` with write access, `bplist` creates an debug log file in this directory that you can use for troubleshooting.

The output of `bplist` goes to standard output.

OPTIONS

`-A | -B` Specifies whether to produce the listing from archives (`-A`) or backups (`-B`). The default is `-B`.

`-C` *client* Specifies a client name to use for finding backups or archives to list. This name must be as it appears in the NetBackup configuration. The default is the current client name.

`-S` *master_server*
Specifies the name of the NetBackup server. The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the user interface on the client and click Specify NetBackup Machines on the Actions menu.

`-t` *policy_type*
Specifies one of the following numbers corresponding to the policy type (the default is `0` on all clients except Apollos, where it is `3`):

`0` = Standard

4 = Oracle

6 = Informix-On-BAR

7 = Sybase

10 = NetWare

13 = MS-Windows-2000/NT

14 = OS/2

15 = MS-SQL-Server

16 = MS-Exchange-Server

19 = NDMP

Note The following policy types apply only to NetBackup DataCenter.

3 = Apollo-wbak

11 = DataTools-SQL-BackTrack

17 = SAP

18 = DB2

20 = FlashBackup

21 = Split-Mirror

22 = AFS

`-k` *policy* Names the policy to search to produce the list. If not specified, all policies are searched.

`-F` Specifies that in the list output, symbolic links (applies only to UNIX clients) will end with a trailing @ and executable files with a trailing *.

`-R [`*n*`]` Recursively lists subdirectories encountered to a depth of *n*. The default for *n* is 999.

`-b | -c | -u`

Specifies an alternate date and time to be used for printing with the `-l` option:

`-b` displays the backup date and time of each file.

`-c` displays the last modification date and time for each file.

`-u` displays the last access date and time of each file.

The default is to display the time of last modification of each file.

`-l` Shows file details.

`-Listseconds`

Specifies that seconds granularity be used for the time stamp when the the `-l` option is used.

`-r` Lists disk images that were backed up. The default is to list file systems.

`-flops` *file_options*]

Allows either Backup Exec files to be listed, or both Backup Exec and NetBackup files to be listed. The default (`-flops` not specified) is to list only NetBackup files.

To list only Backup Exe files specify:

```
-flops 524288
```

To list Backup Exe and NetBackup files specify:

```
-flops 1048576
```

`-T` Lists directories in true-image backups. The default is to list non-true-image backups.

`-unix_files`

Lists the files and directories in UNIX format. For example: `/C/users/test`.

`-nt_files`

Lists the files and directories in Windows format. For example: `C:\users\test`.

`-s` *mm/dd/yy* [*hh:mm:ss*]

`-e` *mm/dd/yy* [*hh:mm:ss*]

Specifies the start and end date range for the listing.

`-s` specifies a start date and time for the listing. The resulting list shows only files in backups or archives that occurred at or after the specified date and time. Use the following format for the start date and time:

mm/*dd*/*yy* [*hh*[:*mm*[:*ss*]]]

The valid range of dates are from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the current date minus six months.

`-e` specifies an end date and time for the listing. The resulting list shows only files from backups or archives that occurred at or before the specified date and time. Use the same format as explained above for start date and time. The default is the current date and time.

`-I` Specifies a case-insensitive search. This means that capitalization is not considered when comparing names (for example, Cat matches cat).

`-PI` Specifies a path-independent search, which means that NetBackup searches for a specified file or directory without regard to the path. For example, if a file named `test` exists in the three directories shown below, a search for `test` finds all three instances of the file:

```
/tmp/junk/test
/abc/123/xxx/test
```

/abc/123/xxx/yyy/zzz/test

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-keyword` "*keyword_phrase*"
Specifies a keyword phrase for NetBackup to use when searching for backups or archives from which to restore files. The phrase must match the one that was previously associated with the backup or archive by the `-k` option of the `bpbackup` or `bparchive` command.

You can use this option in place of or in combination with the other restore options in order to make it easier to restore your backups and archives. The following meta characters can be used to simplify the task of matching keywords or parts of keywords in the phrase:

* matches any string of characters.

? matches any single character.

[ ] matches one of the sequence of characters specified within the brackets.

[-] matches one of the range of characters separated by the "-".

The keyword phrase can be up to 128 characters in length. All printable characters are permitted including space (" ") and period (."). The phrase must be enclosed in double quotes ("...") or single quotes (‘...’).

The default keyword phrase is the null (empty) string.

filename Names the file or directory to list. If you do not specify a path, the default is the current working directory.

Any files or directories that you specify must be listed at the end, following all other options.

Use upper case for the drive letter. For example, `C:\NetBackup\log1`.

For directories, if you do not use the `-R` option, include the trailing path separator (\ for Windows and / for UNIX) as in the following:

`bplist -l D:\WS_FTP.LOG\*` (Windows)

`bplist -l /home/user1/*` (UNIX)

EXAMPLES

◆ Example 1

To list recursively, in long format, the files that were backed up in `D:\WS_FTP.LOG`.

```
bplist -l -R D:\WS_FTP.LOG
-rwx------ bjm       bjm                64 Oct 10  1997 D:\WS_FTP.LOG
-rwx------ bjm       bjm                64 Oct 10  1997 D:\WS_FTP.LOG
-rwx------ bjm       bjm                64 Oct 10  1997 D:\WS_FTP.LOG
```

- Example 2

  To list, with details, the files that were backed up and associated with all or part of the keyword phrase

  `"My Home Directory"`

  in directory `C:\home\kwc`, enter the following:

```
bplist -keyword "*My Home Directory*" -l C:\home\kwc\
```

- Example 3

  To list, with details, the files that were archived and associated with all or part of the keyword phrase

  `"My Home Directory"`

  in directory `C:\home\kwc`, enter the following:

```
bplist -A -keyword "*My Home Directory*" -l C:\home\kwc\
```

- Example 4

  To list, recursively and with details, the files that were backed up on drive D of Windows NT client slater and associated with all or part of the keyword phrase

  `"Win NT"`

  enter the following:

```
bplist -keyword "*Win NT*" -C slater -t 13 -R -l D:\
```

FILES

install_path`\NetBackup\logs\bplist\*.log`

bppldelete

NAME

`bppldelete` - Delete policies from the NetBackup database.

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bppldelete [`*policyname*`]`
`[-verbose] [-M` *master_server,...master_server*`]`

DESCRIPTION

`bppldelete` deletes policies from the NetBackup database.

OPTIONS

`-M` *master_server,...master_server*

Delete policy information for a specific master server(s). For example, to delete policy MWF_PM from master server Saturn, enter:

```
bppldelete MWF_PM -M Saturn
```

`-verbose`

Select verbose mode for logging.

bppllist

NAME

`bpplist` - List policy information.

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bppllist [`*policyname*`] [-L | -l | -U] [-allpolicies] [-M` *master_server,...master_server*`] [-hwos] [-byclient` *client*`] [-keyword` *"keyword phrase"*`] [-verbose]`

DESCRIPTION

`bppllist` lists policies within the NetBackup database.

OPTIONS

`-allpolicies`
Lists all policies.

`-hwos` Lists possible hardware and the operating system.

`-L` Displays a full listing.

`-l` Displays information in raw output mode.

`-M` *master_server,...master_server*
Lists policy information for a specific master server(s).

`-U` Displays information in the style used by `xbpadm`.

`-byclient` *client*
Lists policy information for all policies containing the client indicated.

`-verbose`
Select verbose mode for logging.

bpmedia

NAME

`bpmedia` - Freeze, unfreeze, suspend, or unsuspend NetBackup media

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpmedia -freeze| -unfreeze| -suspend|-unsuspend -ev` *media_id* `[-h` *host*`] [-v]`

install_path`\NetBackup\bin\admincmd\bpmedia -movedb -ev` *media_id* `-newserver` *hostname* `[-oldserver` *hostname*`] [-v]`

DESCRIPTION

`bpmedia` allows an individual NetBackup media ID to be controlled in terms of allowing or disallowing future backups or archives to be directed to the media. Note that this command applies only to media managed by Media Manager.

Note Under certain media or hardware error conditions, NetBackup automatically suspends or freezes media. If this happens, the reason is logged in the NetBackup Problems report. If necessary, you can use the `bpmedia -unfreeze` or `-unsuspend` options to reverse this action.

OPTIONS

`-freeze` Freezes the specified media ID. When an active NetBackup media ID is frozen, NetBackup stops directing backups and archives to the media. All unexpired images on the media continue to be available for restores. NetBackup never deletes a frozen media ID from the NetBackup media catalog, nor is it unassigned in the NetBackup volume pool when it expires.

`-unfreeze`
Unfreeze the specified media ID. This reverses the action of `freeze` and allows the media to be used for backups or archives again if it has not expired. If a media is expired when it is unfrozen, it is immediately unassigned in the NetBackup volume pool.

`-suspend`
Suspend the specified media ID. The action is the same as `freeze` except that when the media ID expires, it is immediately unassigned in the NetBackup volume pool.

`-unsuspend`
Unsuspend the specified media ID. This reverses the action of `suspend` and allows the media to be used for backups or archives again.

`-movedb -newserver` *hostname* `[-oldserver` *hostname*`]`

Note You cannot use the `-movedb` option with NetBackup BusinesServer.

Moves a media catalog entry from one server to another in a master and media server cluster. This command moves the media catalog entry for the specified media ID from *oldserver* to *newserver* and updates the NetBackup image catalog to reflect that the media ID was moved. It is assumed that after the move, *newserver* has access to the media.

`-newserver` *hostname* specifies the name of the host to which the entry is moved.

`-oldserver` *hostname* specifies the name of the host where the catalog entry to be moved currently resides. If you do not specify `-oldserver`, the system where the command is being run is considered to be the old server.

The `-movedb` option is most meaningful in configurations where a master and its media servers are sharing a robotic library and have access to all the media in the robot. If this is not the case, at a minimum, all NetBackup servers must use the same Media Manager volume database, so the media can be moved from one robotic library to another without losing their attributes and assignment status.

`-ev` *media_id*

Specifies the media ID that requires action. The media ID must be six or fewer characters and must be in the NetBackup media catalog.

`-h` *host*

Specifies the host name of the server where the media catalog resides. This option is required only if the volume was not written on the server where you run the `bpmedia` command. In this case, the media ID is in the NetBackup media catalog on the other server and you must specify the name of that server on the `bpmedia` command.

For example, assume you have a master server named whale and a media server named eel. You run the following `bpmedia` command on whale in order to suspend media ID BU0001 that is in the media catalog on eel:

```
bpmedia -suspend -ev BU0001 -h eel
```

Use the NetBackup Media List report to determine the host that has the volume in its media catalog.

`-v`

Select verbose mode. This is only meaningful when running with debug logging turned on (that is, when the *install_path*`\NetBackup\logs\admin` directory exists).

EXAMPLE (MOVEDB)

Note You cannot use the `-movedb` option with NetBackup BusinesServer.

Assume that the master server is HOSTM, with HOSTS1 and HOSTS2 being media servers. The following command, run on HOSTM, moves the media catalog entry for media ID DLT001 from HOSTS1 to HOSTS2 and updates the NetBackup image catalog:

```
bpmedia -movedb -ev DLT001 -newserver HOSTS2 -oldserver HOSTS1
```

FILES

install_path`\NetBackup\logs\admin\*.log`

install_path`\NetBackup\db\media\*.log`

bpmedialist

NAME

`bpmedialist` - Display NetBackup media status

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpmedialist [-mlist] [-U | -l | -L] [-ev` *media_id*`] [-rl` *ret_level*`] [-d` *density*`] [-p` *pool_name*`] [-h` *host_name* `| -M` *master_server*`, ... ] [-v]`

install_path`\NetBackup\bin\admincmd\bpmedialist -summary [-U | -L] [-brief [-p` *pool_name*`] [-h` *host_name* `| -M` *master_server*`, ...] [-v]`

install_path`\NetBackup\bin\admincmd\bpmedialist -mcontents -ev` *media_id* `[-U | -l | -L] [-d` *density*`] [-h` *host_name* `| -M` *master_server*`, ...] [-v]`

install_path`\NetBackup\bin\admincmd\bpmedialist -count -rt` *robot_type* `-rn` *robot_number* `[-d` *density*`] [-U | -l] [-h` *host_name* `| -M` *master_server*`] [-v]`

DESCRIPTION

`bpmedialist` queries one or more NetBackup media catalogs and produces a report on the status of the NetBackup media. This command requires administrator privileges. `bpmedialist` produces one of four reports:

MEDIA LIST REPORT

Media List (`-mlist`) report, provides information on either a single volume or all volumes in the NetBackup media catalog. This report does not apply to disk storage units. The report lists, for each volume in the report, the volume's media Id, media server, and other attributes. This is the default report type.

If `-U` is an option, the status field appears as English text. Otherwise, the status appears as a hexadecimal integer. This is a three-digit value. The interpretation of the two upper-order digits is given here. Any or all of these flags can be set. Settings other than those listed here correspond to unreported states.

>= 0x200 Multiplexing is TRUE.

>= 0x080 Imported is TRUE.

>= 0x040 Multiple retention levels is TRUE.

The interpretation for the low-order status digit is determined by comparing the digit to the following values in order.

>= 0x008 The status is Full.

>= 0x004 This is an unreported state.

>= 0x002 The status is Suspended.

== 0x001 The status is Frozen.

== 0x000 The status is Active.

The reported status is the status for the low-order digit combined with the status for the upper-order digits. For instance, for a status value of 0x040, the media ID is active, and multiple retention levels are in effect.

The `-l` option produces a report in Short mode. Each media ID occupies one line of the report. The fields on this line are listed below. The section on the Media List Report in your NetBackup system administrator's guide describes the fields in detail. Any fields listed below that are not documented in that section are reserved for NetBackup internal use.

- media id
- partner id
- version
- density
- time allocated
- time last written
- time of expiration
- time last read
- Kbytes
- nimages
- vimages (unexpired images)
- retention level
- volume pool
- number of restores
- status (described above)
- hsize
- ssize
- l_offset
- reserved

- psize
- reserved
- 4 reserved fields

MEDIA SUMMARY (-SUMMARY) REPORT

The Media Summary report lists, by server, summary statistics for active and inactive media grouped according to expiration date. The report shows the expiration date for the media and the number of media at each retention level, and the status of each media ID.

MEDIA CONTENTS REPORT

The Media Contents report lists the contents of media as read directly from the media. It lists the backup IDs that are on a single media ID. It does not list each individual file. This report does not apply to disk storage units. Note that if you attempt to abort the command by entering ctl-c and the media requested are still being mounted or positioned, the storage unit may stay in use for some time after the break. Each entry in the report appears as that area of the storage unit is read.

The `-l` format for the Media Contents report produces one line for each backup ID, containing the fields below. The section on the Media Contents Report in your NetBackup system administrator's guide contains more details. Any fields not described in that section are reserved for NetBackup internal use.

- version (1 denotes a DB backup image, 2 denotes a regular backup image)
- backup id
- creation time
- expiration time
- retention level
- fragment number
- file number
- block size (in bytes)
- status
- media_id
- size
- reserved
- data_start
- reserved
- client_type *

- copy_num *
- sched_type *
- flags *
- opt_extra
- mpx_headers
- res1
- policy name *
- schedule label *

* These fields are significant only if version is 2.

MEDIA COUNT (-COUNT) REPORT

The Media Count report shows a count of the number of UP devices matching all the criteria specified. The robot type and the robot number are mandatory criteria for this report. The `-U` format provides a title, Number of UP devices for *rt*(*rn*) = *value*. The `-l` format provides only the value.

OPTIONS

Report-type Options

`bpmedialist` produces one of four types of reports. An option on the command line determines the type of report produced. The report-type options are as follows:

`-mlist`
: Produce a Media List report. This is the default report type.

`-summary`
: Produce a Media Summary report.

`-mcontents`
: Produce a Media Contents report.

`-count`
: Produce a Media Count report. This report also displays the media attribute `ALLOW_MULT_RET_PER_MEDIA` and its value, 0 (do not allow) or 1 (allow).

Report-format Options

The `bpmedialist` report can appear in one of several formats. The report-format options are as follows:

`-brief`
: Produce a brief report. This option is available for the Media Summary report only. The default is a full report, which includes a breakdown of active and non-active media, reporting on each media ID's status within these categories.

`-U`
: Report in user mode. This is the default report mode. The report includes a banner listing the column titles, and the report style is descriptive, rather than terse.

`-L`
: Report in long mode. This format produces the report with the most complete information. For instance, for the Media List report, the report lists the attributes of each media ID as a series of *keyword* = *value* pairs, one attribute per line. A value may be expressed as both a numeric value and a descriptive value.

`-l`
: Report in short mode. This format produces a terse report. This option is useful for scripts or programs that rework the listing contents into a customized report format.

Other Options

The following are the remaining options used by `bpmedialist`:

`-density` *density_type*
: Report on media of this density type. If the robot type is specified on the command line, the value for density should be consistent with the robot type. Available density types are:

`4mm` - 4mm Cartridge

`8mm` - 8mm Cartridge

`dlt` - DLT Cartridge

`qscsi` - 1/4 Inch Cartridge

Note The following densities are supported only on NetBackup DataCenter servers.

`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

`-ev` *media_id*

Report on this media ID only. This is a required option for the Media Contents report.

For the Media List report, this option is optional, and, by default, all media IDs are included in that report. The media ID can be provided in either upper- or lower-case. The media ID must be six or fewer characters and must be in the NetBackup media catalog (that is, assigned from the NetBackup volume pool).

`-h` *host_name*

Note For NetBackup BusinesServer, there is only one server (the master) so use the name of that server for *host_name*.

host_name is either the name of a host, or the character string `ALL`. If *host_name* is the name of a host, the query goes to the media catalog residing on the system host_name. For the `-mcontents` and `-count` options, this option can appear once. For the `-mlist` and `-summary` options, this option can appear more than once. The default is all servers in the set of storage units for removable media.

The system host_name must allow access by the system running `bpmedialist`. *host_name* can be a media server for a master server other than the local master server. The default is the master server of the local cluster.

For a media server for a master server other than the local master, if a `bpmedialist` query is made using `-h` *the_media_server*, and an equivalent `bpmedialist` query uses `-M` *the_media_servers_master*, the `bpmedialist` using `-h` may complete faster. This difference in response time can be significant if the master server addressed by `-M` is located remotely, and the media server addressed by `-h` is local.

If host_name is `ALL`, the query goes to the local master server and its media servers.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server*, . . .

A list of alternative master servers. This is a comma-delimited list of host names. If this option is present, each master server in the list runs the `bpmedialist` command. If an error occurs for any master server, processing stops at that point.

The report is the composite of the information returned by all the master servers in this list. `bpmedialist` queries each of these master servers. Each master server in the list must allow access by the system issuing the `bpmedialist` command.

For `-mcontents` (Media Contents report) only, the master server returns media information from the media catalogs. This media information is for both the master and its media servers (except for NetBackup BusinesServer which does not support remote media servers). For example, if a media ID exists on a media server of one of the master servers in the `-M` list, the master retrieves the media information from the media server and returns it to the system running `bpmedialist`. In this case, both the master server and the media server must allow access by the system issuing the `bpmedialist` command.

The default is the master server for the server running `bpmedialist`.

Note NetBackup BusinesServer supports only one server, the master; so the default, in this case, is always the NetBackup BusinesServer master where you run `bpmedialist`.

`-p` *pool_name*

Report on the media IDs that belong to this volume pool. The default is all pools.

`-rl` *retention_level*

Report on media that are using this retention level. The retention level determines how long to retain backups and archives. The *retention_level* is an integer between 0 and 24. The default retention level is 1.

Following are the retention levels with the installation values for the corresponding retention periods. Note that your site may have reconfigured the retention periods corresponding to the retention levels.

0 1 week

1 2 weeks

2 3 weeks

3 1 month

4 2 months

5 3 months

6 6 months

7 9 months

8 1 year

9 infinite

10 - 24 expires immediately

`1-rn` Report on the robot using this robot number. This is a required option when the `-count` option is used. The robot number can be obtained from the Media Manager device configuration. For rules concerning the use of this number, see your Media Manager system administrator's guide.

`-rt` *robot_type*
Report on a robot of this type. This is a required option when the `-count` option is used. For non-robotic (standalone) devices select NONE. Valid robot types include the following

`RSM` - Removable Storage Manager

`TL4` - Tape Library 4MM

`TL8` - Tape Library 8MM

`TLD` - Tape Library DLT

`TS8` - Tape Stacker 8MM

`TSD` - Tape Stacker DLT

`NONE` - Not robotic

Note The following robot types apply only to NetBackup DataCenter.

`ACS` - Automated Cartridge System

`LMF` - Library Management Facility

`ODL` - Optical Disk Library

`TLH` - Tape Library Half-Inch

`TLM` - Tape Library Multimedia

`TSH` - Tape Stacker Half-Inch

`-v` Select verbose mode. This option causes `bpmedialist` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined).

EXAMPLES

◆ Example 1

The following example produces a media report for all media IDs defined for the master server of the local system and any media servers.

Note For NetBackup BusinesServer, the report includes only media IDs for the master server because remote media servers are not supported.

```
Server Host = hat

id      rl  images   allocated      last updated   density   kbytes  restores
            vimages   expiration     last read        <------- STATUS ------->
-----------------------------------------------------------------------------
143191  0    28   12/03/2000 23:02  12/22/2000 23:00    dlt     736288     1
              7   12/29/2000 23:00  12/09/2000 10:59

144280  0     9   11/25/2000 11:06  12/01/2000 23:03    dlt     290304     0
              0   12/08/2000 23:03      N/A         EXPIRED  FROZEN

AEK800  0    22   12/06/2000 03:05  12/23/2000 03:01    dlt    23213184    0
              7   12/30/2000 03:01  12/09/2000 10:48

C0015   0    28   11/26/2000 02:09  12/23/2000 02:01    dlt     896448     0
              7   12/30/2000 02:01      N/A

IBM001  0    16   12/16/2000  01:01  12/23/2000 01:07   dlt     6447360    0
             14   12/30/2000 01:07      N/A

L00103  0    20   12/07/2000 08:33   12/23/2000 01:07   dlt     7657728    0
              9   12/30/2000 01:07      N/A

L00104  0     9   12/11/2000  01:09  12/21/2000 01:04   dlt     5429504    0
              5   12/28/2000 01:04      N/A
```

- Example 2

  The following example produces a media count report for robot type TLD and robot number 0:

```
bpmedialist -count -rt TLD -rn 0
   ALLOW_MULT_RET_PER_MEDIA 0
   Number of UP devices for TLD(0) = 2
```

- Example 3

  The following example produces a media contents report for media ID AEK802. The report is partially listed below.

```
   bpmedialist -mcontents -ev AEK802
media id = AEK802, allocated 01/08/2001 03:10, retention level = 0


   File number 1
    Backup id = hat_0915786605
    Creation date = 01/08/2001 03:10
    Expiration date = 01/15/2001 03:10
    Retention level = 0
    Copy number = 1
    Fragment number = 2
    Block size (in bytes) = 65536
```

```
File number 2
   Backup id = hat_0915809009
   Creation date = 01/08/2001 09:23
   Expiration date = 01/15/2001 09:23
   Retention level = 0
   Copy number = 1
   Fragment number = 1
 Block size (in bytes) = 65536
```

- Example 4

  In this example, `bpmedialist` runs on the master server buffalo. `bpmedialist` produces a Media List report for master servers hat and duo.

```
bpmedialist -M hat,duo
Server Host = hat

 id     rl  images   allocated      last updated    density  kbytes   restores
           vimages   expiration     last read        <------- STATUS ------->
-------------------------------------------------------------------------
143191   0     51   12/03/2000 23:02  01/11/2001 23:04    dlt    1436686      2
               9   01/18/2001 23:04  01/08/2001 10:26

144280   0      9   11/25/2000 11:06  12/01/2000 23:03    dlt     290304      0
               0   12/08/2000 23:03  01/12/2001 16:10  EXPIRED  FROZEN

AEK800   0     38   12/06/2000 03:05  01/08/2001 03:10     dlt  3922200024      0
               3   01/15/2001 03:10  12/09/2000 10:48  FULL

AEK802   0      6   01/08/2001 03:10  01/12/2001 03:05     dlt   6140544      0
               6   01/19/2001 03:05  01/12/2001 16:12

C0015    0     48   11/26/2000 02:09  01/12/2001 02:11     dlt   1531968      0
               7   01/19/2001 02:11      N/A

IBM000   0     19   01/01/2001 01:09  01/12/2001 02:05    dlt    8284224       0
              13   01/19/2001 02:05  01/09/2001 05:41

Server Host = duo

 id     rl  images   allocated      last updated    density    kbytes  restores
           vimages   expiration     last read        <------- STATUS ------->
-------------------------------------------------------------------------
A00004   0      0   11/16/2001 05:31      N/A            4mm         0       0
               0       N/A             N/A         FROZEN

DLT210   1      5   12/09/2000 06:10  01/08/2001 06:04     dlt      2560       0
               2   01/22/2001 06:04      N/A

DLT215   0    124   12/08/2000 14:57  01/12/2001 08:07     dlt   9788072       4
              28   01/19/2001 08:07  12/31/2000 15:42
```

- Example 5

  In this example, `bpmedialist` reports which of two hosts has a given media ID configured. Since the host hat does not have A00004 configured in its media catalog, it reports, the requested media ID was not found in the NetBackup media catalog or Media Manager volume database

  The host duo does have A00004 configured, so it produces a Media List report for A00004 (the command is all on one line).

```
bpmedialist -mlist -h hat -h duo -ev A00004
```

```
requested media id was not found in NB media database and/or
MM volume database

Server Host = duo

 id     rl  images   allocated      last updated    density    kbytes  restores
           vimages   expiration     last read        <------- STATUS ------->
-------------------------------------------------------------------------
A00004   0      0   11/16/2001 05:31      N/A            4mm       0       0
                0       N/A             N/A         FROZEN
```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\media\mediaDB`

bpminlicense

NAME

`bpminlicense` - Manage NetBackup license file

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpminlicense [-path license_key_file | -M server] [-debug] [-verbose] [-list_keys] [-nb_features | -sm_features]`

install_path`\NetBackup\bin\admincmd\bpminlicense [-path license_key_file | -M server] [-debug] [-verbose] -find_keys | -delete_keys | -add_keys` *keystring1 .. keystringn*

DESCRIPTION

The `bpminlicense` utility manages a NetBackup license file. The preferred method to manage NetBackup licenses is to use the **Help > License Keys** panel in the NetBackup Administration console. For UNIX servers, you may use the `get_license_key`(1M) utility to manage the NetBackup licenses, which is preferred to this command.

OPTIONS

`-add_keys | -delete_keys | -find_keys` *keystring1 .. keystringn*
Respectively, these options find and list, add, or delete one or more specified *keystrings* in the NetBackup license file.

`-debug` Display detailed information to standard error.

`-list_keys`
List the keys in the NetBackup license file.

`-M` *server* Use the standard NetBackup license file from the specified NetBackup *server*.

`-nb_features`

`-sm_features`
Respectively, list only active NetBackup or Storage Migrator feature IDs (and active keys when specified with the `-verbose` option).

`-path` *license_key_file*
Use the specified *license_key_file* on the local system. The default is the standard NetBackup license file.

`-verbose` Display additional information to standard output.

bpplclients

NAME

`bpplclients`, `bpclclients` - Administer the clients within NetBackup policies

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpplclients`

install_path`\NetBackup\bin\admincmd\bpplclients [`*policy_name* | `-allunique [-pt` *policy_type*`]] [-L | -l | -U | -noheader] [-M` *master_server,...*`] [-v]`

install_path`\NetBackup\bin\admincmd\bpplclients` *policy_name* `[-M` *master_server,...*`] [-v] -add` *host_name* *hardware* *os* `[`*priority*`]`

install_path`\NetBackup\bin\admincmd\bpplclients` *policy_name* `[-M` *master_server,...*`] [-v] -delete` *host_name ...*

install_path`\NetBackup\bin\admincmd\bpplclients` *policy_name* `[-M` *master_server,...*`] [-v] -modify` *host_name* `[-hardware` *hardware*`] [-os` *os*`] [-priority` *priority*`]`

install_path`\NetBackup\bin\admincmd\bpplclients` *policy_name* `-rename` *old_client_name* *new_client_name* `[-os` *os*`] [-hardware` *hardware*`]`

DESCRIPTION

Note The command name `bpclclients` is being changed to `bpplclients`. The `bpclclients` command will be completely replaced by `bpplclients` in a future release.

`bpplclients` will do one of the following:

- Produce a listing of clients.
- Add a new client to a policy.
- Delete a list of clients from a policy.
- Modify an existing client in a policy.

For the `-add`, `-delete`, and `-modify` options, `bpplclients` returns to the system prompt immediately after it submits the client change request to NetBackup. To determine whether the change was successful, run `bpplclients` again to list the updated client information.

When the listing option is used, the list is ordered alphabetically by client name. Each client entry is on a single line, and there is a single entry for each client.

This command requires administrator privileges.

OPTIONS

The options used with `bpplclients` depend on the form of `bpplclients` being used.

The first form of `bpplclients` has no options and produces a listing of information about the clients for all policies.

The second form of `bpplclients` produces a listing of information about the clients for a single policy or for all policies. The following options apply to this form:

policy_name | `-allunique [-pt` *policy_type*`]`

policy_name specifies the name of a policy and lists client information only for the policy with this name.

`-allunique` without [`-pt` *policy_type*] lists client information for all policies defined for NetBackup on the master server.

If you use `-allunique -pt` *policy_type*, where *policy_type* is a specific policy type (such as Sybase), the command lists the client information only for the clients that belong to that type of policy.

If the command line contains neither the *policy_name* nor `-allunique` option, the listing contains client information for all policies.

These options, if used, must be the first option on the command line.

`-L`

List in long format. There is no two-line header at the top of the listing; the header is embedded in the line for each client. The line for each client includes the following fields:

Client / HW / OS / Pri: (the header)

Client name

Hardware type

Operating system

Priority

There are also four additional fields which can be ignored. These fields are either unused or used for internal processing.

`-l`

List in short format; this produces a terse listing and is also called *raw output mode*. There is no two-line header at the top of the listing; the header is embedded in the line for each client. The line for each client includes the following fields:

CLIENT (the header)

Client name

Hardware type

Operating system

Priority

There are also four additional fields which can be ignored. These fields are either unused or used for internal processing.

This option is useful for scripts or programs that rework the listing contents into a customized report format.

`-U` List in user format. The listing consists of one line for each client, containing the hardware type, operating system, and client name. A two-line header begins the listing. This is the default format for the listing.

`-noheader`
List without any header. The listing consists of one line for each client, containing the hardware type, operating system, and client name.

`-M` *master_server,* . . .
A list of alternative master servers. This is a comma-delimited list of host names. If this option is present, each master server in the list runs the `bpplclients` command. Each master server in the list must allow access by the system issuing the `bpplclients` command. If an error occurs for any master server, processing stops at that point.

If `bpplclients` is producing a listing, the listing is the composite of the information returned by all the master servers in this list.

If `bpplclients` is adding, deleting, or modifying a client (explained later), the change is made on all the master servers in this list.

`-v` Selects verbose mode. This option causes `bpplclients` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined).

The next three forms of `bpplclients` affect one or more clients in a single policy. The client will be added, deleted, or have its attributes modified within the policy. This form of `bpplclients` uses the following options:

policy_name
Change the client information for this policy. This option must be the first option on the command line.

`-M` *master_server,* . . .
Explained earlier. This option must precede the `-add`, `-delete`, or `-modify` option on the command line.

`-v` Explained earlier. This option must precede the `-add`, `-delete`, or `-modify` option on the command line.

Note The next three options, `-add`, `-delete`, and `-modify`, determine the change that `bpplclients` makes to the clients for the policy. Any of these options, with its accompanying client information, must be the final option on the command line. Only one of these options can be used at a time.

`-add` *host_name hardware os* [*priority*]
: Add a client to the policy. If the local system already has the maximum number of clients defined, an error is returned. The installation default for the maximum number of clients is unlimited for DataCenter and 4 for BusinesServer. Specify the host name, hardware type, and operating system (see the definitions below). (*priority* is not implemented at this time)

`-delete` *host_name ...*
: Delete one or more clients from the policy. Up to twenty clients can be deleted at a time. The clients are provided as a space-delimited list of host names.

`-modify` *host_name ...*
: Modify the attributes for a client within a policy. The client has been added to the policy previously. The attribute values that follow the client name replace the previous equivalent attribute values for this client. At least one of the client's attributes must be modified. `-priority` is not implemented at this time.

`-hardware` *hardware*
: The hardware type of this client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

`-os` *os*
: The operating system of this client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

  The values chosen for the hardware and os options must form a valid combination.

`-priority` *priority*
: Not implemented.

The following form of `bpplclients` changes the name of the client in a policy and can also change the operating system and hardware type that is specified for the client. This form of `bpplclients` uses the following options:

policy_name
: The policy that has the client. This option must be the first option on the command line.

`-rename` *old_client_name new_client_name*

old_client_name specifies the current name of the client and *new_client_name* specifies the new name.

`-hardware` *hardware*

Specifies a different operating system for the client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

`-os` *os*

Specifies a different operating system for the client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

The values chosen for the hardware and os options must form a valid combination.

EXAMPLES

- Example 1

While running on the master server, list the clients known to the master server.

```
bpplclients
```

The output returned will look like the following:

```
Hardware         OS               Client
---------------  ---------------  --------------
C910_920         IRIX5            boris
C910_920         IRIX6            hat
Novell           NetWare          marge
PC               WindowsNT        marmot
HP9000-800       HP-UX10.20       squash
PC               WindowsNT        tiger
```

This command could also be entered on a client of hat, with the same results.

- Example 2

List the clients defined for the policy onepolicy:

```
bpplclients onepolicy
Hardware         OS               Client
---------------  ---------------  --------------
Sun4             Solaris2.6       buffalo
Sun4             Solaris2.5       jeckle
RS6000           AIX              streaky
HP9000-800       HP-UX            chilly
SGI              IRIX5            yak
ALPHA            OSF1             alpha
Sun4             Solaris2.5       heckle
```

```
HP9000-700        HP-UX            shark
NCR               UNIX             cougar
RS6000            AIX              whale
Sun4              SunOS4           oahu
```

- Example 3

  Add the client marmot to the policy twopolicy on the master servers serv1 and serv2. marmot's hardware type is C910_920, and marmot's operating system is IRIX6. The default priority is used. (the command is all on one line)

  ```
  bpplclients twopolicy -M serv1,serv2 -add marmot C910_920 IRIX6
  ```

- Example 4

  Delete the clients marmot and vole from the policy twopolicy on the master servers serv1 and serv2. (the command is all on one line)

  ```
  bpplclients twopolicy -M serv1,serv2 -delete marmot vole
  ```

- Example 5

  While running on the master server hat, list client information for policy BackTrack on the master server beaver:

```
bpplclients BackTrack -M beaver
Hardware         OS               Client
---------------  ---------------  --------------
Sun4             Solaris2.5       saturn
```

- Example 6

  Assume you have a policy called my_policy that has 1 client defined. The client name is pear, the operating system is Solaris2.6, and the hardware type is Solaris.

```
  bpplclients my_policy -rename pear apple -os MacOS \
-hardware MACINTOSH
```

  This command changes the client name pear in my_policy to apple. It also changes the os from Solaris2.6 to MacOS and hardware from Solaris to MACINTOSH.

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bpplclients: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\policy\`*policy_name*`\clients`

SEE ALSO

`bpplinfo`

bpplinfo

NAME

bpplinfo, bpclinfo - Manage or display policy attributes for NetBackup

SYNOPSIS

install_path\NetBackup\bin\admincmd\bpplinfo *policy_name* -L | -l | -U [-v] [-M *master_server,...*]

install_path\NetBackup\bin\admincmd\bpplinfo *policy_name* -set | -modify [-v] [-M *master_server,...*] [-active | -inactive] [-pt *policy_type*] [-ut] [-ef *effective_time*] [-residence *label*] [-pool *label*] [-priority *priority*] [-rfile *flag*] [-blkincr *flag*] [-multiple_streams *flag*] [-keyword "*keyword phrase*"] [-encrypt *flag*] [-collect_tir_info *value*] [-compress *flag*] [-crossmp *flag*] [-disaster *flag*] [-follownfs *flag*] [-policyjobs *max_jobs*]

DESCRIPTION

Note The command name bpclinfo is being changed to bpplinfo. The bpclinfo command will be completely replaced by bpplinfo in a future release.

bpplinfo initializes, modifies, or displays the attribute values for a NetBackup policy. Only the administrator can run this command.

OPTIONS

The options used with bpplinfo depend on the form of bpplinfo being used.

The first form of bpplinfo displays a policy. The following options apply to this form:

policy_name -L | -l | -U

List information for this policy. This is a required option.

-L specifies a long list type and produces a listing with one policy attribute per line, in the format *policy_attribute*: *value*. The value may be expressed both in numeric and name form. Fields in the list include:

Policy Type

Active

Follow NFS Mounts (applies only to NetBackup DataCenter)

Cross Mount Points

Client Compress

Collect TIR Info

Policy Priority

Ext Security Info

File Restore Raw

Client Encrypt

Max Jobs / Policy

Multiple Streams

Frozen Image

Backup Copy

Disaster Recovery

Max Frag Size

Residence

Volume Pool

`-l` specifies a short list type and produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format. A short listing contains the following information for the specified policy:

Line 1: "INFO", client_type, follow_nfs_mounts, client_compress, priority, proxy_client, client_encrypt, disaster recovery, max_jobs_per_policy, cross_mount_points, max_frag_size, active, collect_tir_info, block_incr, ext_sec_info, i_f_r_f_r, streaming, frozen_image, backup_copy, effective_date, policy ID

Line 2: "KEY",keyword

Line 3: "BCMD",backup_command

Line 4: "RCMD",restore_command

Line 5: "RES", residence

Line 6: "POOL", pool

Line 7: "FOE", this field is not used

`-U` specifies a user list type and produces a listing with one policy attribute per line, in the format *policy_attribute*: *value*. This listing is similar to the -L listing, but contains fewer fields.

`-M` *master_server,...*

A list of alternative master servers. This is a comma-delimited list of hostnames. If this option is present, each master server in the list runs the `bpplinfo` command. Each master server in the list must allow access by the system issuing the `bpplinfo` command. If an error occurs for any master server, processing terminates at that point.

For the display form of `bpplinfo`, the report is the composite of the information returned by all the master servers in this list. `bpplinfo` queries each of these master servers. The master server returns information from its policy catalog.

For the policy-definition form of `bpplinfo`, the policy is created or modified on each master server in the list.

The default is the master server for the system running `bpplinfo`.

`-v` Selects verbose mode. This option causes `bpplinfo` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined).

The second form of `bpplinfo` initializes attribute values for a policy or modifies the attribute values for a policy. The following options apply to this form:

Note Not all options apply to every policy type. For instance, if the policy type is *MS-Windows-NT*, `bpplinfo` accepts the options `-compress` and `-crossmp`. When `bpplinfo` completes, it returns a zero status. However, NetBackup's subsequent handling of the policy with the `MS-Windows-NT` policy type is as though the options had not been set.

`-active | -inactive`

Set the policy to active or inactive. If the policy is active, NetBackup runs all its automatic schedules and permits user-directed backups and archives to be used. A policy must be active for an automatic backup to occur. This is the default.

If the policy is inactive, NetBackup does not run any automatic schedules or permit user-directed schedules to be used. This option is useful for temporarily inactivating a policy to prevent schedules from being used.

`-blkincr` *flag*

Note This option applies only if you are running NetBackup DataCenter and also have VERITAS Oracle Edition, which supports block-level incrementally.

`0` (disabled) or `1` (enabled). Perform block-level-incremental backups for clients in this policy.

If `1`, do perform block-level-incremental backups.

If `0`, do not perform block-level-incremental backups.

`-collect_tir_info` *value*

Collect true-image-recovery (TIR) information. True-image recovery allows NetBackup to restore a directory to exactly what it was at the time of any scheduled full or incremental backup. Files deleted before the time of the selected backup are not restored. After enabling this attribute, NetBackup starts collecting additional information beginning with the next full or incremental backup for the policy.

If `0`, NetBackup does not keep track of true-image-recovery information.

If `1`, NetBackup collects TIR information.

If `2`, NetBackup collects TIR information and tracks client files.

`-compress` *flag*

`0` (disabled) or `1` (enabled). Specifies whether to compress files or not. If 1, the files selected are compressed by the client software onto the media. Compression may increase total backup time. If 0, the files are not compressed onto the media. This is the default.

This option has no effect on the hardware compression that may be available on the storage unit.

Image compression is not available on Apollo clients (Note that Apollo clients are supported only by NetBackup DataCenter servers.)

`-crossmp flag`

`0` (disabled) or `1` (enabled). Specifies whether to cross mount points during backups or not.

If `1`, NetBackup backs up or archives all files and directories in the selected path regardless of the file system on which they reside.

If 0, NetBackup backs up or archives only those files and directories that are on the same file system as the selected file path. This is the default.

This attribute can affect the **Follow NFS** policy attribute, which applies only to NetBackup DataCenter. Refer to NetBackup DataCenter system administrator's guide for more details.

This attribute does not affect Apollo clients. Those clients always behave as if the attribute is enabled. (Note that Apollo clients are supported only by NetBackup DataCenter servers.)

`-disaster 0|1`

Collect information required for intelligent disaster recovery. This attribute applies only when you back up Windows clients.

`0` = Do not allow disaster recovery (Default)

`1` = Allow disaster recovery

`-encrypt` *flag*

`0` (disabled) or `1` (enabled). Specifies whether files should be encrypted or not.

If 1, encryption is enabled.

`-followfs 0|1`

Note The `followfs` option applies only to NetBackup DataCenter

0 (disabled) or 1 (enabled). Specifies whether to follow NFS mount points or not. For policy types MS-Windows-NT and OS/2, setting this flag affects the policy attribute **Backup Network Drives** instead of the **Follow NFS** attribute.

If 1, NetBackup backs up or archives any NFS-mounted files encountered.

If 0, NetBackup does not back up or archive any NFS-mounted files encountered. This is the default.

The behavior of this attribute varies somewhat depending on the setting of the **Cross Mount Points** attribute. Refer to the *NetBackup System Administrator's Guide* for more details.

This attribute does not affect Apollo clients. Apollo clients always behave as though the attribute is enabled. Therefore, avoid putting NFS-mounted files in the file list for policy containing Apollo clients unless you want them backed up.

`-keyword "`*keyword phrase*`"`

The value will be associated with all backups created using this policy. The keyword phrase can be used to link related policies. It can also be used during restores to search only for backups that have the keyword phrase associated with them.

`-M` *master_server*`, . . .`

Same as explained earlier.

`-multiple_streams` *flag*

0 (disabled) or 1 (enabled). Allow Multiple Data Streams.

If 1, allow multiple data streams.

If 0, do not allow multiple data streams.

policy_name `-set | -modify`

Initialize or modify attributes for this policy. This is a required option.

`-set` initializes (or reinitializes) attributes for the policy to their default values, except for those attributes set by options on the current command line.

`-modify` modifies attributes for the policy. Attributes that are not explicitly set by options on the current command line do not change their values.

`-pool` *label*

Specifies the volume pool for the policy. The default is NetBackup. The volume pool should be one of the volume pools for the policy storage unit. This attribute is not relevant if a disk storage unit is the residence for the policy. If the policy storage unit is Any_available (Residence: - appears on the `bpplinfo` display), the volume pool for any storage unit can be selected. If "*NULL*" is specified, the volume pool is set to NetBackup. To display the configured volume pools, run *install_path*`\Volmgr\bin\vmpool -listall`.

`-policyjobs` *max_jobs*

The maximum number of concurrent jobs that NetBackup allows for this policy (corresponds to the Limit Jobs per Policy setting in the administration interface). *max_jobs* is always greater than or equal to 0.

For the default or when `-policyjobs` is `0`, `bpplinfo` sets *max_jobs* to a value that corresponds to unlimited. The effective maximum number of jobs in this instance is 8 for NetBackup BusinesServer and 2001 for NetBackup DataCenter.

`-priority` *flag*

The priority of this policy in relation to other policies. Priority is greater than or equal to 0. This value determines the order in which policies are run. The higher the value, the earlier the policy is run. The default is 0, which is the lowest priority.

`-pt` *policy_type*

Specify the policy type by entering one of the following character strings (the default is Standard):

`Informix-On-BAR`

`MS-Exchange-Server`

`MS-SQL-Server`

`MS-Windows-NT`

`NDMP`

`NetWare`

`Oracle`

`OS/2`

`Standard`

`Sybase`

Note The following policy types apply only to NetBackup DataCenter.

`AFS`

`Apollo-wbak`

DataTools-SQL-BackTrack

DB2

FlashBackup

SAP

Split-Mirror

`-residence` *label*

Specifies the label of the storage unit for storing the backups created according to this schedule. The default is Any_available. This allows the policy to use any storage unit which has the attribute On Demand Only? set to No. If the policy needs to use a specific storage unit or the storage unit desired has the attribute On Demand Only? set to Yes, then specify the storage unit. If "*NULL*" is specified, the residence for the schedule is set (or reset) to Any_available. The policy residence determines the residence for the policy schedules, unless the Override Policy Storage Unit setting on an individual schedule specifies a residence. Run `bpstulist` to display the set of defined storage units..

`-rfile` *flag*

`0` (disabled) or `1` (enabled).

If `1`, allow Individual File Restore From Raw.

If `0`, do not allow Individual File Restore From Raw.

For a FlashBackup policy, this option is ignored, since the attribute is always enabled.

Note Note that FlashBackup is available only if you are running NetBackup DataCenter and have the separately-priced FlashBackup option.

`-ut` Any of the date/time arguments that follow `-ut` will be accepted as UNIX time, instead of the standard time format. The `-ut` option is used primarily for Java.

The third form of `bpplinfo` (not shown in the synopsis) shows usage information and has only one option as follows:

`-help` Prints a command line usage message when `-help` is the only option on the command line.

EXAMPLES

Note that references to Follow NFS Mounts in these examples apply only to NetBackup DataCenter.

- Example 1

To set the storage unit of the policy tstpolicy to tstunit and view the results, perform the following:

```
bpplinfo tstpolicy -modify -residence tstunit
bpplinfo tstpolicy -L
Policy Type:         Standard (0)
  Active:             no
  Follow NFS Mounts:  no
  Cross Mount Points: no
  Client Compress:    no
  Collect TIR Info:   no
  Policy Priority:     0
  Ext Security Info:  no
  File Restore Raw:   no
  Client Encrypt:     no
  Max Jobs/Policy:     8
  Multiple Streams:   1
  Disaster Recovery:  0
  Max Frag Size:      0 MB  (unlimited)
  Residence:          tstunit
  Volume Pool:        NetBackup
```

- Example 2

  To set the attributes of policy tstpolicy back to their default values, perform the following:

```
bpplinfo tstpolicy -set
bpplinfo tstpolicy -L
  Policy Type:         Standard (0)
  Active:             yes
  Follow NFS Mounts:  no
  Cross Mount Points: no
  Client Compress:    no
  Collect TIR Info:   no
  Policy Priority:     0
  Ext Security Info:  no
  File Restore Raw:   no
  Client Encrypt:     no
  Multiple Streams:   0
  Disaster Recovery:  0
  Max Jobs/Policy:     8
  Max Frag Size:      0 MB  (unlimited)
  Residence:          -
  Volume Pool:        NetBackup
```

- Example 3

  The following is an example of a short listing for the policy named mkbpolicy:

```
bpplinfo mkbpolicy -l
INFO 0 0 0 0 *NULL* 0 0 99 0 0 0 0 0 0 0 0 *NULL* 1
KEY my temp directory
BCMD *NULL*
RCMD *NULL*
RES mkbunit *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
POOL NetBackup *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
FOE 0 0 0 0 0 0 0 0 0 0
```

FILES

install_path`\NetBackup\logs\admin/*`

install_path`\NetBackup\db\policy\`*policy_name*`\info`

bpplinclude

NAME

bpplinclude, bpclinclude - Maintain the list of files automatically backed up by a NetBackup policy

SYNOPSIS

install_path\NetBackup\bin\admincmd\bpinclude policy_name [-v] [-M *master_server*,...] -add *path_name*

install_path\NetBackup\bin\admincmd\bpinclude policy_name [-v] [-M *master_server*,...] -delete *path_name*

install_path\NetBackup\bin\admincmd\bpinclude policy_name [-v] [-M *master_server*,...] -modify {*old_path_name* *new_path_name*}

install_path\NetBackup\bin\admincmd\bpinclude policy_name [-v] [-M *master_server*,...] -L | -l

DESCRIPTION

Note The command name bpclinclude is being changed to bpplinclude. The bpclinclude command will be completely replaced by bpplinclude in a future release.

bpplinclude maintains the policy file list for a NetBackup policy. This is the list of files backed up when NetBackup runs an automatic backup for the policy. The policy file list does not apply to user backups or archives since users select the files when they start those operations.

bpplinclude performs one of the following operations:

- Adds pathnames to the policy file list
- Deletes pathnames from the policy file list
- Modifies pathnames in the policy file list
- Displays the policy file list for a policy

The -add, -delete, and -modify options include a list of pathnames. The list of pathnames must be the final part of the bpplinclude command line. The pathname must be the entire path from the root of the file system to the desired location. For the absolute pathname syntax for your client type, refer to the File-Path Rules topics in the *NetBackup System Administrator's Guide*. The last part of the path can be a filename, a directory name, or a wildcard specification. You can enclose pathnames in quotes. Use enclosing quotes if the pathname contains special characters or a wildcard specification.

File-Path Rules for does not verify the existence of the input directories or files. NetBackup backs up only the files it finds and does not require that all entries in the list be present on every client.

See the *NetBackup System Administrator's Guide* for additional information on policy file lists.

For database extensions, the input entries are scripts. NetBackup runs these during the backup. See the NetBackup guide that comes with the extension product for additional information.

For certain policy attributes (such as Allow Multiple Data Streams) and extension products (such as NetBackup for NDMP), the entries added to the policy file list may be directives, rather than pathnames. Refer to the *NetBackup System Administrator's Guide* or the NetBackup guide for the extension product.

The options `-l` and `-L` produce nearly identical displays of the policy file list.

`bpplinclude` sends its error messages to stderr. `bpplinclude` sends a log of its activities to the NetBackup admin log file for the current day.

This command requires administrator privileges.

OPTIONS

`-add` *path_name*
: Add these path_names to the policy file list. A pathname must be enclosed in quotes (") if it contains special characters, such as blank(" "), or a wildcard specification. Use a blank to separate two pathnames, not a comma. `bpplinclude` interprets a comma as part of the pathname. This means that `bpplinclude` concatenates two or more comma-delimited pathnames into a single pathname with embedded commas. `bpplinclude` does not verify the syntax or the existence of the pathnames. This option must be the final entry on the command line.

`-delete` *path_name*
: Delete these path_names from the policy file list. Refer to `-add` for the pathname-list syntax. Deleting a pathname from the policy file list does not prevent you from recovering any backups or archives for that pathname. This option must be the final entry on the command line.

`-help`
: Prints a command line usage message when `-help` is the only option on the command line.

`-L`
: Display the contents of the policy file list in long format.

`-l`
: Display the contents of the policy file list in compact format.

Note The `-l` and `-L` displays are similar.

`-modify` {*old_path_name new_path_name*}
Modify an entry in the policy file list. The values are a list of pathname pairs {*old_path_name new_path_name*}. For each pathname pair, *new_name_path* replaces *old_name_path* in the policy file list. If no list entry matches old_path_name, then new_path_name is not entered into the policy file list. Refer to the `-add` option for the pathname syntax. Delimit the list entries with spaces, both within a pathname pair and between pathname pairs. This option must be the final entry on the command line.

`-M` *master_server,...*
A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-v`
Select verbose mode for logging. This is only meaningful when running with debug logging turned on (the *install_path*`\NetBackup\logs\admin` is defined).

OPERANDS

`policy_name`
Specifies the policy for which the policy file list is to be set.

EXAMPLES

- Example 1

  While running on another master server kiwi, display the policy file list for policy oprdoc_policy on the master server plum:

```
bpplinclude oprdoc_policy -L -M plum
 Include:           c:\oprdoc
```

- Example 2

  Illustrate `bpplinclude`'s interpretation of wildcards by adding and deleting pathnames that include one wildcard entry:

```
bpplinclude mkbpolicy -add C:\yap C:\y*
bpplinclude mkbpolicy -L
 Include: C:\yap
 Include: C:\y*
bpplinclude mkbpolicy -delete C:\y*
bpplinclude mkbpolicy -L
 Include: C:\yap
```

Note The wildcard entry `C:\y*` for `-delete` is not interpreted by `bpplinclude` as meaning that both `C:\yap` and `C:\y*` should be deleted. Only `C:\y*` is deleted from the include list for mkbpolicy. The interpretation of the wildcard occurs when NetBackup is selecting files to be backed up, during the actual backup.

- Example 3

  Add two entries to the policy file list for a policy, and then modify them:

```
bpplinclude mkbpolicy -add "C:\ima file" "C:\ura file"
bpplinclude mkbpolicy -L
   Include: C:\ima file
   Include: C:\ura file
bpplinclude mkbpolicy -modify "C:\ima file" "C:\ima file 2" "C:\ura
file" "C:\ura file 2"
bpplinclude mkbpolicy -L
  Include: C:\ima file 2
  Include: C:\ura file 2
```

- Example 4

  Add a raw partition to the policy file list for the policy rc (UNIX clients). The full path name for the device is used (the command is all on one line):

```
bpplinclude rc -add /devices/sbus@2,0/dma@2,81000/esp@2,80000/sd@6,0:h,raw
```

  (see the Adding Unix Raw Partitions to the File List section of the *NetBackup System Administrator's Guide*).

- Example 5

  Display the policy file list for the policy mkb_policy:

```
   bpplinclude mkb_policy -l
  INCLUDE C:\services
  INCLUDE C:\aliases
  INCLUDE C:\Programs
```

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bpplinclude: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\dv\policy\`*policy_name*`\includes`

SEE ALSO

`bpplclients`, `bpplinfo`, `bpplsched`, `bppldelete`, `bppllist`

bpplsched

NAME

bpplsched, bpclsched - Add, delete, or list NetBackup schedules

SYNOPSIS

install_path\NetBackup\bin\admincmd\bpplsched *policy_name* [-v] [-M *master_server*,...] -add *sched_label* [-st *sched_type*] [-freq *frequency*] [-mpxmax *mpx_factor*] [-number_copies *number*] [-rl *retention_level*[,*rl-copy2*,...,*rl-copyn*]] [-residence *storage_unit_label*[,*stunit-copy2*,... *stunit-copyn*]] [-pool *volume_pool_label*[,*pool-copy2*,... *pool-copyn*]] [-fail_on_error 0|1[,0|1,...,0|1][-window *start_duration*] [-cal 0|1|2] [-ut] [-incl *mm/dd/yyyy*] [-excl *mm/dd/yyyy*] [-weekday *day_name_week*] [-dayomonth 1-31 or l]

install_path\NetBackup\bin\admincmd\bpplsched *policy_name* [-v] [-M *master_server*,...] -delete *sched_label*

install_path\NetBackup\bin\admincmd\bpplsched *policy_name* [-v] [-M *master_server*,...] -deleteall

install_path\NetBackup\bin\admincmd\bpplsched *policy_name* [-v] [-M *master_server*...] [-L | -l | -U] [-label *sched_label*]

DESCRIPTION

Note The command name bpclsched is being changed to bpplsched. The bpclsched command will be completely replaced by bpplsched in a future release.

bpplsched will do one of the following:

- Add a new schedule to a policy.
- Delete one or more schedules from a policy.
- Delete all the schedules from a policy.
- List one or all schedules in a policy.

For the -add and -delete options, bpplsched returns to the system prompt immediately after it submits the schedule change request to NetBackup. To determine whether the change was successful, run bpplsched again to list the updated schedule information.

When the listing option is used there is a single entry for each schedule, even if the `-M` option is used. The `-l` form lists the information for each schedule on several lines. `-l` does not identify the attributes by name; these are as follows (where the names are not described, they are reserved for internal NetBackup use):

Line 1: SCHED, schedule name, type, max_mpx, frequency, retention level, u_wind/o/d, 2 internal attributes, maximum fragment size, calendar, number of copies, and fail on error. Note that u_wind/o/d is a field reserved for future use. This is also true for the `u_wind` entry in the `-L` display.

Line 2: SCHEDWIN, seven pairs of the form *start,duration*, expressing the start and duration of the window for each day of the week, starting with Sunday.

Line 3: SCHEDRES, residence (a value for each copy).

Line 4: SCHEDPOOL, pool (a value for each copy).

Line 5: SCHEDRL, retention level (a value for each copy).

Line 6: SCHEDFOE, fail on error (a value for each copy).

If the `-M` option is used, `bpplsched` performs the operation on each of the master servers listed. For instance, if `bpplsched` is adding a schedule, `bpplsched` adds the schedule to the policy on each of the master servers listed for `-M`. If the `-M` option is used on a listing request, the listing is the composite of the information returned by all of the master servers in the `-M` list. If the command fails for any of the master servers, activity stops at that point.

To modify an existing NetBackup schedule, use the NetBackup command `bpplschedrep`.

This command requires administrator privileges.

OPTIONS

These options are common to all forms of `bpplsched`:

policy_name
: The name of the policy that contains the schedules. The policy must exist before running this command. This option is required, and must be the first one on the command line.

`-help`
: Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server*, . . .
: A list of alternative master servers. This is a comma-separated list of host names. If this option is present, each master server in the list runs the `bpplsched` command. Each master server in the list must allow access by the system issuing the `bpplsched` command.

If this option is present, the command is run on each master server in the list. If an error occurs for any master server, processing terminates at that point.

If `bpplsched` is producing a listing, the listing is the composite of the information returned by all the master servers in this list.

If `bpplsched` adds or deletes a schedule, all master servers in this list receive the change.

`-v` Selects verbose mode. This option causes `bpplsched` to log additional information for debugging purposes. The information goes into the NetBackup administration debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined).

The remaining options depend on the form of `bpplsched`. The first form of `bpplsched` adds a schedule to the named policy. The following options apply to this form of `bpplsched`:

`-add` *sched_label* [*suboptions*]

Add a single schedule to the named policy.

The suboptions for the `-add` option explained below. These are attributes of the schedule being added. Refer to the *NetBackup System Administrator's Guide* for details on schedules and their attributes.

`-cal 0|1|2`

Indicates whether `bpplschred` is following a calendar-based schedule or a frequency-based schedule.

0 = frequency-based schedule

1 = calendar-based schedule with no retries after run day

2 = calendar-based schedule with retires after run day

`-dayomonth 1-31 l`

Specifies the day of every month to run the schedule. Enter l (lowercase L) to run the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to run the schedule the 15th day of every month, enter:

```
-dayomonth 15
```

To run the last day of every month, enter:

```
-dayomonth l
```

`-excl` *mm/dd/yyyy*

Indicates to exclude this single date.

`-fail_on_error 0|1[,0|1,...,0|1]`

Specifies whether to fail all other copies if one copy fails. If no parameter is specified, `0` is assumed for all copies. Specify a value for each copy.

0 = Do not fail the other copies

1 = Fail other copies

`-freq` *frequency*

The frequency determines how often backups run for this schedule. The *frequency* represents the number of seconds between backups for this schedule. This frequency does not apply to user backups and archives. The default is one week. Valid range is 0 through 4.

`-incl` *mm/dd/yyyy*

Indicates to include this single date.

`-mpxmax` *mpx_factor*

This is the maximum number of jobs for this schedule that NetBackup will multiplex on any one drive. *mpx_factor* is an integer that can range from 1 through 8 for NetBackup BusinesServer and 1 through 32 for NetBackup DataCenter. A value of 1 means that backups for this schedule are not multiplexed. The default is no multiplexing.

`-number_copies` *number*

Specify the number of simultaneous backup copies. The minimum value is 1. The maximum value is 4 or the Maximum Backup Copies global parameter, whichever is smaller. The default is 1.

`-pool` *volume_pool_label*`[,`*pool-copy2*`, . . .` *pool-copyn*`]`

This is the name of the volume pool. This choice overrides the policy-level volume pool. Entering "*NULL*" causes NetBackup to use the volume pool specified at the policy level. The default is to use the volume pool specified at the policy level. The volume pool label cannot be None. If you do not specify a volume pool at either the schedule level or the policy level, NetBackup uses a default value of NetBackup.

When specifying `-number_copies` greater than 1, specify a pool for each copy.

`-residence` *storage_unit_label*`[,`*stunit-copy2*`, . . .` *stunit-copyn*`]`

This is the name of the storage unit, which specifies the location of the backup images. The value "*NULL*" causes NetBackup to use the storage unit specified at the policy level. The default is for NetBackup to use the storage unit specified at the policy level. If you do not specify a storage unit at either the schedule level or the policy level, NetBackup uses the next storage unit available.

When specifying `-number_copies` greater than 1, specify a residence for each copy.

`-rl` *retention_level* `[,` *rl-copy2* `, . . . ,` *rl-copyn* `]`

The retention level determines how long to retain backups and archives. The retention_level is an integer between 0 and 24. The default retention level is 1. Valid retention levels and their corresponding default retention times are listed below.

When specifying `-number_copies` greater than 1, specify a retention level for each copy.

Caution Because the retention period associated with each level can be changed by using the NetBackup administration interface, your configuration may have different values for each level than those shown here. Use the NetBackup administration interface to determine the actual retention periods before making any changes with this command. Otherwise, backups could expire sooner than you expect, resulting in loss of data.

0 1 week

1 2 weeks

2 3 weeks

3 1 month

4 2 months

5 3 months

6 6 months

7 9 months

8 1 year

9 infinite

10 - 24 expires immediately

`-st` *sched_type*

This is the type of the schedule. The default schedule type is FULL. Here are the possible values, with their meanings, for this attribute:

`FULL` - full

`INCR` - differential incremental

`CINC` - cumulative incremental

`UBAK` - user backup

`UARC` - user archive

`-ut` Any of the date/time arguments that follow `-ut` will be accepted as UNIX time, instead of the standard time format. The `-ut` option is used primarily for Java.

`-weekday` *day_name week*

Specifies a day of the week, and the week of the month, as a run day in the schedule.

The *day_name* is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.

The *week* is the number of the week in the month.

For example, to instruct the policy to run the second Monday of the month, enter:

```
-weekday Monday 2
```

`-window` *start duration*

Specifies when NetBackup can run the backups for this schedule. Every day of the week has the same window.

start is the time at which the backup window opens for this schedule. This is the number of seconds since midnight. This is an integer between 0 and 86399 (there are 86400 seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. This is a non-negative integer.

The second form of `bpplsched` deletes one or more schedules from the named policy. The following option applies to this form of `bpplsched`:

`-delete` *sched_label*

Delete the listed schedules from the named policy. The elements of the sched_label list must be separated by spaces. There can be up to 25 labels in the list.

The third form of `bpplsched` deletes all schedule from the named policy. The following option applies to this form of `bpplsched`:

`-deleteall`

Delete all schedules from the named policy.

The fourth form of `bpplsched` produces a listing of information about the schedules for the named policy. The following options apply to this form of `bpplsched`:

`-l` The list type is short. This is the default list type. This produces a terse listing that includes all attributes for the schedule. Each schedule occupies one line of the listing. Most attribute values are expressed numerically. This option is useful for scripts or programs that rework the listing contents into a customized report format.

`-L` The list type is long. This listing includes all attributes for the schedule. Some attribute values are descriptive terms, rather than numbers.

`-label` *sched_label*
List the attributes for this schedule in the named policy. The default is to list information for all schedules for the named policy.

`-U` The list type is user. This listing is similar to the long-type listing, but it has fewer entries. Most attribute values are descriptive terms, rather than numbers.

EXAMPLES

◆ Example 1

In this example, `bpplsched` lists the information for schedule user within policy tstpolicy in two different ways. The first display is in long mode. The second is in User mode, which shows fewer entries than the Long mode display.

```
bpplsched tstpolicy -L -label user
Schedule:          user
  Type:            UBAK (2)
  Frequency:       1 day(s) (86400 seconds)
  Retention Level: 0 (1 week)
  u-wind/o/d:      0 0
  Incr Type:    DELTA (0)
  Incr Depends: (none defined)
  Max Frag Size:0 MB (unlimited)
  Maximum MPX:  1
  Number copies:1
  Fail on Error:0
  Residence:       (specific storage unit not required)
  Volume Pool:     (same as policy volume pool)
  Daily Windows:
  Day         Open       Close       W-Open     W-Close
   Sunday      000:00:00  024:00:00   000:00:00  024:00:00
   Monday      000:00:00  024:00:00   024:00:00  048:00:00
   Tuesday     000:00:00  024:00:00   048:00:00  072:00:00
   Wednesday   000:00:00  024:00:00   072:00:00  096:00:00
   Thursday    000:00:00  024:00:00   096:00:00  120:00:00
   Friday      000:00:00  024:00:00   120:00:00  144:00:00
  Saturday    000:00:00  024:00:00   144:00:00  168:00:00

bpplsched tstpolicy -U -label user
Schedule:          user
  Type:            User Backup
  Retention Level: 0 (1 week)
  Maximum MPX:     1
  Number copies:1
  Fail on Error:0
  Residence:       (specific storage unit not required)
```

```
 Volume Pool:      (same as policy volume pool)
 Daily Windows:
  Sunday     00:00:00  -->  Sunday     24:00:00
  Monday     00:00:00  -->  Monday     24:00:00
  Tuesday    00:00:00  -->  Tuesday    24:00:00
  Wednesday  00:00:00  -->  Wednesday  24:00:00
  Thursday   00:00:00  -->  Thursday   24:00:00
  Friday     00:00:00  -->  Friday     24:00:00
  Saturday   00:00:00  -->  Saturday   24:00:00
```

- Example 2

  While running on the system hat, list information for the schedule named full in policy tstpolicy, as defined on the master server beaver:

```
bpplsched tstpolicy -M beaver -L -label full
Schedule:          full
 Type:            FULL (0)
 Frequency:       0+ day(s) (14400 seconds)
 Retention Level: 0 (1 week)
 u-wind/o/d:      0 0
 Incr Type:       DELTA (0)
 Incr Depends:    (none defined)
 Max Frag Size:   0 MB (unlimited)
 Maximum MPX:     1
  Number copies:1
  Fail on Error:0
  Residence:       (specific storage unit not required)
 Volume Pool:     (same as policy volume pool)
 Daily Windows:
 Day          Open       Close       W-Open     W-Close
 Sunday       000:00:00  024:00:00   000:00:00  024:00:00
 Monday       000:00:00  024:00:00   024:00:00  048:00:00
 Tuesday      000:00:00  024:00:00   048:00:00  072:00:00
 Wednesday    000:00:00  024:00:00   072:00:00  096:00:00
 Thursday     000:00:00  024:00:00   096:00:00  120:00:00
 Friday       000:00:00  024:00:00   120:00:00  144:00:00
 Saturday     000:00:00  024:00:00   144:00:00  168:00:00
```

- Example 3

  The following example adds a new schedule, full_2, to the policy tstpolicy on beaver, and then lists the new schedule in Long mode. These commands run on the system hat:

```
bpplsched tstpolicy -M beaver -add full_2
bpplsched tstpolicy -M beaver -label full_2 -L
Schedule:          full_2
 Type:            FULL (0)
```

```
 Frequency:       7 day(s) (604800 seconds)
 Retention Level: 1 (2 weeks)
 u-wind/o/d:      0 0
 Incr Type:       DELTA (0)
 Incr Depends:    (none defined)
 Max Frag Size:   0 MB (unlimited)
 Maximum MPX:     1
  Number copies:1
  Fail on Error:0
  Residence:       (specific storage unit not required)
 Volume Pool:     (same as policy volume pool)
 Daily Windows:
 Day         Open       Close       W-Open     W-Close
 Sunday      000:00:00  000:00:00
 Monday      000:00:00  000:00:00
 Tuesday     000:00:00  000:00:00
 Wednesday   000:00:00  000:00:00
 Thursday    000:00:00  000:00:00
 Friday      000:00:00  000:00:00
 Saturday    000:00:00  000:00:00
```

- Example 4

  In this example, `bpplsched` deletes the schedules, full_3, user, user_2, and user_3 from policy tstpolicy:

  ```
  bpplsched tstpolicy -delete full_3 user user_2 user_3
  ```

- Example 5

  In this example, `bpplsched` lists the schedule information for policy tstpolicy:

```
bpplsched tstpolicy -L
Schedule:          full
 Type:            FULL (0)
 Frequency:       1 day(s) (86400 seconds)
 Retention Level: 0 (1 week)
 u-wind/o/d:      0 0
 Incr Type:       DELTA (0)
 Incr Depends:    (none defined)
 Max Frag Size:   0 MB (unlimited)
 Maximum MPX:     1
  Number copies:1
  Fail on Error:0
  Residence:       (specific storage unit not required)
 Volume Pool:     (same as policy volume pool)
 Daily Windows:
 Day         Open       Close       W-Open     W-Close
 Sunday      000:00:00  024:00:00   000:00:00  024:00:00
```

```
 Monday      000:00:00  024:00:00   024:00:00  048:00:00
 Tuesday     000:00:00  024:00:00   048:00:00  072:00:00
 Wednesday   000:00:00  024:00:00   072:00:00  096:00:00
 Thursday    000:00:00  024:00:00   096:00:00  120:00:00
 Friday      000:00:00  024:00:00   120:00:00  144:00:00
 Saturday    000:00:00  024:00:00   144:00:00  168:00:00


Schedule:          user
 Type:            UBAK (2)
 Frequency:       1 day(s) (86400 seconds)
 Retention Level: 0 (1 week)
 u-wind/o/d:      0 0
 Incr Type:       DELTA (0)
 Incr Depends:    (none defined)
 Max Frag Size:   0 MB (unlimited)
 Maximum MPX:     1
Number copies:1
Fail on Error:0
Residence:       (specific storage unit not required)
 Volume Pool:     (same as policy volume pool)
 Daily Windows:
 Day         Open       Close       W-Open     W-Close

 Sunday      000:00:00  024:00:00   000:00:00  024:00:00
 Monday      000:00:00  024:00:00   024:00:00  048:00:00
 Tuesday     000:00:00  024:00:00   048:00:00  072:00:00
 Wednesday   000:00:00  024:00:00   072:00:00  096:00:00
 Thursday    000:00:00  024:00:00   096:00:00  120:00:00
 Friday      000:00:00  024:00:00   120:00:00  144:00:00
 Saturday    000:00:00  024:00:00   144:00:00  168:00:00
```

- Example 6

  In this example, `bpplsched` adds a new schedule, full, with a window from 11 pm to midnight. The second `bpplsched` lists the information for schedule full:

```
bpplsched elevenpm -add full -window 82800 3600
bpplsched elevenpm -U -label full
Schedule:          full
 Type:            Full Backup
 Frequency:       every 7 days
 Retention Level: 1 (2 weeks)
 Maximum MPX:     1
  Number copies:1
  Fail on Error:0
  Residence:       (specific storage unit not required)
 Volume Pool:     (same as policy volume pool)
```

```
Daily Windows:
      Sunday     23:00:00  -->  Sunday     24:00:00
      Monday     23:00:00  -->  Monday     24:00:00
      Tuesday    23:00:00  -->  Tuesday    24:00:00
      Wednesday  23:00:00  -->  Wednesday  24:00:00
      Thursday   23:00:00  -->  Thursday   24:00:00
      Friday     23:00:00  -->  Friday     24:00:00
      Saturday   23:00:00  -->  Saturday   24:00:00
```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\policy\`*policy_name*`\schedule`

SEE ALSO

`bpplschedrep`

bpplschedrep

NAME

bpplschedrep, bpclschedrep - Modify the attributes of a NetBackup schedule

SYNOPSIS

install_path\NetBackup\bin\admincmd\bpplschedrep *policy_name* *sched_label* [-M *master_server*, . . .] [-v] [-st *sched_type*] [-freq *backup_frequency*] [-mpxmax *mpx_factor*] [-cal 0|1|2] [-incl *mm/dd/yyyy*] [-excl *mm/dd/yyyy*] [-delincl *mm/dd/yyyy*] [-delexcl *mm/dd/yyyy*] [-weekday *day_name week*] [-dayomonth 1-31 l] [-delweekday *day_name week*] [-deldayomonth 1-31 l] [-ci] [-ce] [-cw] [-cd] [-number_copies *number*] [-rl *retention_level*[,*rl-copy2*, . . . , *rl-copyn*]] [-fail_on_error 0|1[,0|1,...,0|1]] [-residence *storage_unit_label*[,*stunit-copy2*, . . . *stunit-copyn*]] [-pool *volume_pool_label*[,*pool-copy2*, . . . *pool-copyn*]] [-(0..6) start duration]

DESCRIPTION

Note The command name bpclschedrep is being changed to bpplschedrep. The bpclschedrep command will be completely replaced by bpclschedrep in a future release.

bpplschedrep changes the attributes of a NetBackup schedule. The schedule and policy named by bpplschedrep should already exist when this command is run. If the -M option is used, bpplschedrep changes the schedule on each of the master servers listed.

This command requires administrator privileges.

OPTIONS

-(0..6) *start duration*

Specifies the window during which NetBackup can run the backups for this schedule. This window applies to a specific day of the week. 0 corresponds to Sunday, 1 to Monday, and so on.

start is the time at which the backup window opens for this schedule. This is the number of seconds since midnight. It is an integer between 0 and 86400 (the number of seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. This is a non-negative integer.

`-cal 0|1|2`

Indicates whether `bpplschedrep` is following a calendar-based schedule or a frequency-based schedule.

0 = frequency-based schedule

1 = calendar-based schedule with no retries after run day

2 = calendar-based schedule with retires after run day

`-dayomonth 1-31 l`

Specifies the day of every month to run the schedule. Enter l (lowercase L) to run the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to run the schedule the 15th day of every month, enter:

```
-dayomonth 15
```

To run the last day of every month, enter:

```
-dayomonth l
```

`-deldayomonth 1-31 l`

Specifies a day of every month to be excluded as a run day. Enter 1 (lowercase L) to exclude the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to exclude the 20th day of every month from the schedule, enter:

```
-deldayomonth 20
```

`-delweekday` *day_name week*

Specifies a day of the week and the week of the month to be excluded as a run day from the schedule.

The *day_name* is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday.

The *week* is the number of the week in the month.

For example, to exclude the second Monday of the month, enter:

```
-delweekday Monday 2
```

`-excl` *mm/dd/yyyy*

Indicates to exclude this single date.

`-fail_on_error 0|1[,0|1,...,0|1]`

Specifies whether to fail all other copies if one copy fails. If no parameter is specified, `0` is assumed for all copies. Specify a value for each copy.

0 = Do not fail the other copies

1 = Fail other copies

`-freq` *backup_frequency*

The backup frequency controls how much time can elapse between successful automatic backups for clients on this schedule. Frequency does not apply to user schedules because the user can perform a backup or archive any time the backup window is open. This value is a positive integer, representing the number of seconds between successful automatic backups for this schedule.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-incl` *mm/dd/yyyy*

Indicates to include this single date.

`-M` *master_server*`,...`

A list of alternative master servers. This is a comma-separated list of hostnames. If this option is present, each master server in the list runs the `bpplschedrep` command. Each master server in the list must allow access by the system issuing the `bpplschedrep` command. If an error occurs for any master server, processing terminates at that point.

The schedule attributes will be modified on all the master servers in this list.

`-mpxmax` *mpx_factor*

This is the maximum multiplexing factor for this schedule. Multiplexing sends concurrent, multiple backups from one or several clients to a single drive.

The multiplexing factor can range from 1 through 8 for NetBackup BusinesServer and 1 through 32 for NetBackup DataCenter. A value of 1 specifies no multiplexing and a value greater than 1 means that NetBackup should create multiplexed images on the destination media. The multiplexing factor should be less than or equal to the multiplexing factor for the storage unit.

For more information on multiplexing refer to the multiplexing topic in the *NetBackup System Administrator's Guide*.

`-number_copies` *number*

Specify the number of simultaneous backup copies. The minimum value is 1. The maximum value is 4 or the Maximum Backup Copies global parameter, whichever is smaller. The default is 1.

policy_name

The name of the policy that contains the schedule. This policy has been previously created.

`-pool` *volume_pool_label* `[,` *pool-copy2* `, . . .` *pool-copyn* `]`

Specifies the volume pool(s) for the schedule. Do not use this option if a disk storage unit is the residence for the schedule. If "*NULL*" is specified, the volume pool for the schedule is the volume pool of the policy which contains this schedule.

Specify a pool for each copy.

To display the configured volume pools, run *install_path*`\Volmgr\bin\vmpool -listall`.

`-residence` *storage_unit_label* `[,` *stunit-copy2* `, . . .` *stunit-copyn* `]`

Specifies the label(s) of the storage unit to be used for storing the backups created according to this schedule. If "*NULL*" is specified, the residence for the schedule defaults to the residence of the policy which contains this schedule. If the residence value is a storage unit label, the residence for the schedule becomes that storage unit, overriding the residence for the policy.

Specify a storage unit for each copy.

Run `bpstulist` to display the set of defined storage units.

`-rl` *retention_level* `[,` *rl-copy2* `, . . . ,` *rl-copyn* `]`

Specifies how long NetBackup retains the backups that it creates using this schedule. Valid retention levels and their corresponding default retention times are listed below.

Specify a retention level for each copy.

Caution Because the retention period associated with each level can be changed by using the NetBackup administration interface, your configuration may have different values for each level than those shown here. Use the NetBackup administration interface to determine the actual retention periods before making any changes with this command. Otherwise, backups could expire sooner than you expect, resulting in loss of data.

0	1 week
1	2 weeks
2	3 weeks
3	1 month
4	2 months
5	3 months
6	6 months
7	9 months
8	1 year
9	infinite

10 - 24 expires immediately

NetBackup keeps the information about the backups for the specified time. Then it deletes information about them. Once deleted, the files in the backups are unavailable for restores. When all the backups on a volume have expired, the volume can be reassigned.

sched_label

The name of the schedule to be changed. This schedule has been previously created.

`-st` *sched_type*

Specifies the type of backup this schedule performs. Schedule types fall into two main categories: automatic and user. Automatic schedules define the windows during which the NetBackup scheduler can initiate a backup for this policy.

User schedules define the windows during which a user can initiate a backup or archive.

The values for schedule type are

`FULL`	(full backup)
`INCR`	(differential incremental backup)
`CINC`	(cumulative incremental backup)
`UBAK`	(user backup)
`UARC`	(user archive)

`-weekday` *day_name week*

Specifies a day of the week, and the week of the month, as a run day in the schedule.

The *day_name* is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.

The *week* is the number of the week in the month.

For example, to instruct the policy to run the second Monday of the month, enter:

```
-weekday Monday 2
```

`-v`

Selects verbose mode. This option causes `bpplschedrep` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has debug logging enabled (*install_path*`\NetBackup\logs\admin` directory defined).

EXAMPLES

- Example 1

Set the frequency for a schedule.

```
bpplschedrep mkbpolicy incr -freq 604800
```

This sets to 1 week the frequency with which automatic backups will be performed for the schedule incr in policy mkbpolicy.

◆ Example 2

For Saturday and Sunday of each week, have the window for schedule full in policy newpolicy open at 10 pm instead of 11 pm. Also, have the window duration be 2 hours instead of 1 hour. `bpplschedrep` resets the windows, and `bpplsched` lists the new schedule values.

```
bpplschedrep newpolicy full -0 79200 7200 -6 79200 7200
bpplsched newpolicy -U -label full
Schedule:          full
  Type:            Full Backup
  Frequency:       every 7 days
  Retention Level: 1 (2 weeks)
  Maximum MPX:     1
  Residence:       (specific storage unit not required)
  Volume Pool:     (same as policy volume pool)
  Daily Windows:
        Sunday     22:00:00  -->  Sunday     24:00:00
        Monday     23:00:00  -->  Monday     24:00:00
        Tuesday    23:00:00  -->  Tuesday    24:00:00
        Wednesday  23:00:00  -->  Wednesday  24:00:00
        Thursday   23:00:00  -->  Thursday   24:00:00
        Friday     23:00:00  -->  Friday     24:00:00
        Saturday   22:00:00  -->  Saturday   24:00:00
```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\policy\`*policy_name*`\schedule`

SEE ALSO

`bpplsched`

bppolicynew

NAME

bppolicynew, bpclassnew - Create, copy, or rename a NetBackup policy

SYNOPSIS

install_path\NetBackup\bin\admincmd\bppolicynew *policy_name* [-verbose] [-M *master_server*, . . .]

install_path\NetBackup\bin\admincmd\bppolicynew *policy_name* -sameas *existing_policy_name* [-verbose] [-M master_server,...]

install_path\NetBackup\bin\admincmd\bppolicynew *existing_policy_name* -renameto *policy_name* [-verbose] [-M *master_server*, . . .]

DESCRIPTION

Note The command name bpclassnew is being changed to bppolicynew. The bpclassnew command will be completely replaced by bppolicynew in a future release.

bppolicynew performs one of the following operations on a NetBackup policy:

- Create a new NetBackup policy with default attribute values
- Create a new NetBackup policy with the same attributes as an existing policy r
- Rename an existing NetBackup policy

When bppolicynew runs without -sameas or -renameto, it creates a new NetBackup policy with default attribute values. If -M is present, the defaults used for the policy definition on each master server are the defaults for that master server.

bppolicynew copies a policy by adding a new policy to the NetBackup database. The clients, files, schedules, and attributes for the new policy are the same as those for the existing policy. bppolicynew does not create a policy copy with the same name as an existing policy.

If bppolicynew renames a policy, the existing association of images with the policy is lost. This means that an image listing for the renamed policy does not include the images that were created before the policy was renamed. bppolicynew does not rename a policy to have the same name as an existing policy.

The NetBackup command bpplinfo replaces the policy-attribute defaults with new values. bpplclients, bpplinclude, and bpplsched define the clients, backup files, and schedules for the policy. A policy needs to have at least one client, one file specification, and one automatic schedule before it can run automatic backups.

`bppolicynew` sends its error messages to stderr. `bppolicynew` sends a log of its activity to the NetBackup admin log file for the current day.

This command requires administrator privileges.

See the *NetBackup System Administrator's Guide* for additional information on policies.

OPTIONS

policy_name
: The name of a NetBackup policy which `bppolicynew` creates or the name to which `bppolicynew` changes an existing policy. There is no default value.

  This policy name must differ from any existing policy name. It is composed of numeric, alphabetic, plus, minus, underscore, and period characters. Do not use a minus as the first character or leave any spaces between characters.

existing_policy_name
: The name of a NetBackup policy which already exists when `bppolicynew` runs. There is no default value.

`-renameto`
: Change the name of the existing policy to the new policy name.

`-sameas`
: Create a new policy, copying its characteristics from the existing policy.

`-help`
: Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server,...*
: A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-verbose`
: Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory *install_path*`\NetBackup\logs\admin` is defined).

EXAMPLES

Note that references to Follow NFS Mounts in these examples apply only to NetBackup DataCenter.

- Example 1

Create a policy with default attribute values on the master server plum:

```
bppolicynew ishkabibble -M plum
bppllist ishkabibble -U -M plum
------------------------------------------------------------
Policy Name:        ishkabibble
  Policy Type:          Standard
  Active:              yes
  Client Compress:     no
  Follow NFS Mounts:   no
  Cross Mount Points:  no
  Collect TIR info:    no
  Block Incremental:   no
  Mult. Data Streams:  no
  Client Encrypt:      no
  Policy Priority:      0
  Max Jobs/Policy:      99
  Disaster Recovery:   0
  Residence:           (specific storage unit not required)
  Volume Pool:         NetBackup
  Keyword:             (none specified)

  Clients:      (none defined)

  Include:      (none defined)

  Schedule:     (none defined)
```

◆ Example 2

Create a new policy, mypolicy_copy from the existing policy mypolicy. `bppllist` shows that mypolicy_copy has the same attributes as mypolicy. For brevity, most of the schedule information is omitted here:

```
bppolicynew mypolicy_copy -sameas mypolicy
bppllist mypolicy -U
------------------------------------------------------------
Policy Name:        mypolicy
  Policy Type:          Standard
  Active:              yes
  Client Compress:     no
  Follow NFS Mounts:   no
  Cross Mount Points:  no
  Collect TIR info:    no
  Block Incremental:   no
  Mult. Data Streams:  no
  Client Encrypt:      no
```

```
  Policy Priority:      0
  Max Jobs/Policy:      99
  Disaster Recovery:   0
  Residence:           myunit
  Volume Pool:         NetBackup
  Keyword:             (none specified)

  HW/OS/Client:  CRAY_J90      UNICOS.10.0   ixnay
                 Linux         RedHat        zippity
                 SGI           IRIX6         mango

  Include:  /tmp/my

  Schedule:          full
    Type:            Full Backup
    Frequency:       every 7 days
    Maximum MPX:     1
    Retention Level: 0 (1 week)
    Residence:       (specific storage unit not required)
    Volume Pool:     (same as policy volume pool)
    Daily Windows:
          Sunday     00:00:00  -->  Sunday     08:00:00
          Monday     00:00:00  -->  Monday     08:00:00
          Tuesday    00:00:00  -->  Tuesday    08:00:00
          Wednesday  00:00:00  -->  Wednesday  08:00:00
          Thursday   00:00:00  -->  Thursday   08:00:00
          Friday     00:00:00  -->  Friday     08:00:00
          Saturday   00:00:00  -->  Saturday   08:00:00

  Schedule:          incr
    Type:            Differential Incremental Backup

bppllist mypolicy_copy -U
------------------------------------------------------------
Policy Name:        mypolicy_copy
  Policy Type:          Standard
  Active:              yes
  Client Compress:     no
  Follow NFS Mounts:   no
  Cross Mount Points:  no
  Collect TIR info:    no
  Block Incremental:   no
  Mult. Data Streams:  no
  Client Encrypt:      no
  Policy Priority:      0
  Max Jobs/Policy:      99
  Disaster Recovery:   0
```

```
Residence:           myunit
Volume Pool:         NetBackup
Keyword:             (none specified)

HW/OS/Client:  CRAY_J90      UNICOS.10.0   ixnay
               Linux         RedHat        zippity
               SGI           IRIX6         mango

Include:  /tmp/my

Schedule:          full
  Type:            Full Backup
  Frequency:       every 7 days
  Maximum MPX:     1
  Retention Level: 0 (1 week)
  Residence:       (specific storage unit not required)
  Volume Pool:     (same as policy volume pool)
  Daily Windows:
        Sunday     00:00:00  -->  Sunday     08:00:00
        Monday     00:00:00  -->  Monday     08:00:00
        Tuesday    00:00:00  -->  Tuesday    08:00:00
        Wednesday  00:00:00  -->  Wednesday  08:00:00
        Thursday   00:00:00  -->  Thursday   08:00:00
        Friday     00:00:00  -->  Friday     08:00:00
        Saturday   00:00:00  -->  Saturday   08:00:00

Schedule:          incr
  Type:            Differential Incremental Backup
```

- Example 3

  Rename a policy from policy_old to policy_new. Before and after the renaming, `bppllist` shows the policies in the NetBackup configuration database:

```
bppllist
 mypolicy
 policy_old
 test
bppolicynew policy_old -renameto policy_new
bppllist
 mypolicy
 policy_new
 test
```

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bppolicynew: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\policy\`*policy_name*

SEE ALSO

`bpplclients`, `bpplinfo`, `bpplsched`, `bppldelete`, `bppllist`

bprecover

NAME

`bprecover` - Recover selected NetBackup related catalogs

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bprecover [-v]`

`-l -m media_id -d` *density* `[-v]`

`-l -dpath` *disk_path* `[-v]`

`-l -tpath` *tape_device_path* `[-v]`

`-r [all | ALL |` *image_number*`] -m` *media_id* `-d` *density* `[-stdout] [-dhost` *destination_host*`] [-v]`

`-r [all | ALL |` *image_number*`] -dpath` *disk_device_path* `[-stdout] [-dhost` *destination_host*`] [-v]`

`-r [all | ALL|`*image_number*`] -tpath` *raw_tape_device_path* `[-stdout] [-dhost` *destination_host*`] [-v]`

`-r [all | ALL |` *image_number*`] -opath` *optical_device_path* `[-stdout] [-dhost` *destination_host*`] [-v]`

Note Stop the NetBackup Database Manager service and NetBackup Request Manager service before using this command. Also, ensure that is running on any system that is being recovered.

DESCRIPTION

`bprecover` initiates the NetBackup utility for restoring the NetBackup internal databases called catalogs and recovers catalogs that were backed up by using the procedures described in the NetBackup system administrator's guide. Use `bprecover` only if catalogs were destroyed on disk.

The command has two main modes: list and recover. List shows the contents of a backup media or disk path. Recover recovers the catalog files.

Only the administrator can run this command.

OPTIONS

`-l` Lists the header information from the specified media or disk path.

`-m` *media_id* `-d` *density*

Specifies the media ID and the density of the media from which to recover files. The Device Manager and Volume Manager services must be running when you use the `-m` option. When the `Volmgr\database` directory is restored you will see messages about busy files and must reboot.

media_id must be six or less characters and must be defined in the Media Manager volume database.

density must be one of the following:

`4mm` (4-mm cartridge)

`8mm` (8-mm cartridge)

`dlt` (dlt cartridge)

`dlt2` (dlt cartridge alternate)

`qscsi` (1/4-in cartridge)

Note The following densities apply only to NetBackup DataCenter servers.

`hcart` (1/2 Inch cartridge)

`hcart2` (1/2 Inch cartridge alternate)

`dtf` (DTF cartridge)

`-dpath` *disk_path*

`-tpath` *tape_path*

Specifies a raw device path. If `-m` and `-d` are not specified. You must use `-dpath` or `-tpath` to specify a raw device path. Stop the NetBackup Device Manager and Volume Manager services when using one of these options.

`-r [all | ALL |` *image_number*`]`

Recovers images from the specified media or disk path. There are three modes of recovery available with `-r`:

If `-r all` (or `ALL`) is specified, recover all the images contained in the specified media or disk path.

If `-r` *image_number* is specified, recover only the selected image number from the specified media or disk path.

If `-r` is specified by itself, `bprecover` interactively prompts and asks if you want to recover the images contained in the specified media or disk path.

`-stdout` Specifies that the selected backup image be written to stdout instead of automatically being restored. This option is useful, for example, if only one individual file was lost and you want to restore it without restoring the rest of the catalog files in the image.

Note You cannot specify `-r ALL` with `-stdout` because the `-stdout` option permits only one file image to be read at a time.

`-dhost` *destination_host*

Specifies the host to which the selected catalog is restored. Normally, catalogs are restored to the host where the data originated (as displayed with the `-l` option). The `-d` option makes it possible to restore the catalog to another host.

The NetBackup client or server software must be installed on the destination host and the NetBackup Client service must be running.

Caution Use the `dhost` option with EXTREME caution, since it can overwrite existing catalogs on the destination host. To permit recovery in case you unintentionally overwrite the wrong catalogs, you can move existing catalogs to a temporary directory on the destination host.

Note Do not specify `-r all` (or `ALL`) with `-dhost`. Either explicitly specify an image (for example, `-r 2`) or use the interactive mode (`-r`).

`-v` Selects verbose mode. This is meaningful only when running with debug logging turned on (that is, when the *install_path*`\NetBackup\logs\admin` directory exists).

EXAMPLES

◆ Example 1

List the backup header information for the catalog backup done to disk path `D:\apps\dbbackup`.

```
cd D:\VERITAS\NetBackup\bin\admincmd\
bprecover -l -dpath D:\apps\dbbackup
Database Backup Information from D:\apps\dbbackup

Created:      03/31/97 11:31:34
Server:       bphost

              Path
              ----
IMAGE1 D:\VERITAS\NetBackup\db
IMAGE2 D:\VERITAS\Volmgr\database
```

◆ Example 2

List the backup header information from media ID 000001, which is density dlt.

```
cd D:\VERITAS\NetBackup\bin\admincmd
```

```
bprecover -l -m 000001 -d dlt
 Database Backup Information from 000001

 Created:      03/31/97 05:50:51
 Server:       bphost
 Block size:   32768

             Path
             ----
 IMAGE1 D:\VERITAS\NetBackup\db
 IMAGE2 D:\VERITAS\Volmgr\database
```

◆ Example 3

Recover the `D:\VERITAS\NetBackup\db` files from disk path `D:\apps\dbbackup`.

```
cd D:\VERITAS\NetBackup\bin\admincmd
bprecover -r 1 -dpath D:\apps\dbbackup
Recovering bphost:D:\VERITAS\NetBackup\db
```

◆ Example 4

Recover all the backed up catalogs from media ID JBL29.

```
cd D:\VERITAS\NetBackup\bin\admincmd
bprecover -r ALL -m JBL29 -d 8mm
Recovering bphost:D:\VERITAS\NetBackup\db
Recovering bphost: D:\VERITAS\Volmgr\database
```

◆ Example 5

Interactively restore selected images. Use raw tape path `\\.\Tape1`. Assume that the media that is loaded into the drive is the same one as in example 4.

```
cd D:\VERITAS\NetBackup\bin\admincmd
bprecover -r -tpath \\.\Tape1
 Recover bphost: D:\VERITAS\NetBackup\db y/n (n)? n
 Recover bphost: D:\VERITAS\Volmgr\database y/n (n)? y
 Recovering bphost: D:\VERITAS\Volmgr\database
```

ERRORS

If errors occur during the recover operation, NetBackup writes error messages to the MS-DOS command window when you run the `bprecover` command.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\*`

install_path`\Volmgr\database\*`

SEE ALSO

`tpreq`

NetBackup Troubleshooting Guide Windows versionfor information on disaster recovery.

bprestore

NAME

bprestore - Restores files from the NetBackup server

SYNOPSIS

install_path\NetBackup\bin\bprestore [-A | -B] [-BR *be_redirection_path*] [-F *file_options*] [-K] [-l | -H | -y] [-r] [-T] [-L *progress_log* [-en]] [-R *rename_file*] [-C *client*] [-D *client*] [-S *master_server*] [-t *policy_type*] [-p *policy*] [-s *mm/dd/yy* [*hh:mm:ss*]] [-e *mm/dd/yy* [*hh:mm:ss*]] [-w [*hh:mm:ss*]] [-k "*keyword_phrase*"] -f *listfile* | *filenames*

DESCRIPTION

bprestore lets users restore a backed up or archived file or list of files. You can also name directories to restore. If you include a directory name, bprestore restores all files and subdirectories of that directory. You can exclude a file or directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or directory path (does not apply to NDMP restores). The exclude capability is useful, for example, if you want to exclude part of a directory from the restore.

By default, you are returned to the system prompt after bprestore is successfully submitted. The command works in the background and does not return completion status directly to you. The -w option lets you change this behavior so bprestore works in the foreground and returns completion status after a specified time period.

The bprestore command restores the file from the most recent backups within the time period you specify, except for a true-image restore (see the -T option description).

bprestore overwrites any file of the same name that already exists on the local client disk, unless you include the -K option. It is also possible to restore files that were backed up or archived on another client (-C option). You must be validated by the NetBackup administrator to restore from other clients.

Use the bplist command to display information on the files and directories that were backed up or archived.

bprestore writes informative and error messages to a progress-log file if you create the file prior to running the bprestore command and then specify the file with the -L *progress_log* option. If bprestore cannot restore the requested files or directories, you can use the progress log to find the reason for the failure.

For detailed troubleshooting information, create a directory named *install_path*\NetBackup\logs\bprestore with write access. bprestore then creates an debug log file in this directory.

The following restrictions apply to `bprestore`:

- You can restore files and directories that you own and those owned by other users if you have read access. You need write access to another user's directories and files to restore that user's files to their original location.
- The operating system restricts the number of files and directories that you can specify on a single `bprestore` command line. If this is a problem, use the `-f` option to restore the files.

OPTIONS

`-A | -B` Specifies whether to restore from archives (`-A`) or backups (`-B`). The default is `-B`.

`-BR` *be_redirection_path*

Contains the redirection path when restoring Backup Exec files. Valid only when `-F` is set to 524288. For example, when only Backup Exec files are being restored.

`-F` *file_options*

Allows either Backup Exec files to be restored, or both Backup Exec and NetBackup files to be restored. The default (`-F` is not specified), is to restore only NetBackup files.

To restore only Backup Exe files specify:

```
-F 524288
```

To restore Backup Exe and NetBackup files specify:

```
-F 1048576
```

`-K` Specifying this option causes `bprestore` to keep existing files rather than writing over them when restoring files with the same name. The default is to overwrite existing files.

Note The `-l | -H | -y` options apply only when restoring UNIX files to a UNIX system.

`-l | -H | -y`

Specifying `-l` renames the targets of UNIX links by using the `-R` *rename_file* option in the same way as when renaming files.

Specifying `-H` renames UNIX hard links by using the `-R` *rename_file* option in the same way as when renaming files. Soft links are unchanged.

Specifying `-y` renames UNIX soft links by using the `-R` *rename_file* option in the same way as when renaming files. Hard links are unchanged.

See Example 5 in the EXAMPLES section.

`-r` Specifying this option restores disk images instead of file systems.

`-L` *progress_log* `[-en]`

Specifies the name of an existing file in which to write progress information.

For example: `c:\proglog`

The default is to not use a progress log.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-R` *rename_file*

Specifies the name of a file with name changes for alternate-path restores.

For example: `bprestore -R /C/renamefile /C/origfile`

Where `/C/rename_file` is the file with the name change and `/C/origfile` is the file to be renamed.

Use the following form for entries in the rename file:

`change` *backup_filepath* `to` *restore_filepath*

The file paths must start with / (slash)

The first *backup_filepath* that is matched is replaced with the *restore_filepath* string. Use all upper case for the drive letter.

The default is to restore using the original path.

For example, the following entry renames `C:\users\fred` to `C:\users\fred2`:

```
change /C/users/fred to /C/users/fred2
```

(be sure to end the entry with a return)

When restoring to a Windows client, you can also use the following method for specifying entries in the rename file (do not use this method for other clients):

`rename` *bulength backup_filepath reslength restore_filepath*

Where:

bulength is the number of ASCII characters in the backup path.

reslength is the number of ASCII characters in the restore path.

The first *backup_filepath* that is matched is replaced with the *restore_filepath* string.

For example, the following entry renames `C:\fred.txt` to `C:\fred2.txt`:

```
rename 11 /C/fred.txt 12 /C/fred2.txt
```

(be sure to end the entry with a return)

`-C` *client* Specifies a client name to use for finding backups or archives from which to restore files. This name must be as it appears in the NetBackup catalog. The default is the current client name.

Note The destination client does not default to the source client. See the description for `-D` *client* option.

`-D` *client* Specifies a destination client. This can be done by an administrator on the master server in order to direct the restored files to a machine other than the client specified with the `-C` option. The default is the current client name.

`-S` *master_server*
Specifies the name of the NetBackup server. The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the user interface on the client and click Specify NetBackup Machines on the Actions menu.

`-t` *policy_type*
Specifies one of the following numbers corresponding to the policy type (the default is `0` on all clients except Apollos, where it is `3`):

`0` = Standard

`4` = Oracle

`6` = Informix-On-BAR

`7` = Sybase

`10` = NetWare

`13` = MS-Windows-NT

`14` = OS/2

`15` = MS-SQL-Server

`16` = MS-Exchange-Server

`19` = NDMP

Note The following policy types apply only to NetBackup DataCenter.

`3` = Apollo-wbak

`11` = DataTools-SQL-BackTrack

`17` = SAP

`18` = DB2

`20` = FlashBackup

`21` = Split-Mirror

`22` = AFS

`-p` *policy* Specifies the policy for which the backups or archives were performed.

`-s` *mm/dd/yy* [*hh:mm:ss*]

`-e` *mm/dd/yy* [*hh:mm:ss*]

Specifies the start and end date range for the listing. The `bprestore` command restores only files from backups or archives that occurred within the specified start and end date range.

`-s` specifies a start date and time for the restore window. `bprestore` restores files only from backups or archives that occurred at or after the specified date and time. Use the following format:

mm/*dd*/*yy* [*hh*[:*mm*[:*ss*]]]

The valid range of dates are from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default start date is 01/01/1970 00:00:00.

`-e` specifies an end date and time for the restore window. `bprestore` restores only files in backups or archives that occurred at or before the specified date and time. Use the same format as for the start date and time.

The end backup date and time do not need to be exact, except for a true-image restore (see the `-T` option description). The bprestore command restores the file that has the specified backup date and time or the file that is the most recent backup preceding the end date and time. The default is the current date and time."

If you do not specify either `-s` or `-e`, `bprestore` restores the most recently backed up version of the file.

`-T` Specifies a true-image restore, where only files and directories that existed in the last true-image backup are restored. This option is useful only if true-image backups were performed. If this option is not specified, all files and directories meeting the specified criteria are restored, even if they were deleted.

When the `-T` option is specified, the image requested must be uniquely identified. Unique identification is accomplished by using the `-e` option with seconds granularity. The `-s` option, if any, is ignored. The seconds granularity of an image can be retrieved by using the `bplist` command with the `-l` and `-Listseconds` options.

`-w` [*hh:mm:ss*]

Causes NetBackup to wait for a completion status from the server before returning you to the system prompt.

You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the restore is complete, the command exits with a timeout status. The restore, however, still completes on the server.

Specifying 0 or not specifying a time, means wait indefinitely for the completion status.

`-k "`*keyword_phrase*`"`

Specifies a keyword phrase for NetBackup to use when searching for backups or archives from which to restore files. The phrase must match the one that was previously associated with backup or archive by the `-k` option of the `bpbackup` or `bparchive` command.

You can use this option in place of or in combination with the other restore options in order to make it easier to restore your backups and archives. The following meta characters can simplify the task of matching keywords or parts of keywords in the phrase:

* matches any string of characters.

? matches any single character.

[ ] matches one of the sequence of characters specified within the brackets.

[-] matches one of the range of characters separated by the "-".

The keyword phrase can be up to 128 characters in length. All printable characters are permitted including space (" ") and period (."). The phrase must be enclosed in double quotes ("...") or single quotes (‘...’).

The default keyword phrase is the null (empty) string.

`-f` *listfile*

Specifies a file (*listfile*) containing a list of files to be restored and can be used instead of the *filenames* option. In *listfile*, list each file path on a separate line.

The format required for the file list depends on whether the files have spaces or newlines in the names.

To restore files that do not have spaces or newlines in the names, use this format:

filepath

Where *filepath* is the path to the file that you are restoring. For example:

Note Use upper case for the drive letter. For example, `C:\NetBackup\Log1`.

```
C:\programs
C:\winnt
C:\documents\old_memos
```

To restore files that have spaces or newlines in the names, use one of the following formats:

filepathlen filepath

filepathlen filepath start_date_time end_date_time

filepathlen filepath `-s` *datetime* `-e` *datetime*

The *filepath* is the path to the file you are restoring.

The *filepathlen* is the total number of characters in the file path.

The *start_date_time* and *end_date_time* are the decimal number of seconds since 01/01/1970 00:00:00.

datetime is the same as the command line (*mm/dd/yy* [*hh*[:*mm*[:*ss*]]]). The start and end date and time specified on the command line is used unless a line in *listfile* overrides it. The dates may change from line to line.

You can exclude a file or directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or directory path (except when performing NDMP restores).

The following is an example that uses *filepathlen filepath*:

```
11 C:\programs
8 C:\winnt
22 C:\documents\old memos
17 !C:\programs\test
```

filenames Names one or more files to be restored and can be used instead of the `-f` option.

Any files that you specify must be listed at the end, following all other options. You must also specify absolute file paths. You can exclude a file or directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or directory path (except when performing NDMP restores).

Use upper case for the drive letter. For example, `C:\NetBackup\log1`.

EXAMPLES

- Example 1

  To restore files from backups of `C:\programs\file1` that were performed between 04/01/2001 06:00:00 and 04/10/2001 18:00:00, enter the following (all on one line):

```
bprestore -s 04/01/93 06:00:00 -e 04/10/93 18:00:00 C:\user1\file1
```

- Example 2

  To restore files listed in a file named `restore_list` by using the most recent backups, enter the following:

```
bprestore -f c:\restore_list
```

- Example 3

To restore the directory `C:\kwc` from the backups that are associated with a keyword phrase that contains “My Home Directory” and use a progress log named `d:\kwc\bkup.log`, enter the following (all on one line):

```
bprestore -k "*My Home Directory*" -L d:\kwc\bkup.log C:\kwc
```

- Example 4

  To restore the `D` drive on the Windows NT client slater from the backups that are associated with a keyword phrase that contains “My Home Dir” and use a progress log named `c:\kwc\bkup.log`, enter the following (all on one line, or using the backslash continuation character):

```
bprestore -k "*My Home Dir*" -C slater -D slater -t 13 -L
c:\kwc\bkup.log  D:\
```

- Example 5

  Assume you have a rename file named `/home/kwc/rename` on a UNIX client and it contains the following:

```
change /home/kwc/linkback to /home/kwc/linkback_alt
```

  To restore the hard link named `/home/kwc/linkback` to alternate path `/home/kwc/linkback_alt` on that client, run the following command:

```
bprestore -H -R /home/kwc/rename /home/kwc/linkback
```

- Example 6

  Assume you want to restore files from backups of `C:\user1\` that were performed between 04/01/01 06:00:00 and 04/10/01 18:00:00. You also want to exclude all files with a `.pdf` extension, except for the one named `final_doc.pdf`. To do this, run the following (all on one line, or using the backslash continuation character):

```
bprestore -s 04/01/01 06:00:00 -e 04/10/01 18:00:00 C:\user1\
!C:\user1\*.pdf C:\user1\final_doc.pdf
```

FILES

install_path`\NetBackup\logs\bprestore\*.log`

bpstuadd

NAME

`bpstuadd` - Create a NetBackup storage unit group or a storage unit

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpstuadd -group` *group_name* *stunit_name*`, . . .`

install_path`\NetBackup\bin\admincmd\bpstuadd -label` *storage_unit_label* `-path` *path_name* | {`-density` *density* `[-rt` *robot_type* `-rn` *robot_number*`]} [-host` *host_name*`] [-cj` *max_jobs*`] [-odo` *on_demand_only*`] [-mfs` *max_fragment_size*`] [-maxmpx` *mpx_factor*`] [-nh` *NDMP_attach_host*`] [-verbose] [-fastrax] [-M` *master_server*`, . . .]`

DESCRIPTION

The `bpstuadd` command creates a NetBackup storage unit or storage unit group. When creating a single storage unit, ensure you include a label for the new storage unit and either the `-density` or the `-path` option. The `bpstuadd` command will not create the storage unit if the master server has already created the maximum number of storage units allowed by its NetBackup configuration.The command will not create a storage unit that specifies the same destination medium as an existing storage unit.

There are several types of storage units. The storage-unit type affects how NetBackup stores the data. The options on the `bpstuadd` command line determine the storage-unit type, which is one of the following:

- Disk. The storage destination is a disk file system directory.
- Media Manager. The storage destination is a medium (a tape or optical device) managed by the Media Manager.
- NDMP. An NDMP storage unit is controlled by Media Manager. The NetBackup for NDMP option must be installed. Where the Media Manager storage-unit type is discussed in this command description, the discussion also applies to the NDMP storage-unit type, unless it is specifically excepted. The media for an NDMP storage unit always attach directly to an NDMP host and cannot be used to store data for other NetBackup clients. When defining an NDMP storage unit, t `bpstuadd` command must be run on the master server. Refer to the NetBackup for NDMP System Administrator's Guide for more information on adding NDMP storage units.

Errors go to stderr. A log of the command's activity goes to the NetBackup admin log file for the current day.

This command requires administrator privileges.

See the NetBackup system administrator's guide for additional information on storage units.

OPTIONS

`-cj` *max_jobs*

The maximum number of concurrent jobs permitted for this storage unit. *max_jobs* is a non-negative integer. The appropriate value depends on your server's ability to comfortably run multiple backup processes and the available space on the storage media. Also, refer to Maximum Jobs per Policy in the *NetBackup System Administrator's Guide*.

0 means that this storage unit will never be selected when a job is being scheduled. The default is 1.

`-density` *density*

If this option is present, the storage unit type is Media Manager. There is no default for this option. Either `-density` or `-path` must be on the command line. Do not use `-path` when `-density` is being used. If the robot type is specified on the command line, the value for *density* should be consistent with the robot type.

Valid *density* types are:

`dlt` - DLT Cartridge

`dlt2` - DLT Cartridge alternate

`8mm` - 8mm Cartridge

`4mm` - 4mm Cartridge

`qscsi` - 1/4 Inch Cartridge

Note The following densities are supported only on NetBackup DataCenter servers.

`hcart` - 1/2 Inch Cartridge

`hcart2` - 1/2 Inch Cartridge alternate

`dtf` - DTF Cartridge

`odiskwm` - Optical Disk Write-Many

`odiskwo` - Optical Disk Write-Once

`-fastrax`

Specifies a Fastrax storage unit.

`-group` *group_name stunit_name stunit_name*

Add a storage unit group, specifiying the group name and the storage unit(s) that comprise the group. Add multiple storage units to the storage unit group by separating the names with a space. The maximum length of a storage unit group label is 128 characters.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-host` *host_name*

Note NetBackup BusinesServer does not support remote media servers.

The NetBackup host that is associated with the destination media. The default is the hostname of the local system.

The host you select must be either your NetBackup master server or a remote media server (if you are configuring remote media servers). The host name must be the network name for the server as known by all NetBackup servers and clients.

If *host_name* is a valid network name, but it has not been configured in NetBackup previously, *host_name* will be added to NetBackup's configuration as a media server. On UNIX, this shows up as a `SERVER` entry in the `bp.conf` file; on Windows, this shows up on the Servers tab in the server properties dialog box in the NetBackup configuration window. If *host_name* is not a valid network name, you must configure it manually.

`-label` *storage_unit_label*

The name of the storage unit. This is a required option unless you are using `-group`. The maximum length of a storage-unit label is 128 characters.

`-mfs` *max_fragment_size*

The maximum fragment size specifies, in megabytes, how large a fragment for a NetBackup image can be.

For a Media Manager storage unit, this value is either zero (the fragment size is unlimited, meaning there is no fragmentation) or any integer greater than or equal to 50 megabytes (MB). The default value is 0.

For a Disk storage unit, this value ranges from 20 megabytes to 2000 megabytes (2 gigabytes). The default value is 2000 (2 gigabytes).

`-maxmpx` *mpx_factor*

The maximum multiplexing factor. Multiplexing sends concurrent, multiple backups from one or several clients to a single drive. Refer to the topic "Multiplexing (MPX)" in the NetBackup system administrator's guide.

The multiplexing factor can range from 1 to 32. 1 means no multiplexing. A value greater than 1 means that NetBackup can create multiplexed images on the destination medium. Licensing determines the effective subset of the 1,_,32 range for the local NetBackup installation.

The default is 1.

`-M` *master_server*

A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point. The default is the master server for the system where the command is entered.

`-nh` *NDMP_attach_host*

Specifies the hostname of the NDMP server. If this option is present, the storage unit type is set to NDMP. The default is no NDMP server.

`-odo` *on_demand_only*

The On-Demand-Only flag controls the condition under which NetBackup uses the storage unit:

To make the storage unit available only to policies or schedules that request it, set the flag to 1 (enabled).

To make the storage unit available to any policy or schedule, set the flag to 0 (disabled).

If the storage unit's type is Disk, the default is 1; NetBackup uses the storage unit only when explicitly requested. Otherwise, the default is 0.

`-path` *path_name*

The path to a disk filesystem, expressed as an absolute pathname. This is the data storage area for this storage unit. When this option is present, the storage unit type is Disk. There is no default for this option. Either `-path` or `-density` must be on the command line. Do not use `-density` when `-path` is being used.

In general when this option is used, it is recommended that the On-Demand-Only flag be enabled (see `-odo`). Otherwise, any NetBackup policy that does not require a specific storage unit has the opportunity to fill the disk filesystem *path_name*. This can cause serious system problems. For instance, if the system swap area happens to be on the same filesystem, new processes may fail.

`-rn` *robot_number*

The robot number for this storage unit. The robot number must be greater than or equal to 0. The robot number can be obtained from the Media Manager device configuration. The Media Manager system administrator's guide discusses the rules concerning the use of this number. This option is ignored unless the `-rt` option is present. There is no default for this option.

`-rt` *robot_type*

The robot type for this storage unit. For non-robotic (standalone) devices select `NONE` or omit this option. The default value is `NONE` (Not Robotic). The value for density should be consistent with the robot type.

If this option is set to any value other than `NONE`, the -rn option is required. Available robot type codes are:

`NONE` - Not Robotic

`TLD` - Tape Library DLT

`TSD` - Tape Stacker DLT

`ACS` - Automated Cartridge System

`TS8` - Tape Stacker 8MM

`TL8` - Tape Library 8MM

`TL4` - Tape Library 4MM

`ODL` - Optical Disk Library

`TSH` - Tape Stacker Half-inch

`TLH` - Tape Library Half-inch

`TLM` - Tape Library Multimedia

`LMF` - Library Management Facility

`RSM` - Removable Storage Manager

`-verbose`

Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory *install_path*`\NetBackup\logs\admin` is defined).

EXAMPLES

◆ Example 1

Create a new storage unit, named hatunit. Its storage unit type is Disk. The path for the storage unit is `C:\tmp\hatdisk`:

```
bpstuadd -label hatunit -path C:\tmp\hatdisk/tmp/hatdisk -verbose
  <2>bpstuadd: INITIATING: NetBackup 3.2Beta created: 98121513
  <2>bpstuadd: EXIT status = 0.
```

◆ Example 2

Note The following example refers to remote media servers and applies only to NetBackup DataCenter. NetBackup BusinesServer supports only a master server, not remote media servers.

Create a storage unit using a UNIX server, which has not been configured previously in NetBackup:

```
% bpstuadd -label parrot_stu -host parrot -density dlt -rt TLD -rn 2
```

The remote media server parrot was added to the `bp.conf` file.

You must also install NetBackup and Media Manager on parrot and run the `add_slave_on_clients` shell script on mango.

```
% grep parrot /usr/openv/netbackup/bp.conf
SERVER = parrot
SERVER = parrot
```

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bpstuaddnew: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\config\storage_units`

SEE ALSO

`bpstudel`, `bpstulist`, `bpsturep`

bpstudel

NAME

`bpstudel` - Delete a NetBackup storage unit or storage unit group

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpstudel -label` *storage_unit_label* `[-verbose] [-M` *master_server*`, . . .`*master_server*`]`

install_path`\NetBackup\bin\admincmd\bpstudel -group` *group_name* `[-verbose] [-M` *master_server*`, . . .`*master_server*`]`

DESCRIPTION

The `bpstudel` command deletes a NetBackup storage unit or storage unit group. The command must include either a label name for the storage unit or a group name for the storage unit group, but not both.

If `bpstudel` cannot delete the storage unit (if for instance, if the storage unit label is mistyped on the command line), it does not return an error message. You can run `bpstulist` to verify that the storage unit was deleted.

Errors are sent to stderr. A log of the command's activity is sent to the NetBackup admin log file for the current day.

This command requires administrator privileges.

See your NetBackup system administrator's guide for additional information on storage units.

OPTIONS

`-label` *storage_unit_label*
: The name of the storage unit. This is a required option. The maximum length for a storage-unit label is 128 characters.

`-group` *group_name*
: The name of a storage unit group. If this option is present, the named storage unit group is deleted.

`-M` *master_server*
: A list of master servers. This is a comma-separated list of host names. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point. The default is the master server for the system where the command is entered.

`-verbose` Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory *install_path*`\NetBackup\logs\admin` is defined).

EXAMPLES

Delete the storage unit named tst.dsk, listing the existing storage units before and after the deletion:

```
bpstulist
stuunit 0 mango 0 -1 -1 1 0 C:\tmp\stuunit 1 1 2000 *NULL*
tst.dsk 0 mango 0 -1 -1 3 0 C:\hsm3\dsk 1 1 2000 *NULL*

bpstudel -label tst.dsk

bpstulist
stuunit 0 mango 0 -1 -1 1 0 C:\tmp\stuunit 1 1 2000 *NULL*
```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\config\storage_units`

SEE ALSO

`bpstuadd`, `bpstulist`, `bpsturep`

bpstulist

NAME

`bpstulist` - Display one or all of the NetBackup storage units or storage unit groups

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpstulist [-label` *storage_unit_label*`] [-L|-l|-U] [-g] [-verbose] [-M` *master_server*`, . . .` *master_server*`]`

install_path`\NetBackup\bin\admincmd\bpstulist [-group` *group_name*`] [-verbose] [-M` *master_server*`, . . .` *master_server*`]`

DESCRIPTION

The `bpstulist` command displays the attributes for a NetBackup storage unit or storage unit group. If no storage unit label or storage unit group name is specified, the command displays the attributes for all NetBackup storage units or storage unit groups.

Errors are sent to stderr. A log of the command's activity is sent to the NetBackup admin log file for the current day.

This command requires administrator privileges.

See your NetBackup system administrator's guide for additional information on storage units.

OPTIONS

List-type options:

`-L` The list type is long. This option produces a listing with one storage-unit attribute per line, in the format *storage-unit attribute*: *value*. Some attribute values are expressed in both interpreted and raw form. For instance, a robot-type entry might be `TL4 (7)` (7 is NetBackup's internal value for a TL4 robot).

For a disk storage unit, a long listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Concurrent Jobs
- On Demand Only
- Path
- Robot Type (not robotic)

- Max Fragment Size
- Max MPX

For a Media Manager storage unit, a long listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Number of Drives
- On Demand Only
- Density
- Robot Type/Number
- Max Fragment Size
- Max MPX/drive

`-l` The list type is short. This produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format. This is the default list type.

A single line contains the information for a storage unit, with all attribute values expressed in raw form. The fields on this line are:

- label
- storage unit type
- host
- robot_type
- robot_number
- density
- concurrent_jobs
- initial_mpx
- path
- on_demand_only
- max_mpx
- maxfrag_size
- ndmp_attach_host

`-U` The list type is user. This option produces a listing with one storage-unit attribute per line, in the format *storage-unit attribute*: *value*. Attribute values are expressed in interpreted form. For instance, a robot-type value might be `TL4`, instead of `7`.

For a disk storage unit, a user-type listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Concurrent Jobs
- On Demand Only
- Max MPX
- Path
- Max Fragment Size

For a Media Manager storage unit, a user-type listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Number of Drives
- On Demand Only
- Max MPX/drive
- Density
- Robot Type/Number
- Max Fragment Size

`-g` This list type causes the storage unit list to include the storage unit groups. The format of this option produces a listing with one storage unit group per line, in the format *group_name*: *group_members*.

Here are the remaining options for `bpstulist`:

`-label` *storage_unit_label*
The name of the storage unit. If this option is not present, the listing is for all storage units. The maximum length for a storage-unit label is 128 characters.

`-group` *group_name*
A list that includes all defined storage units and storage unit groups. The list type for the list of storage units is short. This produces a terse listing. The list of storage unit groups is in the format *group_name*: *group_members*.

`-M` *master_server*, . . . *master_server*
A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the

command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-verbose` Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory *install_path*`\NetBackup\logs` is defined).

EXAMPLES

List the storage units defined on the master server apricot, using the `-U` display option:

```
bpstulist -U -M apricot

Label:             redtest
Storage Unit Type: Disk
Host Connection:   apricot
Concurrent Jobs:   1
On Demand Only:    yes
Max MPX:           4
Path:              /usr/redtest
Max Fragment Size: 2000 MB

Label:             bluetest
Storage Unit Type: Media Manager
Host Connection:   apricot
Number of Drives:  6
On Demand Only:    yes
Max MPX/drive:     1
Density:           4mm - 4mm Cartridge
Robot Type/Number: TL4 / 0
Max Fragment Size: (unlimited)
```

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\config\storage_units`

SEE ALSO

`bpstuadd`, `bpstudel`, `bpsturep`

bpsturep

NAME

`bpsturep` - Replace selected NetBackup storage unit attributes

SYNOPSIS

install_path`\NetBackup\bin\Admincmd\bpsturep -label` *storage_unit_label* `[-host` *host_name*`] [-cj` *max_jobs*`] [-odo` *on_demand_only*`] [-mfs` *max_fragment_size*`] [-maxmpx` *mpx_factor*`] [{-path` *path_name*`} | {-density` *density_type* `[-rt` *robot_type* `-rn` *robot_number*`]}] [-nh` *NDMP_attach_host*`] [-verbose] [-M` *master_server*`, . . .]`

install_path`\NetBackup\bin\admincmd\bpsturep` *storage_unit_group* `[-addstu | -delstu] <`*storage_unit*`>`

DESCRIPTION

The `bpsturep` command modifies an existing NetBackup storage unit by replacing selected storage-unit or storage-unit-group attributes in the NetBackup catalog. The command line must include a label for the storage unit or a group name for the storage unit group. The label or group name is the only storage-unit attribute that `bpsturep` cannot modify.

Use the `bpsturep` command with care. The changes to the storage unit or storage unit group must be compatible with existing attributes. Make sure resulting attribute combinations are valid, especially for the following attributes:

robot_type

robot_number

`density`

max_fragment_size

`path`

NDMP_attach_host

The safest way to modify these attributes is to run `bpsturep` once for each attribute to be replaced.

`bpsturep` makes the changes by deleting the old storage unit and adding a new storage unit with the specified attribute changes. Therefore, if `bpsturep` specifies invalid options or an invalid combination of options, the storage unit may be deleted without being re-added. It is best to run `bpstulist` after `bpsturep` to determine whether the intended changes were actually applied.

Errors go to stderr. A log of the command's activity goes to the NetBackup admin log file for the current day.

This command requires administrator privileges.

See your NetBackup system administrator's guide for additional information on storage units.

OPTIONS

`-cj` *max_jobs*

The maximum number of concurrent jobs permitted for this storage unit. max_jobs is a non-negative integer. The appropriate value depends on your server's ability to comfortably run multiple backup processes and the available space on the storage media. Also, refer to the Maximum Jobs per Policy topic in your NetBackup system administrator's guide.

0 means that this storage unit will never be selected when a job is being scheduled. The default is 1.

`-density` *density_type*

If this option is present, the storage unit type is Media Manager. There is no default for this option. One of `-density` or `-path` must be on the command line, but not both. If the command line includes a robot type, the value for density should be consistent with the robot type.

Valid density types are:

`dlt` - DLT Cartridge

`dlt2` - DLT Cartridge alternate

`8mm` - 8mm Cartridge

`4mm` - 4mm Cartridge

`qscsi` - 1/4 Inch Cartridge

Note The following densities apply only to NetBackup DataCenter servers.

`hcart` - 1/2 Inch Cartridge

`hcart2` - 1/2 Inch Cartridge alternate

`dtf` - DTF Cartridge

`odiskwm` - Optical Disk Write-Many

`odiskwo` - Optical Disk Write-Once

`-host` *host_name*

Note NetBackup BusinesServer does not support remote media servers.

The NetBackup host to which the destination media is attached. The default is the hostname of the local system.

The host you select must be either your NetBackup master server or a media server (if you are configuring media servers). The host name must be the network name for the server as known by all NetBackup servers and clients.

If *host_name* is a valid network name and is not yet configured in NetBackup, the value *host_name* will be added to NetBackup's configuration as a media server. On UNIX, this shows up in `bp.conf`; on Windows, this shows up in the Configuration window for Servers. If *host_name* is not a valid network name, you must configure it manually.

`-label` *storage_unit_label*

The name of a storage unit. This is the storage unit whose attributes `bpsturep` replaces. This is a required option. The maximum length of a storage-unit label is 128 characters.

`-mfs` *max_fragment_size*

The maximum fragment size specifies, in megabytes, how large a fragment for a NetBackup image can be. For a Media Manager storage unit, this value is either zero (the fragment size is unlimited, meaning there is no fragmentation) or any integer greater than or equal to 50 megabytes (MB). The default value is 0.

For a Disk storage unit, this value ranges from 20 megabytes to 2000 megabytes (2 gigabytes). The default value is 2000 (2 gigabytes).

`-maxmpx` *mpx_factor*

The maximum multiplexing factor. Multiplexing sends concurrent, multiple backups from one or several clients to a single drive. Refer to the topic "Multiplexing (MPX)" in your NetBackup system administrator's guide.

The multiplexing factor can range from 1 to 32, where 1 means no multiplexing. A value greater than 1 means that NetBackup can create multiplexed images on the destination medium. Depending on the licensing of the local NetBackup installation, it may not be possible to assign multiplexing factors in the entire range 1..32.

The default is 1.

`-M` *master_server_*

A list of master servers. This is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-nh` *NDMP_attach_host*

Specifies the hostname of the NDMP server. If this option is present, the storage unit type is set to NDMP. The default is no NDMP server.

`-odo` *on_demand_only*

The *on-demand-only* flag controls whether the storage unit is used only for backups that explicitly request (demand) the storage unit:

To make the storage unit available only to policies or schedules that request it, set the flag to 1 (enabled).

To make the storage unit available to any policy or schedule, set the flag to 0 (disabled).

If the storage unit's type is Disk, the default is 1; NetBackup uses the storage unit only when explicitly requested. Otherwise, the default is 0.

`-path` *path_name*

The path to a disk filesystem, expressed as an absolute pathname. This is the data storage area for this storage unit. When this option is present, the storage unit type is `Disk`. There is no default for this option. One of `-density` or `-path` must be on the command line, but not both.

In general when this option is used, it is recommended that the *on-demand-only* flag be enabled (see `-odo`). Otherwise, any NetBackup policy that does not require a specific storage unit has the opportunity to fill the disk filesystem *path_name*. This can cause serious system problems. For instance, if the system swap area happens to be on the same filesystem, new processes may fail.

`-rn` *robot_number*

The robot number for this storage unit. The robot number must be greater than or equal to 0. The robot number can be obtained from the Media Manager device configuration. The Media Manager system administrator's guide discusses the rules concerning the use of this number. This option is ignored unless the `-rt` option is present. There is no default for this option.

`-rt` *robot_type*

The robot type for this storage unit. For non-robotic (standalone) devices select `NONE` or omit this option. The default value is `NONE` (Not Robotic). The value for density should be consistent with the robot type

If this option is set to any value other than `NONE`, the `-rn` option is required.

Available robot type codes are:

`NONE` - Not Robotic

`TLD` - Tape Library DLT

`TSD` - Tape Stacker DLT

ACS - Automated Cartridge System

TS8 - Tape Stacker 8MM

TL8 - Tape Library 8MM

ODL - Optical Disk Library

TSH - Tape Stacker Half-inch

TLH - Tape Library Half-inch

TLM - Tape Library Multimedia

LMF - Library Management Facility

RSM - Removable Storage Manager

-verbose Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory *install_path*\NetBackup\Logs is defined).

-group *storage_unit_group*
The name of a storage unit group. This is the storage unit whose members bpsturep adds or deletes. Use -addstu *storage_unit* to add storage units to the group. Use -delstu *storage_unit* to remove storage units from the group.

EXAMPLES

Change the path for a disk storage unit, mkbunit. The path is changed from C:\tmp\mkbunit to C:\tmp\mkbunit2:

```
bpstulist
mkbunit 0 beaver 0 -1 -1 1 0 C:\tmp\mkbunit 1 1 2000 *NULL*
bpsturep -label mkbunit -path C:\tmp\mkbunit2
bpstulist
mkbunit 0 beaver 0 -1 -1 1 0 C:\tmp\mkbunit2 1 1 2000 *NULL*
```

FILES

install_path\NetBackup\logs\admin*

install_path\NetBackup\db\config\storage_units

SEE ALSO

bpstuadd, bpstudel, bpstulist

bpverify

NAME

`bpverify` - Verify the backups created by NetBackup

SYNOPSIS

install_path`\NetBackup\bin\admincmd\bpverify [-l] [-p] [-pb] [-v] [-local] [-client` *name*`] [-st` *sched_type*`] [-sl` *sched_label*`] [-L` *output_file* `[-en]] [-policy` *name*`] [-s` *mm/dd/yyyy hh:mm:ss*`] [-e` *mm/dd/yyyy hh:mm:ss*`] [-M` *master_server*`] [-Bidfile` *file_name*`] [-backup_copy` *backup_copy_value*`] [-pt` *policy_type*`] [-hoursago` *hours*`] [[-cn` *copy number*`] | [-primary]][-backupid` *backup_id*`] [-id` *media_id* | *path*`]`

DESCRIPTION

`bpverify` verifies the contents of one or more backups by reading the backup volume and comparing its contents to the NetBackup catalog. This operation does not compare the data on the volume with the contents of the client disk. However, it does read each block in the image, thus verifying that the volume is readable. NetBackup verifies only one backup at a time and tries to minimize media mounts and positioning time.

If either `-Bidfile` or `-backupid` is specified, `bpverify` uses this option as the sole criterion for selecting the set of backups it will verify. If the command line does not contain `-Bidfile` or `-backupid`, then `bpverify` selects the backups that satisfy all the selection options. For instance, if the command line looks like

```
bpverify -pt Standard -hoursago 10
```

then `bpverify` verifies the set of backups with policy type `Standard` that have been run in the past 10 hours.

If `-p` or `-pb` is specified, `bpverify` previews the set of backups that meet the selection criteria. In this case, `bpverify` displays the backup IDs, but does not perform the verification.

`bpverify` sends its error messages to `stderr`. `bpverify` sends a log of its activity to the NetBackup admin log file for the current day (found in .

This command requires administrator privileges.

OPTIONS

`-Bidfile` *file_name*

file_name specifies a file that contains a list of backup IDs to be verified. The file contains one backup ID per line. If this option is specified, other selection criteria are ignored. The default is no file of backup Ids, meaning any backup can be verified.

`-backup_copy` *backup_copy_value*

Where *backup_copy_value* is 3, indicates that the import is for Fastrax.

`-backupid` *backup_id*

Specifies the backup ID of a single backup to verify. This option takes precedence over any other selection criteria except `-Bidfile`. The default is any backup.

`-policy` *name*

Search for backups to verify in the specified policy. The default is any policy.

`-client` *name*

Specifies the name of the client that produced the original backup. The default is any client.

`-cn` *copy_number*|`-primary`

Determines the copy number of the backup ID to verify. Valid values are 1 through the setting indicated by the `bpconfig -max_copies` setting, up to 10. The default is 1.

`-primary` indicates that the primary copy should be verified rather than the copy.

`-pt` *policy_type*

Specifies the policy type for selecting backups to verify. The default is any policy type.

The valid policy types are the following:

`AFS`

`Apollo-wbak`

`DataStore`

`DataTools-SQL-BackTrack`

`DB2`

`FlashBackup`

`Informix-On-BAR`

`Lotus-Notes`

`MS-Exchange-Server`

`MS-SQL-Server`

MS-Windows-NT

NCR-Teradata

NDMP

NetWare

Oracle

OS/2

SAP

Split-Mirror

Standard

Sybase

`-e` *mm/dd/yyyy* [*hh*[:*mm*[:*ss*]]]

Specifies the end of the time range for selecting backups to verify. The `-s` option or the `-hoursago` option specifies the start of the range.

The date and time format depend on the user's locale.
The default ending time is the current date and time.

`-help` Prints a command line usage message when `-help` is the only option on the command line.

`-hoursago` *hours*

Specifies the number of hours before the current time to search for backups. This is equivalent to specifying a start time (`-s`) of the current time minus hours. Do not use both this option and the `-s` option.

Hours is a non-negative integer. The default starting time is 24 hours ago.

`-id` *media_id* | *path*

Search the image catalog for backups to verify that are on this media ID or pathname. If a backup has some fragments on this media ID and some fragments on another media ID, NetBackup skips verifying that backup. For images stored on disk rather than removable media, specify an absolute pathname instead of *media_id*. The default is any media ID or pathname.

`-L` *output_file* [`-en`]

Specifies the name of a file in which to write progress information. The default is to not use a progress file, in which case the progress information is written to `stderr`. For additional information, see DISPLAY FORMATS later in this command description.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-l` Specifies that the list type is long, causing `bpverify` to write additional information to the progress log. The default list type is short. For additional information, see DISPLAY FORMATS later in this command description.

`-local` When `bpverify` is initiated from a host other than master server and the `-local` option is *not* used (default), `bpverify` starts a remote copy of the command on the master server.

The remote copy allows the command to be terminated from the **Activity Monitor**.

Use the `-local` option to prevent the creation of a remote copy on the master server and to run the `bpverify` only from the host where it was initiated.

If the `-local` option is used, `bpverify` cannot be canceled from the **Activity Monitor**.

`-M` *master_server*
Specifies the master server that provides the bpverify image data. The master server must allow access by the system issuing the `bpverify` command. The default is the master server for the system where `bpverify` is entered:

For NetBackup BusinesServer:

The default is always the master server where the command is entered.

For NetBackup DataCenter:

If the command is entered on a master server, then that server is the default.

If the command is entered on a remote media server, then the master for that media server is the default.

`-p` Previews the verification, but does not perform the verification. For additional information, see DISPLAY FORMATS later in this command description.

`-pb` Previews the verification but does not perform the verification. This is similar to the `-p` option, but `-pb` does not display information about the individual backups. For additional information, see DISPLAY FORMATS later in this command description.

`-s` *mm/dd/yyyy* [*hh*[:*mm*[:*ss*]]]
Specifies the start of the range of dates and times that include all backups to verify. The `-e` option specifies the end of the range. The date and time format depend on the user's locale. The default is 24 hours ago.

`-sl` *sched_label*
Search for backups to verify that were created by the specified schedule. The default is all schedules.

`-st` *sched_type*

Search for backups to verify that were created by the specified schedule type. The default is any schedule type.

Valid values are:

`FULL` (full backup)

`INCR` (differential-incremental backup)

`CINC` (cumulative-incremental backup)

`UBAK` (user backup)

`UARC` (user archive)

`NOT_ARCHIVE` (all backups except user archive)

`-v` Selects verbose mode. When `-v` is specified, the debug and progress logs include more information. The default is not verbose.

DISPLAY FORMATS

PREVIEW DISPLAYS:

`bpverify` runs a preview by searching for backups and displaying them. `bpverify` does not actually verify the backups.

- The `-p` display lists backup IDs that meet the criteria set by the bpverify command-line options. The `-p` display is ordered by volume. For each volume containing a selected backup, the media ID and server are displayed, followed by the selected backup Ids that reside on that volume
- The `-pb` display is a brief version of the `-p` display. It lists the media ID and server for each volume that contains backups that meet the selection criteria.

VERIFICATION DISPLAYS:

`bpverify` creates these displays as it verifies images. If the `bpverify` command line contains no option to set the list format, the display format is short. If the command line contains `-l`, the display format is long. If the command line contains both `-l` and `-L`, `bpverify` creates a file containing the progress log.

The verification display is ordered by volume.

- In long format, `bpverify` displays the following information for each selected backup ID:

  Policy, schedule, backup ID, media ID or path, and creation time

  Files backed up

  Any problems that `bpverify` detects while verifying the image

  Whether the image verification is successful or not
- In short format, `bpverify` omits listing the files backed up.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting. The examples in this command description are for a locale setting of C.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the usage. The following is part of the `bpverify` usage statement output that shows the `-s` and `-e` options:

```
[-s mm/dd/yy hh:mm:ss] [-e mm/dd/yy hh:mm:ss]
```

EXAMPLES

- Example 1

  The following example verifies the backups run in the past 36 hours:

```
  bpverify -hoursago 36
  Verify started Thu Feb  3 11:30:29 2001
  INF - Verifying policy mkb_policy, schedule Full
(plum_0949536546), path /tmp/mkbunit, created 02/02/01 18:09:06.
INF - Verify of policy mkb_policy, schedule Full
(plum_0949536546) was successful.
INF - Status = successfully verified 1 of 1 images.
```

- Example 2

  The following example compares the two preview displays, `-p` and `-pb`:

```
bpverify -p -hoursago 2000
Media id = A00002  Server = plum
Bid = plum_0949616279  Kbytes = 32800  Filenum = 1  Fragment = 1
Bid = guava_0949681647  Kbytes = 12191  Filenum = 2  Fragment = 1
Bid = guava_0949683298  Kbytes = 161  Filenum = 3  Fragment = 1
Bid = guava_0949683671  Kbytes = 11417  Filenum = 4  Fragment = 1
Bid = guava_0949684009  Kbytes = 11611  Filenum = 5  Fragment = 1
Bid = guava_0949684276  Kbytes = 806  Filenum = 6  Fragment = 1
Bid = guava_0949688704  Kbytes = 9869  Filenum = 7  Fragment = 1
Bid = guava_0949688813  Kbytes = 9869  Filenum = 8  Fragment = 1
Bid = guava_0949949336  Kbytes = 10256  Filenum = 9  Fragment = 1
Bid = plum_0949949337  Kbytes = 6080  Filenum = 9  Fragment = 1
Bid = plum_0949949337  Kbytes = 4176  Filenum = 10  Fragment = 2
Bid = guava_0949949686  Kbytes = 10256  Filenum = 11  Fragment = 1
Bid = plum_0949949687  Kbytes = 5440  Filenum = 11  Fragment = 1
Bid = plum_0949949687  Kbytes = 4816  Filenum = 12  Fragment = 2
Bid = guava_0949949902  Kbytes = 10256  Filenum = 13  Fragment = 1
Bid = plum_0949949901  Kbytes = 8832  Filenum = 13  Fragment = 1
Bid = plum_0949949901  Kbytes = 1424  Filenum = 14  Fragment = 2
Bid = plum_0950053561  Kbytes = 10256  Filenum = 15  Fragment = 1
```

```
Media id = 400032  Server = plum
Bid = toaster2_0950199621 Kbytes = 298180  Filenum = 1  Fragment = 1
Bid = toaster2_0950199901 Kbytes = 298180  Filenum = 3  Fragment = 1

bpverify -pb -hoursago 200
Media id = A00002  Server = plum
Media id = 400032  Server = plum
```

EXIT STATUS

An exit status of 0 means that the command ran successfully.

Any exit status other than 0 means that an error occurred.

If administrative logging is enabled, the exit status is logged in the administrative daily log under the directory *install_path*`\NetBackup\logs\admin` in the form:

`bpverify: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

install_path`\NetBackup\logs\admin\*`

install_path`\NetBackup\db\error\*`

install_path`\NetBackup\db\images\*`

cat_convert

NAME

`cat_convert` - NetBackup catalog format conversion utility

SYNOPSIS

install_path`\NetBackup\bin\cat_convert.exe [ -o [ -a2b | -b2a ] -s -v]` *source_file_directory* [*target_file_directory*]

DESCRIPTION

`cat_convert` converts NetBackup catalog `.f` files between version 3.4, 4.0v or 4.5 ASCII format and 4.5 binary format. `cat_convert` automatically detects the soure catalog file format and converts it to the other format.

This command requires administrator privileges.

OPTIONS

`-o`	Overwrite original catalog file content with the new, converting format. `-o` cannot be used with *target_file_directory*.
`-a2b`	Convert NetBackup 3.4, 4.0V, 4.5 ASCII format catalog `.f` file(s) to NetBackup 4.5 binary format `.f` file(s). Do not use `-a2b` with `-b2a`.
`-b2a`	Convert the NetBackup 4.5 binary format catalog `.f` file(s) to NetBackup 4.5 ASCII format `.f` file(s). Do not use `-b2a` with `-a2b`.
`-s`	Show statistic information to the console window.
`-v`	Show current progress information.

Specify either a single source file or an entire directory to convert:

- In order to specify a target file, the source must be a file.
- In order to specify a target directory, the source must be a directory.

  If the source is a directory, you must use `-a2b` or `-b2a`.

  The new files created by the conversion are converted to the specified format and the original file names are used in the target directory.

If the target file or directory is not specified when converting source files, the new files created by the conversion process will have a suffix appended (`_bin.f` or `_ascii.f`).

If the `catalog .f` file size is more than 4 megabytes, the binary catalog leaves output files separate and puts them in the `catstore` directory.

EXAMPLES

- Example 1

  Consider the following command:

  ```
  cat_convert abc.f
  ```

  If *abc.f* is in ASCII format, the *target_file_path* will be `abc_bin.f`.

  If *abc.f* is in binary format, the *target_file_path* will be `abc_ascii.f`.

- Example 2

  Consider the following command:

  ```
  cat_convert abc.f  /usr/tmp/abc1.f
  ```

  `abc.f` will be converted to the other format and copied to `/usr/tmp/abc1.f`.

- Example 3

  Consider the following command:

  ```
  cat_convert -a2b /home/john/catalog
  ```

  Every ASCII `.f` file in `/home/john/catalog` will be converted to the NetBackup 4.5 binary format with new file name `*_bin.f`.

- Example 4

  Consider the following command:

  ```
  cat_convert -b2a /home/john/catalog /home/john/catalog_ascii
  ```

  Every NetBackup 4.5 binary `.f` file in `/home/john/catalog` will be converted to NetBackup 4.5 ASCII format and copied to `/home/john/catalog_ascii`.

- Example 5

  Consider the following command:

  ```
  cat_convert -o abc.f
  ```

  The content of `abc.f` will be converted to the other file format.

- Example 6

  Consider the following command:

  ```
  cat_convert -o -b2a /home/john/catalog
  ```

  The content of every NetBackup 4.5 binary `.f` file under `/home/john/catalog` will be converted to NetBackup 4.5 ASCII format.

nbdbsetport

NAME

`nbdbsetport` - Set TCP/IP port used by the nbdbd database service

SYNOPSIS

install_path`\NetBackup\bin\admincmd nbdbsetport -get`

install_path`\NetBackup\bin\admincmd nbdbsetport -set` *port_number*

DESCRIPTION

When the nbdbd database service is initially installed, the port number for the nbdbd database service is set to 13784. The default port is adequate in most cases.

If this port number is already being used by another service on your machine, the nbdbd database service will not run until the port is changed using `nbdbsetport -set` *port_number*

OPTIONS

`-get` Returns the TCP/IP port numbercurrent being used by the nbdbd service.

`-set` *port_number*
Set the nbdbd service TCP/IP port number to *port_number*. The new port number will take effect the next time NetBackup is restarted.

nbdbsetpw

NAME

`nbdbsetpw` - Modify passwords used by the nbdbd database service

SYNOPSIS

install_path`\NetBackup\bin\admincmd nbdbsetpw [-reset]`

DESCRIPTION

When the nbdbd database service is initially installed, it has two password: one for the `root` user and one for `nbu` user. If you wish, you can use `nbdbsetpw` to modify these passwords.

When invoked, `nbdbsetpw` prompts for new passwords for the `root` user and `nbu` user.

NetBackup stores encrypted nbdbd passwords if private data files. NetBackup must know the passwords in order to change them. If for some reason these encrypted passwords are not in sync with the passwords in the nbdbd database authorization tables, you must reset the passwords to the default by running `nbdbsetpw -reset`. Resetting the passwords should not be necessary during normal operations. The `nbdbsetpw` command will inform you if reset is necessary.

If the reset fails, you should contact VERITAS Technical Support.

OPTIONS

`-reset` Sets passwords to default. `nbdbsetpw` logs the fact that the nbdbd passwords have been changed.

vopied

NAME

`vopied` - Daemon to provide VERITAS One-time Password user authentication

SYNOPSIS

install_path`\NetBackup\bin\vopied [-standalone] [-debug] [-portnum` number`] [-max_time` *seconds*`] [-log_dir` *path*`] [-severity` *mask*`]`

DESCRIPTION

This program is available on Windows and UNIX NetBackup clients. It accepts connections from remote NetBackup servers and clients that are attempting to verify the identity of requests from the local NetBackup system. The authentication method is VERITAS One-time Password (vopie). Normally, `vopied` is started by the NetBackup Client service on Windows and `inetd` on UNIX.

When you install NetBackup on a Windows client or UNIX client, the installation process adds entries for `vopied` to `C:\WINNT\system32\drivers\etc\services` on Windows and `/etc/services` and `/etc/inetd.conf` on UNIX.

The `services` entry looks like this:

```
vopied  13783/tcp       vopied
```

The `inetd.conf` entry on UNIX looks like this:

```
vopied  stream  tcp     nowait  root    /usr/openv/bin/vopied vopied
```

OPTIONS

`-standalone`
: Available only on UNIX clients and specifies that `vopied` will run continuously rather than being started by `inetd`.

`-debug`
: Available only on UNIX clients and implies `-standalone` (that is, `vopied` runs continuously). This option prevents `vopied` from forking and does not disconnect it from standard input, output, and error.

`-portnum` *number*
: Available only on UNIX clients and implies `-standalone` (that is, `vopied` runs continuously). Specifies the port number where `vopied` listens for requests. The default is the `vopied` entry in:

  `/etc/services`

`-max_time` *seconds*

Specifies a time out value for network connections. The default is 60 seconds.

`-log_dir` *path*

Specifies the directory where the `vopied` log directory resides. The default is:

install_path`\NetBackup\logs` (Windows)

`/usr/openv/logs` (UNIX)

To enable logging, create a `vopied` directory in the *path* directory before starting `vopied`. For example:

install_path`\NetBackup\logs\vopied`

`-severity` *mask*

Specifies the type of messages to be logged. *mask* is the sum of zero or more of these values:

`1` Unknown

`2` Debug

`4` Information

`8` Warning

`16` Error

`32` Critical

The default is 48 decimal (0x30 hexadecimal), which specifies critical and error.

SEE ALSO

`bpauthsync`, `vopie_util`

vopie_util

NAME

`vopie_util` - Manage local vopie authentication files

SYNOPSIS

install_path`\NetBackup\bin\vopie_util [-log_dir` *path*`] [-severity mask] [-debug] [-local_name` *name*`] [-always_write] [-hashed | -unhashed]` *remote_name* [*sequence seed hash*]

DESCRIPTION

The `vopie_util` program is available on Windows and UNIX NetBackup servers and clients. It updates the hashed (public) and unhashed (secret) key files for the vopie authentication method on the local system. Typically, `vopie_util` is used to synchronize the vopie key files between two systems.

OPTIONS

`-log_dir` *path*

Specifies the directory where the `vopie_util` log directory resides. The default is:

install_path`\NetBackup\logs` (Windows)

`/usr/openv/logs` (UNIX)

To enable logging, create a `vopie_util` directory in the *path* directory before starting `vopie_util`. For example:

`C:\VERITAS\NetBackup\logs\ vopie_util`

`-severity` *mask*

Specifies the type of messages to be logged. *mask* is the sum of zero or more of these values:

`1` Unknown

`2` Debug

`4` Information

`8` Warning

`16` Error

32 Critical

The default is 48 decimal (0x30 hexadecimal or 060 octal), which specifies critical and error.

`-debug`

Specifies that additional information is logged to standard error.

`-local_name` *name*
: Specifies the name of the local system. The default is the network host name of the system. We recommend that this name match the NetBackup client name for the system.

`-always_write`
: Always update the file even if it already exists. The default is to not overwrite existing files.

`-hashed`
: Updates the hashed (public) key file. This file contains the challenges that this system presents to other systems during authentication. If the *sequence*, *seed*, and *hash* options described below are not specified, the hashed-key file data matches any secret key.

`-unhashed`
: Updates the unhashed (secret) key file. A secret key is randomly generated and written to the unhashed key file. The unhashed file contains the responses that the system returns when challenged by another system.

  The corresponding hashed-key file data is displayed after running the command with this option.

remote_name
: Specifies the name of the remote system with which this one is being synchonized.

sequence seed hash
: Can be used with the `-hashed` option and specifies data that is written in the hashed (public) key file:

  sequence is a decimal number between 10 and 499.

  seed is a 6 to 20 character string.

  hash is a 16 digit hexadecimal number.

EXAMPLES

◆ Example 1

In this example, the vopie key files are set up so the first connection between systems red and blue is not fully authenticated. After the connection, the key files are updated so full authentication is required. This is the easiest way to synchronize the key files but it leaves a small window of insecurity.

1. On system red:

a. Create a secret key file on red by running the following command:

```
vopie_util -local_name red -unhashed blue
```

The public key (hashed) file information for red is displayed:

```
red 0167 jp0167 0aa47eae2d86231d
```

This information can be ignored in this example.

b. Create a public key file on red that will match any secret key on blue:

```
vopie_util -local_name red -hashed blue
```

2. On system blue:

a. Create a secret-key file on blue by running the following command:

```
vopie_util -local_name blue -unhashed red
```

The public key (hashed) file information for blue is displayed:

```
blue 0431 gw3251 0aa47eae2d86231d
```

This information can be ignored in this example.

b. Create a public key file on blue that will match any secret key on red by running the following command:

```
vopie_util -local_name blue -hashed red
```

◆ Example 2

In this example, the vopie key files on systems green and yellow are synchronized. Full authentication is required immediately. This is a more secure method than in example 1.

1. On system green, create a secret key file on green by running the following command:

```
vopie_util -local_name green -unhashed yellow
```

The public key (hashed) file information for green is displayed:

```
green 0209 fz9365 f852019bde05e92f
```

yellow uses this key when it issues challenges.

2. On system yellow:

a. Create a public key file on yellow that matches the secret key file on green by running the following (all on one line):

```
vopie_util -local_name yellow -hashed green 0209 fz9365
f852019bde05e92f
```

b. Create a secret key file on yellow by running the following by command:

```
vopie_util -local_name yellow -unhashed green
```

The public key (hashed) file information for yellow is displayed:

```
yellow 0468 yq0860 82723984b43bf474
```

green uses this key when it issues challenges.

3. On system green, create a public key file on green that matches the secret key file on yellow by running the following (all on one line):

```
vopie_util -local_name green -hashed yellow 0468 yq0860
82723984b43bf474
```

SEE ALSO

bpauthsync, vopied

Reference Topics B

The topics in this appendix provide additional information about various aspects of NetBackup configuration and management.

- Rules for Using Host Names in NetBackup
- Factors Affecting Backup Time
- Determining NetBackup Transfer Rate
- Guidelines for Setting Retention Periods
- Guidelines for Setting Backup Frequency
- Determining Backup Media Requirements
- How NetBackup Builds Its Automatic-Backup Worklist
- Incremental Backups Overview
- Storage Management Overview
- Media Management Concepts
- Planning Worksheets

Rules for Using Host Names in NetBackup

NetBackup uses host names to identify, communicate with, and initiate processes on NetBackup client and server computers. The correct use of host names during configuration is essential to the proper operation of NetBackup. (See "Dynamic Host Name and IP Addressing" on page 408.)

NetBackup uses TCP/IP host names to connect to NetBackup servers and clients. NetBackup validates its connections by performing a reverse host name lookup. That is, NetBackup determines the IP address of a connection and then uses the IP address to look up the host name with `gethostbyaddr()`. For this to work reliably, the host name and address resolution must be set up correctly in DNS, WINS, or the local `%Systemroot%\system32\drivers\etc\hosts` file (if necessary).

Note Sometimes placing the system host name and IP address in the `%Systemroot%\system32\drivers\etc\hosts` file accelerates name lookups.

Qualifying Host Names

A major consideration when configuring host names is the extent to which you qualify them. In many cases, using a computer's short host name is adequate. If the network environment is or will eventually be multi-domain, qualify host names to the extent that servers and clients can identify each other in a multi-domain environment.

For example, use a name such as `mercury.bdev.null.com` or `mercury.bdev` rather than just `mercury`.

How NetBackup Uses Host Names

The following discussions explain where NetBackup stores host names and how it uses them. These discussions also mention factors to consider when choosing host names.

Note Do not change the host name of a NetBackup server. This practice is not recommended because it can be necessary to import all previously used media to the server before you can use it under the new host name.

Policy Configuration

The host name that you specify for a client when you add it to a policy is called the client's *configured name*, and is the client's host name as it appears in the NetBackup configuration.

The server uses the client's configured name to connect to the client and start the processes that satisfy client requests. When adding clients to a policy always use host names that are qualified to the extent that all NetBackup servers can connect to the clients.

When a client makes a user backup, archive, or restore request to the NetBackup server, the server uses the peername of the client (identified from its TCP connection) to determine the client's configured name.

If you add a client to more than one policy, always use the same configured name in all cases. Otherwise, the client cannot view all files backed up on its behalf and file restores are complicated because both user and administrator action is required to restore from some of the backups.

Image Catalog

A subdirectory in the image catalog is created for a client when a backup is first created for that client. The subdirectory's name is the client's configured name.

Every backup for a client has a record in this subdirectory. Each of these backup records contains the host name of the server on which the backup was written.

Error Catalog

NetBackup uses entries in the error catalog for generating reports. These entries contain the host name of the server generating the entry and the client's configured name, if applicable. The server host name is normally the server's short host name. (For example, shark instead of shark.null.com.)

Scheduler

The NetBackup scheduler uses the server host name associated with the storage units to start a process on the server. When you specify this host name, always qualify it to the extent necessary for the master server to make a connection to the server that has the storage units. Normally, a short host name is adequate. (For example, shark instead of shark.null.com.)

Special Considerations For Domain Name Service (DNS)

In some requests to the master server, client software sends the name that it obtains through its `gethostname` library function. If this (possibly unqualified) name is unknown to the Domain Name Service (DNS) on the master server, it is possible that the master server cannot reply to client requests.

Whether this situation exists, depends on how the client and the server are configured. If `gethostname` on the client returns host names that are not qualified to the extent that DNS on the master server can resolve them, you will encounter problems.

A possible solution is to reconfigure the client or the master server DNS hosts file. However, because this is not always desirable, NetBackup allows you to create a special file on the master server

install_path`\NetBackup\db\altnames\host.xlate`

in order to force the desired translation of NetBackup client host names.

Each line in the `host.xlate` file has three elements, a numeric key and two host names. Each line is left-justified, and each element of the line is separated by a space character.

key hostname_from_ client client_as_known_by_server

Where

- *key* is a numeric value used by NetBackup to specify the cases where translation is to be done. Currently this value must always be 0, indicating a configured name translation.
- *hostname_from_client* is the value to translate. This must correspond to the name obtained by the client's `gethostname` and be sent to the server in the request.
- *client_as_known_by_server* is the name to substitute for *hostname_from_client* when responding to requests. This name must be the name configured in the NetBackup configuration on the master server and must also be known to the master server's network services.

For example, the line

```
0 danr danr.eng.aaa.com
```

specifies that when the master server receives a request for a configured client name (numeric key 0), the name danr is always replaced by the name danr.eng.aaa.com. This resolves the problem mentioned above, assuming that:

- The client's `gethostname` returned danr.
- The master server's network services `gethostbyname` library function did not recognize the name danr.
- The client was configured and named in the NetBackup configuration as danr.eng.aaa.com and this name is also known to network services on the master server.

Factors Affecting Backup Time

The time NetBackup requires to complete a backup is an important factor in scheduling. This is particularly true for sites that deal with large amounts of data. For example, the total backup time can exceed the time allotted to complete backups and interfere with normal network operations. Longer backup times also increase the possibility of a problem disrupting the backup. The time to back up files can also give you an indication of how long it takes to recover them.

The following formula shows the major factors that affect backup time:

$$\text{Backup Time} = \frac{\text{Total data}}{\text{Transfer rate}} \times \text{Compression Factor} + \text{Device Delays (optional)}$$

Total data

The amount of data you must back up depends on the size of the files for each client in the policy you are backing up. It also depends on whether it is a full or incremental backup.

- Full backups involve all the data. Therefore, a full backup usually takes longer than an incremental.
- Differential-incremental backups include only the data that has changed since the last full or intervening incremental.
- Cumulative-incremental backups include all the data that has changed since the last full backup.

With both differential- and cumulative-incremental backups, the amount of data in the backups, depends on the frequency with which files change. If a large number of files change frequently, incrementals are larger.

Transfer rate

Transfer rate depends on factors such as:

- Speed of the backup device. For example, sending backups to a tape having a maximum transfer rate of 400 kilobytes per second normally takes less time than to a tape that transfers at only 200 kilobytes per second (assuming other factors allow taking advantage of the faster transfer rate).
- Available network bandwidth. The theoretical network bandwidth is about 10 megabits per second for Ethernet and 100 megabits per second for FDDI and 100 base T. The available bandwidth, however, is less than this and depends on how much other network traffic is present. For example, multiple backups occurring on the same network compete for bandwidth.

- Speed with which the client can process the data. This varies with the hardware platform and depends on the other applications running on the platform. File size is also an important factor. Clients can process larger files faster than smaller ones. You can back up 20 files that are 1 megabyte in size faster than 20,000 files that are 1 kilobyte in size.
- Speed with which the server can process the data. Like client speed, server speed also varies with the hardware platform and depends on the other applications running on the platform. The number of concurrent backups being performed also affects server speed.

See “Determining NetBackup Transfer Rate” on page 634 for methods to compute the transfer rate for your clients.

Device delays

Device delays are due to factors such as the device being busy, loading the media, and finding the place on the media at which to start writing the backup. These delays depend on the devices and computing environments and can vary widely.

Determining NetBackup Transfer Rate

You can calculate three different variations of the backup transfer rate by using the data provided in NetBackup reports. The three rates and the methods for calculating them are:

- Network-Transfer Rate
- Network-Transfer Plus End-of-Backup-Processing Rate
- Total-Transfer Rate

You can also use the Microsoft Windows performance monitor to display the NetBackup transfer rate. (See “Using the Performance Monitor” on page 636.)

Network-Transfer Rate

The network-transfer rate considers only the time required to transfer data over the network from client to server. This rate ignores the following:

- Time to load and position media before a backup.
- Time to gracefully close the tape file and write an additional NetBackup information record to the tape.

The network-transfer rate is the one provided in the All Log Entries report.

Network-Transfer Plus End-of-Backup-Processing Rate

This rate ignores the time it takes to load and position media before a backup, but includes the end-of-backup processing that is ignored in the network transfer rate. To determine this rate, use the All Log Entries report and calculate the time from the message:

```
begin writing backup id xxx
```

to the message

```
successfully wrote backup id xxx
```

Then, divide this time (in seconds) into the total bytes transferred (as recorded in the All Log Entries report) to calculate the transfer rate.

Total-Transfer Rate

This transfer rate includes the time for loading and positioning the media as well as the end-of-backup processing. Using the List Client Backups report, calculate the transfer rate by dividing Kilobytes by Elapsed Time (converted to seconds).

Examples

Assume that the reports provide the following data.

All Log Entries Report

```
TIME               SERVER/CLIENT   TEXT
04/28/94 23:10:37 windows giskard begin writing backup
                  id giskard_0767592458, fragment 1 to
                  media id TL8033 on device 1 . . .
04/29/94 00:35:07 windows giskard successfully wrote
                  backup id giskard_0767592458,
                  fragment 1, 1161824 Kbytes at
                  230.325 Kbytes/sec
```

List Client Backups Report

```
Client:                     giskard
Backup ID:                  giskard_0767592458
Policy:                      production_servers
Client Type:                Standard
Sched Label:                testing_add_files
Schedule Type:              Full
Backup Retention Level:     one week (0)
Backup Time:                04/28/94 23:07:38
Elapsed Time:               001:27:32
Expiration Time:            05/05/94 23:07:38
```

```
Compressed:                 no
Kilobytes:                  1161824
Number of Files:            78210
```

Using the backup data from the example reports above, you get the following three rates:

Network Transfer Rate

1161824 Kbytes at 230.325 Kbytes per second

Network Transfer Plus End of Backup Processing Rate

23:10:30 - 00:35:07 = 01:24:30 = 5070 seconds

1161824 Kbytes / 5070 = 229.157 Kbytes per second

Total Transfer Rate

Elapsed time = 01:27:32 = 5252 seconds

1161824 Kbytes / 5252 = 221.216 Kbytes per second

Using the Performance Monitor

To use the Performance Monitor on Microsoft Windows NT or the System Monitor on Windows 2000, see the help for your system. NetBackup adds the NetBackup Disk / Tape performance object to the list of objects monitored by the performance monitor. Four counters are available for the NetBackup Disk / Tape performance object:

- Disk / Tape Read Bytes (GB)
- Disk / Tape Read Bytes / sec (KB)
- Disk / Tape Write Bytes (GB)
- Disk / Tape Write Bytes / sec (KB)

The NetBackup performance object supports *instances* in the Performance Monitor. The instances can be drive names, in the case of tape drives, or absolute paths in the case of disks, to which NetBackup is writing, or from which NetBackup is reading.

The Performance Monitor displays object instances when NetBackup begins to read or write from the disk or tape. The read or write counters are updated depending on the type of NetBackup operation performed. The object instance is removed from the list once the NetBackup operation is completed.

If the performance monitoring is done either locally or remotely during a NetBackup read or write operation, the object instance continues to exist after NetBackup operation is completed. In this case, the object instance is removed when performance monitoring is stopped.

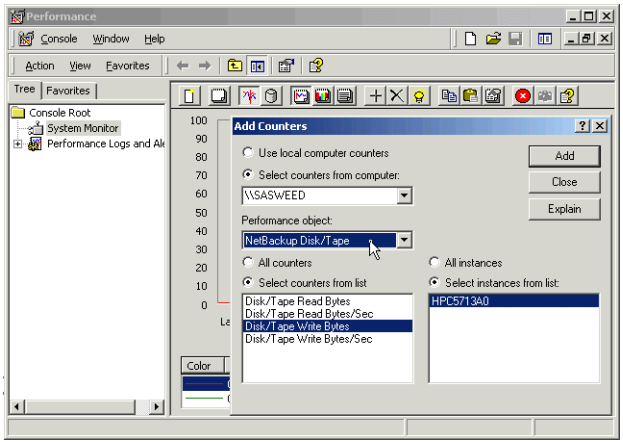
When remotely monitoring NetBackup counters on NT, the initiating computer attaches to the target computer's WinLogon process through RPC, thereby locking the object instances. Thus, the object instances remain until the system is rebooted.

▼ To use the performance monitor

1. Start the performance monitor by selecting **Start** > **Run**.

2. Type **`perfmon`** in the Run dialog, then press **OK**. The Performance Monitor dialog appears.

3. Click the plus sign (+) to add a counter to the display. Select **Netbackup Disk/Tape** from the **Perfomance objects** drop-down list.



4. Select the counter to display from the list of counters.

5. Select one or more object instances from the list of instances. Instances are displayed when NetBackup begins to read or write from the disk or tape drives.

6. Click **Add**.

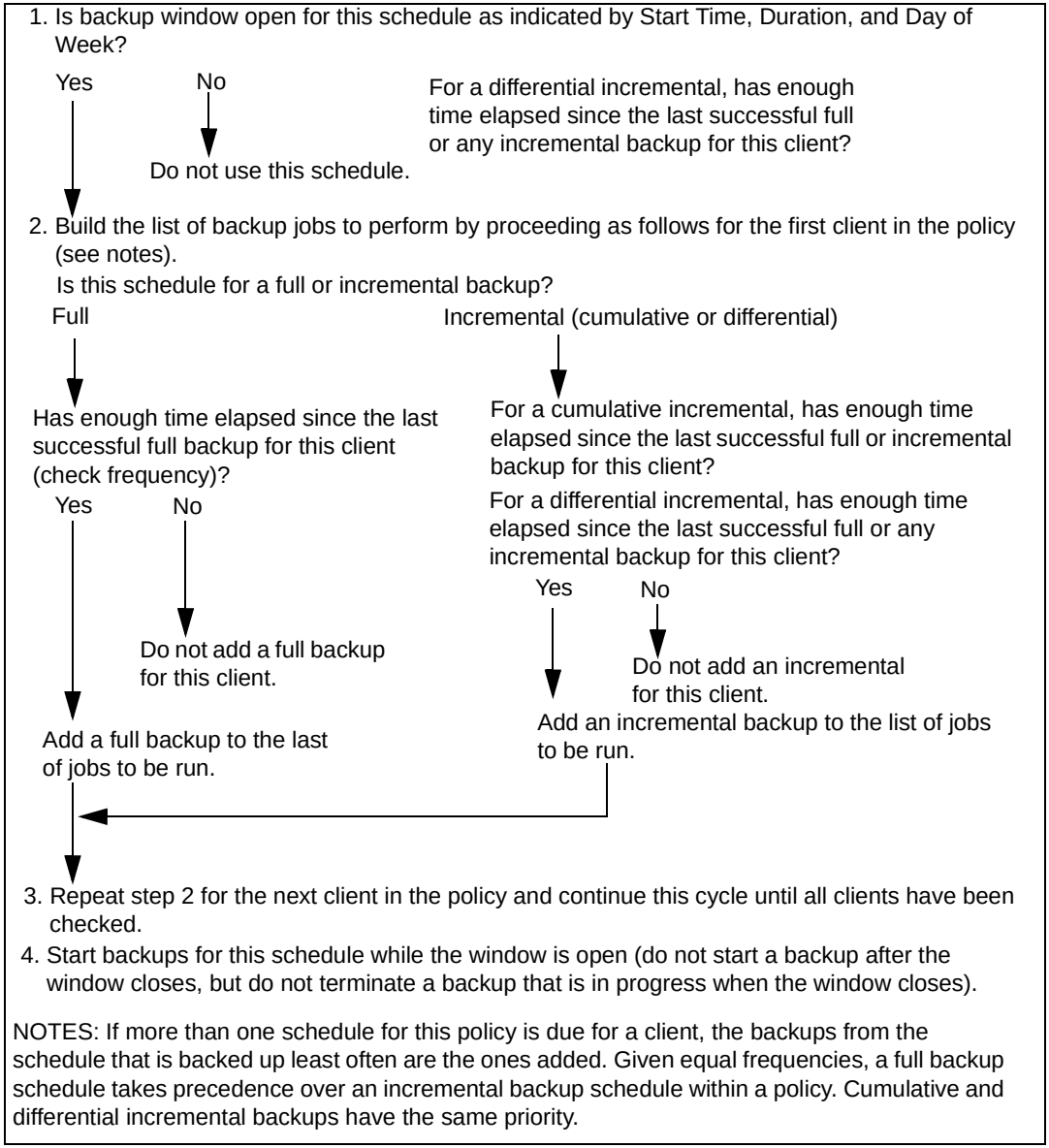
   The NetBackup counter you selected is displayed in the Performance window. The number of bytes read or written and the rate is updated dynamically.

How NetBackup Builds Its Automatic-Backup Worklist

The following topics explain how NetBackup determines the order in which automatic backups occur for each client. This information is for reference only but will be useful in evaluating problems with your schedules.

Building the Worklist (Queue)

When the backup window opens for an automatic-backup schedule, NetBackup proceeds as shown in the following figure to determine whether to add the client backups for that schedule to the worklist (queue).



Prioritizing the Worklist

The worklist typically contains jobs from different policies and schedules. NetBackup checks for the following when determining the order in which to run the backups that are in the worklist:

1. Highest priority backup as determined by the policy Priority attribute.

   Backup jobs from the policy with the highest priority runs first.

   For example, assume that clients ant and beetle are in different policies and that ant is in the policy with the highest priority. Here, the jobs for client ant always run before the client beetle jobs.

2. Backup with a retention level that is the same as a tape that is currently mounted.

   If policy priorities are equal, NetBackup tries to start a backup job that has the same retention period as a tape that is currently mounted. This reduces delays in waiting for tape mounts.

   For example, assume that clients ant and beetle are in the same policy but their schedules have different retention periods. Also, assume that the Ant job is the most overdue. However, a tape is mounted that has the same retention level as client beetle.

   Here, the client beetle job runs first because it can be stored on a tape that is already mounted, thus making the most efficient use of resources. If there is another drive of the correct type available, a tape will be mounted on that drive for the client ant job.

3. Most overdue backup job.

   If the priorities and retention level are equal, NetBackup prioritizes backups according to how long they are overdue. The clients that are the most overdue have the highest priority.

   NetBackup determines how long a backup is overdue by subtracting the backup frequency (on the schedule) from the length of time since the last successful backup for that client.

   For example, assume that clients ant and beetle have backup jobs that are in the same policy and have the same retention level. Also assume that the schedules for these backup jobs both have a frequency of 1 day. If the last backup for client ant ran 25 hours ago and the last backup for client beetle ran 26 hours ago, then both clients are overdue for a backup. However, the client beetle job is the most overdue and will run first.

   This approach ensures that a backup that was not successful during its previous backup window has priority over backups that were successful. This is important on a busy system where the backup window can sometimes close before all backups can begin.

Guidelines for Setting Retention Periods

The length of time that you must retain data usually depends on how likely you are to need it after a certain period of time. Some data, such as tax and other financial records, have legal requirements for retention. Other data, such as preliminary documents can probably be expired when the final version is complete.

How long you keep a backup also depends on what you need to recover from it. For example, if day-to-day changes are critical, you must keep all the incrementals in addition to full backups for as long as you need the data. If incrementals only track work in progress toward monthly reports, then you can probably expire the incrementals sooner and rely on the full backups for long-term recovery.

When deciding on retention periods, establish guidelines that apply to most of your data. After establishing guidelines, note files or directories that have retention requirements outside of these guidelines and plan to create a separate policy (or policies) for them. For example, placing files and directories with longer retention requirements in a separate policy allows you to schedule longer retention times for them without keeping all the others for the longer time period.

Another consideration for data retention is off-site storage of the backup media. This protects against fires or other disasters that occur at the primary site. Set the retention period to infinite for backups you must retain for more than one year.

- One method of implementing off-site disaster recovery is to use the duplicate feature to make a second copy for offsite storage.
- Another approach is to send monthly or weekly automatic full backups to an off-site storage facility. To restore the data, you get the media from off-site storage (a total directory or disk restore with incrementals requires the last full backup plus all incrementals).
- You can also configure an extra set of schedules for the backups to create duplicates for off-site storage.

Regardless of the method you use for off-site storage, ensure that you configure adequate retention periods. You can use the NetBackup import feature to retrieve expired backups but it is easiest just to set an adequate retention period.

Guidelines for Setting Backup Frequency

Choose the backup frequency based on how often you must back up your files to ensure that you can restore critical changes in case of a disk failure. How often the data changes is an important factor in determining backup frequency. For example, determine if files change several times a day, daily, weekly, or monthly. Determine the rate of change by analyzing typical file usage.

Typically, sites perform daily backups to preserve each day's work. This ensures that, at most, only one day's work is lost in case of a disk failure. More frequent backups are necessary when data changes many times during the day and these changes are important and difficult to reconstruct.

Daily backups are usually incrementals that record the changes since the last incremental or full backup. This conserves resources because incrementals use less storage and take less time to perform than full backups.

Full backups usually occur less frequently than incrementals but should occur often enough to avoid accumulating too many consecutive incrementals. Too many incrementals between full backups increases restoration time because of the effort required to merge those incrementals when restoring files and directories. When setting the frequency for full backups:

- Choose longer times between full backups for files that seldom change. This uses fewer system resources. It also does not significantly increase recovery time because there should be smaller incremental backups.
- Choose shorter times between full backups for files that change frequently. This decreases restore time. It can also use less resources because it reduces the cumulative effect of the longer incrementals that are necessary to keep up with frequent changes in the files.

To achieve the most efficient use of resources, ensure that most of the files in a given policy change at about the same rate. For example, assume that about half the files in a policy file list change frequently enough to require a full backup every week, but the rest rarely change and require only monthly full backups. Here, if all the files are in the same policy, you must perform full backups weekly on all the files. This wastes system resources and media because half the files need full backups only once a month. A better approach is to divide them into two policies, each with the appropriate backup schedule.

Determining Backup Media Requirements

To efficiently manage your backup environment, you must know the amount of media that is required for both daily and long-term use. The daily requirement must be known to ensure that enough tape volumes and disk space are available for each backup session. The long-term requirements are necessary to assess costs for acquisition of new media, storage devices, and off-site storage (if required).

For daily requirements, you must first determine the approximate amount of data in the files that you will back up to each type of media each day. Then, you can check the Media Summary report to verify that enough media IDs and disk space are available.

For long term planning, you must also consider the following:

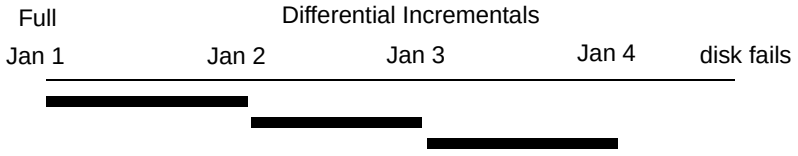
- How long you retain the data. A related consideration is that all backups on a given tape or optical have the same retention level. This means that if you have many different retention levels, you need more tapes or optical disks, unless you set the **Allow Multiple Retentions per Media** property.
- Duplicates for off-site storage or extra security.
- New software releases and other special backups.
- Replacing worn out media.
- Changes in disk usage patterns over the time period under consideration. If your disk usage and capacity increase, your backup needs will also probably increase.
- Number of backups that are on a tape. Because tape marks are created between backups, a tape with many small backups (as with incrementals) contains less real data than if it contains fewer large backups. The size of the tape marks vary depending on the media type. A large number of small files will also have a higher percentage of overhead in the backup because each file requires an extra 512 bytes for catalog information on the tape or disk.
- If you have many different volume pools, ensure that enough media is defined in each one to accommodate the data.

Incremental Backups Overview

NetBackup supports two types of incremental backups:

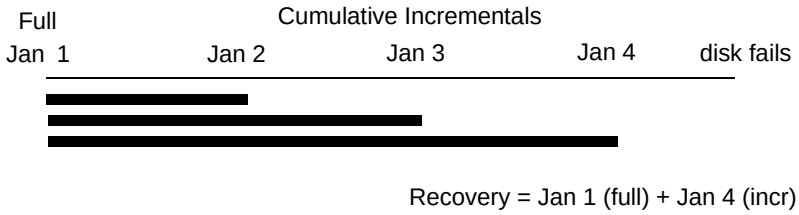
- Differential
- Cumulative

A differential incremental backs up only the data that has changed since the last full or incremental. The following example shows the data that is included in a series of backups between January 1 and January 4. The January 1 backup is a full and includes all files and directories in the policy file list. The subsequent backups are differential incrementals and include only the data that changed since the last full or differential-incremental backup. If the disk fails sometime on January 4 (after the backup), the full and all three of the incrementals are required for the recovery.



Recovery = Jan 1 (full) + Jan 2 (incr) + Jan 3 (incr) + Jan 4 (incr)

A cumulative incremental backs up all the data that has changed since the last full backup. The following example shows the data that is included in a series of backups between January 1 and January 4. The January 1 full backup includes all files and directories in the policy file list. Each of the cumulative-incremental backups include the data changed since the last full backup. If the disk fails sometime on January 4 (after the backup), the full and the last cumulative-incremental are required for the recovery.



The next two topics compare the relative retention requirements and the backup and restore times of these two types of incremental backups. The third topic in this section explains how NetBackup determines the files to include in an incremental backup.

Retention Requirements

The following table compares the retention requirements for differential- and cumulative-incremental backups.

Type	Retention Requirement	Comments
Differential	longer	It is necessary to have the last full backup and all the differential incrementals that have occurred since the last full backup in order to ensure that all files can be restored. Therefore, all the differentials must be kept until the next full backup occurs.
Cumulative	shorter	Each cumulative-incremental backup contains all the changes that have occurred since the last full backup. Therefore, a complete restore requires only the most recent cumulative incremental in addition to the full backup.

Backup and Restore Times

The following table compares the relative backup and restore times for differential- and cumulative-incremental backups.

Type	Backup Time	Restore Time	Comments
Differential	Shorter	Longer	Less data in each backup but all differential incrementals since the last full backup are required for a restore. This results in a longer restore time.
Cumulative	Longer	Shorter	More data in each backup, but only the last cumulative incremental is required for a complete restore (in addition to the full).

It is possible to use a combination of cumulative and differential incrementals in order to obtain some of the advantages of both methods. For example, assume a set of schedules with the following backup frequencies and retention periods (notice that the differential incrementals occur more often.)

Backup Type	Frequency	Retention Period
Full	6 days	2 weeks
Cumulative incremental	2 days	4 days
Differential incremental	1 day	2 days

This set of schedules results in the following series of backups.

day 1	day 2	day 3	day 4	day5	day 6	day 7	day 8
Full	Diff	Cum	Diff	Cum	Diff	Full	Diff

- Every other day a differential-incremental backup occurs, which will usually have a minimum backup time.

- On alternate days, a cumulative-incremental backup occurs, which will require more time than the differential but not as much as a full. The differential can now be expired.
- To recover all files requires, at most, two incremental backups in addition to the most recent full backup. This typically means less restore time than if all differential incrementals were used. The fulls can be done less often if the amount of data being backed up by the incrementals is small.

Determining Files Due for Backup on Windows Clients

On Windows clients, NetBackup performs incremental backups of files based on the **Perform Incrementals Based on Archive Bit** setting. This setting is found in the Backup, Archive and Restore client interface, under **File > NetBackup Client Properties**, on the **General** tab.

If **Perform Incrementals Based on Archive Bit** is checked, incrementals for this client are based on the state of each file's archive bit. The operating system sets the bit whenever a file is changed and it remains set until cleared by NetBackup. The conditions under which NetBackup clears the bit, depends on the type of backup being performed.

- For a full backup, NetBackup backs up files regardless of the state of their archive bit. After a full backup, the archive bit is always cleared.
- For a differential-incremental backup, NetBackup backs up files that have the archive bit set and have therefore been changed. When the client receives a response from the server indicating that the backup was successful (or partially successful) the archive bits are cleared. This allows the next differential incremental to back up only files that have changed since the previous full or differential-incremental backup.
- For a cumulative-incremental backup, NetBackup backs up files that have the archive bit set, but does not clear the archive bits after the backup. This allows the next cumulative incremental to back up not only changed files, but also files that were in this cumulative incremental.

If **Perform Incrementals Based on Archive Bit** box is clear, NetBackup includes a file in an incremental backup only if the file's datetime stamp has been changed since the last backup. The datetime stamp indicates when the file was last backed up.

- For a full backup, NetBackup backs up files regardless of the datetime stamp.
- For a differential-incremental backup, NetBackup compares the file's datetime stamp against the last full or incremental backup.
- For a cumulative-incremental backup, NetBackup compares the file's datetime stamp against the last full backup or incremental backup.

If you install or copy files from another computer, the new files retain the datetime stamp of the originals. If the original date is before the last backup date on this computer, then the new files are not be backed up until the next full backup.

Determining Files Due for Backup on UNIX Clients

The following explains how NetBackup determines that a file on a UNIX client is due for an incremental backup.

When performing incremental backups on NetBackup UNIX clients, all relevant files and directories are looked at to determine if they are due for backup based on a reference date (that is, back up all files changed since date X).

UNIX files and directories have three times associated with them:

- mtime -- the file modification time
- atime -- the file access time
- ctime -- the inode change time

UNIX man pages contain a definition of these attributes.

The mtime for a file or directory is updated by the file system each time the file is modified. Prior to modifying a file, an application can save the file's mtime, and then reset it after the modification using the utime(2) system call.

The atime for a file or directory is updated by the file system each time the file is accessed (read or write). Prior to accessing a file, an application can save the file's atime, and then reset it after the file access using the utime(2) system call.

The ctime for a file or directory is updated each time the file or directory's inode is changed; examples of this are changing permissions, ownership, link-counts, and so on. The ctime for a file or directory can not be saved before and reset after a change. Another significant fact is that the ctime of a file or directory is changed when resetting the mtime and atime (using the utime(2) system call) for the file.

When NetBackup reads the data for a file that is included in a backup, it does not affect the file modification time, but does affect the file's access time. For this reason, NetBackup saves the file's atime and mtime prior to reading the file, and (by default) resets the atime and mtime using the utime(2) system call. By "covering its tracks," NetBackup does not cause problems for storage migration products or administrator scripts that are utilizing file access times (atime) as criteria for their operations. While this benefit is obvious, a side effect is that it does update the file's ctime.

As an option to a NetBackup configuration, customers can choose to have NetBackup not reset the file's access time after it reads a file. Additionally, customers can choose to have NetBackup use the file's ctime, in addition to the mtime, when determining what files to

back up in an incremental. Normally, these two options are used together, but there may be sites which want to use one without the other. By default, NetBackup uses only the file's mtime to determine what files and directories to back up.

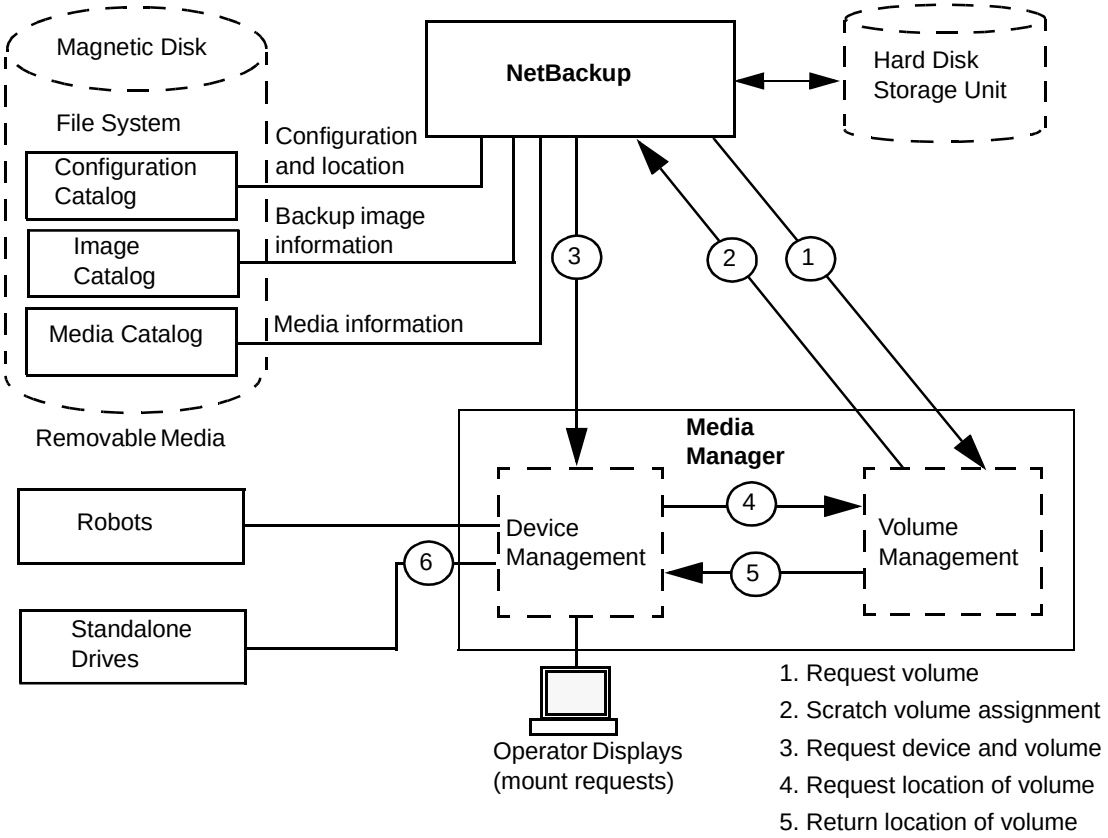
When a file is moved from one location to another, the file's ctime changes, but the mtime remains unchanged. If NetBackup is only using the file modification time (mtime) to determine files due to be backed up during an incremental backup, it will not detect these moved files. For sites where this is an issue, the ctime should also be used (if possible) to determine files due to be included in an incremental backup, using the `bp.conf` attributes `USE_CTIME_FOR_INCREMENTALS` and `DO_NOT_RESET_FILE_ACCESS_TIME`.

When a directory is moved from one location to another, the directory's ctime changes, but the mtime remains unchanged. Neither the mtime nor the ctime are changed for the files or directories within the moved directory. Using file timestamps, there is no reliable method for determining that files within a moved directory need to be included in an incremental backup.

In either case, these moved files and directories will obviously be included in subsequent full backups.

Storage Management Overview

The following figure shows the components involved in managing the storage of client data.



Storage Units

The peripheral that stores the backup data for NetBackup is referred to as a *storage unit*. In this context, the term *storage unit* means a group of one or more storage devices of a specific type and density that attach to a NetBackup server. The storage devices can be for removable media such as tape or a directory on a hard disk. Removable media devices can be robotic or standalone.

The administrator defines the storage units that are available and which storage unit to use for each policy. For example, it is possible to specify a robot as the storage unit for one policy and a standalone tape drive for another policy.

Media Manager

NetBackup keeps records about the files in the backups and also about the media where they are stored. Media Manager manages the removable storage units (for example, tape drives) and tracks the location of both online and offline volumes. If the storage unit is on disk, the data goes to the file path specified during configuration of the storage unit. The operating-system disk manager manages the actual reading and writing of data.

When sending a backup to a Media Manager storage unit, NetBackup looks in its media catalog for a previously used volume that is the correct density and is configured to retain backups for the desired period of time. If none of the previously used volumes are suitable, NetBackup requests a new media ID from Media Manager and then requests Media Manager to mount the volume in a device.

Note When a volume is allocated to NetBackup, other applications cannot use it until backups on the volume are no longer needed.

The request to Media Manager specifies both the volume's media ID and device density. If a request involves a robot, the volume is then automatically mounted in a drive and assigned to the request. With a standalone drive, NetBackup attempts to use the media that is in the drive.

If a standalone drive does not contain media or if the required volume is not available to a robot, Media Manager displays a mount request. An operator can then find the volume, mount it manually, and assign it to the drive.

To restore from a Media Manager storage unit, NetBackup finds the media ID in its media catalog and requests the volume from Media Manager.

Retention

The administrator specifies the retention period for the files associated with each schedule. It is possible to keep all backups with the same retention period on the same volume or to mix different retention periods on a volume.

Volume Pools

For Media Manager storage units, NetBackup supports a concept called volume pools. A *volume pool* is a distinct set of media that can be used *only* by the users and hosts that you designate when configuring the pool. You create volume pools and assign media to them when you configure Media Manager. Whenever a new volume is required for either a robotic or standalone drive, it is allocated to NetBackup from the requested volume pool.

A volume pool named *NetBackup* is always created by default and, unless you specify otherwise in the policy or schedule, all backups go to media in the *NetBackup* pool. You can, however, create other pools for NetBackup to use. For example, if you create *Auto* and *User* volume pools, you can specify that automatic backups will use media from the Auto pool and user backups will go to media in the User pool.

The volume pool concept is relevant only for storage units managed by Media Manager, and does not apply to disk storage units. For more information on volume pools, see the system administrator's guide for Media Manager.

Media Management Concepts

This section discusses concepts involved in managing NetBackup media.

NetBackup and Media Manager Catalogs

NetBackup and Media Manager use internal databases to keep information about media and device configuration. With the exception of the volume database, these internal databases are usually referred to as catalogs.

Caution Do not remove or manually edit the NetBackup or Media Manager catalogs. These files are for internal program use only and altering them in any way can result in permanent loss of data.

Volume Database

The volume database has information about volumes that have been configured for use by Media Manager. When you add volumes they are recorded in the volume database. The volume database resides in the *install_path*`\Volmgr\database` directory (the default *install_path* is `C:\Program Files\VERITAS`).

When you add new volumes, you do it on the NetBackup server that has the volume database. A part of this process is assigning media IDs.

Media IDs must be unique and can consist of six or less alphanumeric characters. Optical disks each have two media IDs, one for side A and one for side B. The terms *media ID* and *external media ID* are equivalent. Storage areas on disk are identified by their pathname.

Media Catalog

NetBackup keeps a media catalog with information that correlates backups to the volumes where they are stored. Each NetBackup server maintains a media catalog for the storage units attaching to that server.

During installation, the media catalog is created in the *install_path*`\NetBackup\db\media` directory. NetBackup refers to the media catalog when it needs a volume for a backup or restore. If the media catalog does not contain a suitable volume, NetBackup has Media Manager assign one. In this manner, the catalog is populated as NetBackup uses new volumes for backups.

When the retention period has ended for all backups on a volume, NetBackup deletes it from the media catalog. Media Manager then unassigns the volume so it is available for reassignment at a future date.

Note Volumes for backups of the NetBackup catalogs are a special case and do not appear in the media catalog. You must track the media IDs for these volumes separately so you can find them in case the media catalog is damaged. However, they do appear in the Media Manager volume catalog and are listed as assigned to NetBackup (they are unassigned only if you delete them from your catalog backup settings).

Device Catalogs

The device catalogs have information about the drives and robots that are in NetBackup storage units. When you configure drives and robots, Media Manager stores this information in its device catalogs. These catalogs are located under *install_path*`\Volmgr\database`.

Media States

The following media states apply to volumes that are in the NetBackup media catalog but are not active. That is, the volumes cannot be used for both backups and restores.

Media States

State	Description
FULL	NetBackup sets FULL status if it encounters an end of media (EOM) during a backup. 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.
SUSPENDED	NetBackup can automatically set volumes to the *SUSPENDED* state. You can also use the `bpmedia` command to manually suspend or unsuspend volumes. When an active NetBackup volume is suspended: - Backups are still available for restores (if they are expired you must import them first). - The volume is unavailable for future backups until the retention period ends for all backups that are on it. At that time, the suspended volume is deleted from the NetBackup media catalog and unassigned from NetBackup.
FROZEN	NetBackup can automatically set a volume to the FROZEN state. You can also use the `bpmedia` command to manually freeze or unfreeze volumes. When an active NetBackup volume is FROZEN: - Backups are still available for restores (if they are expired you must import them first). - The volume is unavailable for future backups. - The volume never expires, even when the retention period ends for all backups that are on the media. This means that the media ID is never deleted from the NetBackup media catalog and, therefore, remains assigned to NetBackup.

Media States (continued)

State	Description
IMPORTED	NetBackup automatically sets volumes to the IMPORTED state if they are imported to this server. When an active NetBackup volume is IMPORTED: - Backups are still available for restores (if they are expired you must import them first). - The volume is unavailable for future backups until the retention period ends for all backups that are on it. At that time, the imported volume is deleted from the NetBackup media catalog and unassigned from NetBackup.

How NetBackup Selects Media in a Robot

When NetBackup automatically selects a volume in a robot, it proceeds as follows:

1. Searches the NetBackup media catalog for a volume that is already mounted in a drive and meets the following criteria:
   - Configured to contain backups at the retention level required by the schedule (unless the NetBackup property **Allow Multiple Retentions per Media** is specified for the server).
   - In the volume pool required by the backup 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 the above conditions, 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. Media Manager then 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 one with the least mounts. 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 no available media.

Spanning Media

After an end of media condition, automatic media selection is a special case and depends on whether NetBackup is configured to allow backups to span media.

- NetBackup spans media if the NetBackup property **Disallow Backups Spanning Media** is not specified for the server. Here, 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 **Disallow Backups Spanning Media** is specified. Here, the backup terminates abnormally and the operation is retried according to the **Schedule Backup Attempts** global attribute.

How NetBackup Uses 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 feature is enabled, NetBackup tries to use whatever labeled or unlabeled media happens to be in a standalone drive. This capability is enabled by default during installation. The selection process is as follows:

1. If a backup is requested and an appropriate standalone drive does not contain a volume, NetBackup selects one in the same way as explained in “How NetBackup Selects Media in a Robot” on page 653.

   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 the volume that is in the drive.

   - A volume that has been previously used for backups must:
     - 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 are used by NetBackup.

     If the unused media is unlabeled, you can label it ahead of time 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.

     If the media is unlabeled:

     - NetBackup labels the media.
     - Media Manager adds a media ID to the volume configuration, if necessary. If a media ID is added, the NetBackup property Media ID Prefix is used as the first characters of the media ID. If Media ID Prefix is not specified, the default prefix is A. For example, A00000.
     - Media Manager adds the requested volume pool to the volume configuration (if the backup policy specifies a volume pool).

Disabling Standalone Drive Extensions

You can disable the standalone drive extensions by specifying the NetBackup property **Disable Standalone Drive Extensions** for the server. This 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 (EOM) condition is a special case and depends on whether NetBackup is configured to allow backups to span media.

- NetBackup spans media if the **Disallow Backups Spanning Media** property is not specified for the server. Here, NetBackup selects another volume to begin the next fragment and the resulting backup has fragments on more than one volume.

  Following an EOM, NetBackup first attempts to use an unassigned volume rather than one that already has images on it, and requests Media Manager to assign one. Media Manager checks its volume database for a volume that is the correct media type, in the correct volume pool, and so on. If Media Manager cannot find a suitable volume, NetBackup selects one from its media catalog. In either case, The Device Monitor shows the mount request and an operator must manually insert the volume and assign it to the drive.

- NetBackup does not span media if **Disallow Backups Spanning Media** is specified. Here, the backup terminates abnormally when the end of media is reached and the operation is rescheduled according to the **Schedule Backup Attempts** global attribute.

When spanning media and an end of media is encountered on a standalone drive that uses a gravity feed stacker (a stacker not controlled by software), you can have NetBackup continue on the next volume loaded by the stacker, rather than looking for another drive. To do this, specify the **Media Request Delay** property for the server. This setting specifies a number of seconds for NetBackup to pause before looking for another drive.

When using a standalone drive without a stacker, **Media Request Delay** can be set to allow enough time for the operator to insert the desired volume.

Keeping Standalone Drives in the Ready State

To leave standalone drives in a ready condition after a backup or restore completes, create an empty file named `NO_STANDALONE_UNLOAD` in the *install_path*`\NetBackup\Volmgr` directory. The setup program creates this file during installation if standalone drives are detected.

When NetBackup detects the presence of this file, it prevents Media Manager from ejecting the tape after an operation completes. The tape does eject if end-of media (EOM) is reached.

It is possible for more than one standalone drive to be ready and contain suitable media. If that occurs, drive selection occurs in logical drive index number order. For example, if drives 2 and 3 are the same type and both contain suitable media, NetBackup selects drive 2.

Hardware Compression

NetBackup tries to turn on hardware compression on all tape drives that support it. To disable this action, create the file *install_path*`\Volmgr\NO_COMPRESSION`. If this file exists, NetBackup disables hardware compression for all tape drives that it uses.

Media Format

NetBackup writes to media in a format that allows position to be verified before appending new backups. The format for tape media differ slightly due to characteristics of the media itself.

To determine the contents of tape media, use the Media Contents report.

Non-QIC Tape Format

For all tape media except QIC, the format for backups that are not multiplexed is:

MH * BH Image * BH Image * BH Image * EH *

Where:

MH = Media Header (1024 bytes)

* = Tape Mark

BH = Backup Header (1024 bytes)

Image = Data from the backup

EH = Empty Backup Header, used for position validation.

When adding a new backup to the above example, the tape is positioned to EH and 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 write, it terminates the tape with two tape marks and does not write an EH.

QIC Tape Format

For QIC tape media, NetBackup does not write empty backup headers (EH) so the format nonmultiplexed backups is:

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.

Fragmented Backups

For fragmented backups the media format is the same as described for QIC and non-QIC tapes, except that NetBackup breaks the backup into fragments of the size that you specify when you configure the storage unit.

For example:

MH * BH1 Image (frag 1)* BH1 Image (frag 2)* BH1 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.

Fragmenting tape backups can also speed up restores because NetBackup can skip to the specific fragment before starting its search for a file. Otherwise, it has to start at the very beginning of the backup and read tar headers until it finds the desired 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.

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 explained above 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: MH * ... *BHn Image (frag 1) * *

Next tape: MH * BHn Image (frag2)* ... * EH *

On the first tape, NetBackup does not write an EH, and terminates the tape with two tape marks.

Multiplexing Format

The tape format for multiplexed backups is:

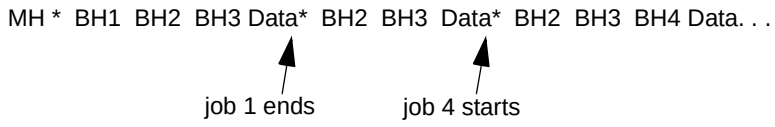
MH * BH1 ... BHn Data...

Where:

- MH is the Media Header (1024 bytes).
- * is a Tape Mark.
- BH1 ... BHn are backup Headers (1024 bytes). One for each job that is part of the set of jobs being multiplexed.

- Data is the data from the backup. By default, the data is in 64 kilobyte blocks. Each block also contains 512 bytes that are reserved for multiplexing control information (less than 1% of the total data) and to identify the backup that the block corresponds to.

Each time 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 figure below shows an example.



Labeling Media

You normally do not have to label media.

- For a robot, you select the media IDs when you configure the robot in Media Manager and tape labeling is done automatically when NetBackup uses the media.
- For standalone drives, the standalone drive extension feature makes it unnecessary to label media in a standalone drive, unless you desire to do so. You can, however, prelabel tapes by using the `bplabel` command.

Note 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 **Allow Media Overwrite** property. In either of these instances, you must label the media by using the `bplabel` command.

Mounting and Unmounting 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 drive.

For example, if a restore requires a volume that has been removed from a robot, the Device Monitor shows a mount request. The operator can then insert the proper volume and assign it to the request.

Automatic Media Suspend Or Device Down

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. 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 a is such that future positioning attempts will be unreliable. Write failures are frequently caused by a tape device with dirty heads or deteriorating media.

If investigation shows that the suspend or down action was incorrect, you can reverse it by:

1. Using the `bpmedia` command to unsuspend the volume.
2. Using the NetBackup Device Monitor to set the device to Up.

Planning Worksheets

The next two figures show a blank copy of a worksheet that will be useful for planning. Following the blank copy is a completed example. See Chapter 3, “Managing Backup Policies,” for information about the items on the worksheets.

Policies Planning Worksheet (Sheet 1)

Policy Name	
Clients	
File List	
Policy type	
Policy storage unit	Label:
Policy volume pool	Label:
☐ Limit jobs per policy	Value:
Job priority	
Keyword phrase	
☐ Active	
☐ Backup network drives (applies to Microsoft Windows clients only)	
☐ Cross mount points (applies to UNIX and Windows 2000 clients only)	
☐ Collect true image restore information	☐ with move detection
☐ Compression (applies to UNIX and Microsoft Windows clients only)	
☐ Collect disaster recovery information	
☐ Allow multiple data streams	

Policies Planning Worksheet (Sheet 2)

Attributes				
Schedule Name		Type of backup		
Schedule type				
	☐ Calendar			
	☐ Frequency	hours	days	weeks
☐ Multiple copies		Number of copies:		
	Storage Unit	Volume Pool	Retention	If this copy fails
☐ Override policy storage unit		Label:		
☐ Override policy volume pool		Label:		
Retention		weeks	months	other
Media multiplexing				
Start Window				
	Sunday	Start	Duration	End
	Monday			
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
Exclude Dates				

Policies Planning Worksheet (Sheet 3)

Attributes				
Schedule Name		Type of backup		
Schedule type				
	☐ Calendar			
	☐ Frequency	hours	days	weeks
☐ Multiple copies		Number of copies:		
	Storage Unit	Volume Pool	Retention	If this copy fails
☐ Override policy storage unit		Label:		
☐ Override policy volume pool		Label:		
Retention		weeks	months	other
Media multiplexing				
Start Window				
	Sunday	Start	Duration	End
	Monday			
	Tuesday			
	Wednesday			
	Thursday			
	Friday			
	Saturday			
Exclude Dates				

Sample Worksheet for UNIX Clients (Sheet 1)

Policy Name W2 on server bunny	
Clients mars (RS6000 / AIX), jupiter (Solaris), neptune (HP)	
File List / usr, / hom, / var	
Policy type Standard	
Policy storage unit	Label: TS_8
Policy volume pool	Label: Backups
☐ Limit jobs per policy	Value:
Job priority 0	
Keyword phrase	
☒ Active	
☐ Backup network drives (applies to Microsoft Windows clients only)	
☐ Cross mount points (applies to UNIX and Windows 2000 clients only)	
☐ Collect true image restore information	☐ with move detection
☐ Compression (applies to UNIX and Microsoft Windows clients only)	
☐ Collect disaster recovery information	
☐ Allow multiple data streams	

Sample Worksheet for UNIX Clients (Sheet 2)

Attributes				
Schedule Name W2DailyIncr		Type of backup Differential Incr		
Schedule type				
	☐ Calendar			
	☒ Frequency	hours	1 days	weeks
☐ Multiple copies		Number of copies:		
	Storage Unit	Volume Pool	Retention	If this copy fails
☐ Override policy storage unit		Label:		
☐ Override policy volume pool		Label:		
Retention		1 weeks	months	other
Media multiplexing 1				
Start Window				
	Sunday	Start	Duration	End
	Monday	22:00	8	
	Tuesday	22:00	8	
	Wednesday	22:00	8	
	Thursday	22:00	8	
	Friday	22:00	8	
	Saturday	22:00	8	
Exclude Dates				

Sample Worksheet for UNIX Clients (Sheet 3)

Attributes				
Schedule Name W2WeeklyFull		Type of backup Full		
Schedule type				
	☐ Calendar			
	☒ Frequency	hours	days	1 weeks
☐ Multiple copies		Number of copies:		
	Storage Unit	Volume Pool	Retention	If this copy fails
☐ Override policy storage unit		Label:		
☐ Override policy volume pool		Label:		
Retention		weeks	1 months	other
Media multiplexing 1				
Start Window				
	Sunday	Start	Duration	End
	Monday	22:00	8	
	Tuesday	22:00	8	
	Wednesday	22:00	8	
	Thursday	22:00	8	
	Friday	22:00	8	
	Saturday	22:00	8	
Exclude Dates				

Sample Worksheet for Windows Clients (Sheet 1)

Policy Name W2 on server mercury	
Clients mars (NT), jupiter (NT), neptune (NT)	
File List C:\	
Policy type MS-Windows-NT	
Policy storage unit	Label: TS_8
Policy volume pool	Label: Backups
☐ Limit jobs per policy	Value:
Job priority 0	
Keyword phrase	
☒ Active	
☐ Backup network drives (applies to Microsoft Windows clients only)	
☐ Cross mount points (applies to UNIX and Windows 2000 clients only)	
☐ Collect true image restore information	☐ with move detection
☐ Compression (applies to UNIX and Microsoft Windows clients only)	
☐ Collect disaster recovery information	
☐ Allow multiple data streams	

Sample Worksheet for Windows Clients (Sheet 2)

Attributes				
Schedule Name W2DailyIncr		Type of backup Differential Incr		
Schedule type				
	☐ Calendar			
	☒ Frequency	hours	1 days	weeks
☐ Multiple copies		Number of copies:		
	Storage Unit	Volume Pool	Retention	If this copy fails
☐ Override policy storage unit		Label:		
☐ Override policy volume pool		Label:		
Retention		1 weeks	months	other
Media multiplexing 1				
Start Window				
	Sunday	Start	Duration	End
	Monday	22:00		
	Tuesday	22:00		
	Wednesday	22:00		
	Thursday	22:00		
	Friday	22:00		
	Saturday	22:00		
Exclude Dates				

Sample Worksheet for Windows Clients (Sheet 3)

Attributes				
Schedule Name W2WeeklyFull		Type of backup Full		
Schedule type				
	☐ Calendar			
	☒ Frequency	hours	days	1 weeks
☐ Multiple copies		Number of copies:		
	Storage Unit	Volume Pool	Retention	If this copy fails
☐ Override policy storage unit		Label:		
☐ Override policy volume pool		Label:		
Retention		weeks	1 months	other
Media multiplexing 1				
Start Window				
	Sunday	Start	Duration	End
	Monday	22:00		06:00
	Tuesday	22:00		06:00
	Wednesday	22:00		06:00
	Thursday	22:00		06:00
	Friday	22:00		06:00
	Saturday	22:00		06:00
Exclude Dates				

UNIX Reference Topics C

This document contains information that pertains specifically to administering UNIX NetBackup clients from a Windows NT/2000 NetBackup master server.

Most administrative tasks on the UNIX systems can be performed by using the NetBackup administration interface on a Windows NT/2000 NetBackup server or administration client.

Cross Mount Points

The following information applies specifically to UNIX clients.

Collect True Image Restore Information

Note **True Image Restore Information** applies only to certain policy types and NetBackup allows you to select it only in those instances.

Specifies that NetBackup will start collecting the information required to restore directories to contain what they had at the time of any incremental (or full backup) that the user chooses to restore. Files that were deleted before the time of the selected backup are not restored. Otherwise, for example, a restore based on the date of an incremental includes all files backed up since the last full backup, including those that were deleted sometime during that period.

NetBackup starts collecting the true-image restore information beginning with the next full or incremental backup for the policy. The true-image restore information is collected for each client regardless of whether any files were actually changed.

NetBackup does not provide true-image restores based on the time of a user backup or archive. It does, however, use the backups from user operations for a true-image restore, if they are more recent than the latest automatic full or incremental.

To have true-image incremental backups include files that were moved, renamed, or newly installed in the directories, you must also select **With Move Detection**.

With Move Detection

Specifies that NetBackup also collect the information required to detect files and directories that have been moved, renamed, or newly installed and then include those files and directories in incremental backups for this policy.

Without move detection, NetBackup skips these files and directories because their archive bits are unchanged. With move detection, NetBackup compares path names with those from the previous full or incremental backup. If a name is new or changed, the file or directory is backed up.

The following are examples where using move detection backs up files that would not otherwise be backed up:

- A file named `C:\pub\doc` is moved to or installed in `C:\spec\doc`. Here, the archive bit is unchanged but `C:\spec\doc` is new in the `C:\spec\` directory and is backed up.
- A directory named `C:\security\dev\` is renamed as `C:\security\devices\`. Here, the archive bit is unchanged but `C:\security\devices\` is a new directory and is backed up.

NetBackup starts collecting information required for move detection beginning with the next full or incremental backup for the policy. This first backup after setting the attribute, always backs up all files, even if it is an incremental.

Move detection takes space on the client and the backup can fail if there is not enough disk space available.

Example of What Happens During True-Image Restores

The following table shows the files backed up in the `C:\home\abc\doc` directory during a series of backups between 12/01/2001 and 12/04/2001. Assume that **True Image Restore Information** was selected for the policy that did the backups.

Day	Type of Backup	Files Backed Up in C:\user\doc						
12/01/2001	Full	file1	file2	dirA\fileA	dirB\fileB	file3		
12/02/2001	Incremental	file1	file2	dirA\fileA	----------	------		
12/03/2001	Incremental	file1	file2	dirA\fileA	----------	------		
12/04/2001	User backup	file1	file2	dirA\fileA	----------	------	dirC\fileC	file4
12/04/2001	Incremental	file1	file2	----------	----------	------	----------	file4

Day	Type of Backup	Files Backed Up in C:\user\doc
Note Dashes (------) indicate that the file was deleted prior to this backup.		

Also, assume that you are going to restore the 12/04/2001 version of the `C:\user\doc` directory.

- If you do a regular restore, the restored directory has all files and directories that ever existed in `C:\user\doc` from 12/01/2001 (last full backup) through 12/04/2001:

  ```
  file1
  file2
  dirA\fileA
  dirB\fileB
  file3
  dirC\fileC
  file4
  ```

- If you do a true-image restore of the 12/04/2001 backup, the restored directory has only the files and directories that existed at the time of the incremental backup on 12/04/2001:

  ```
  file1
  file2
  file4
  ```

  NetBackup does not restore *any* of the files deleted prior to the 12/04/2001 incremental backup.

  The restored directory does not include the `dirA` and `dirC` subdirectories, even though they were backed up on 12/04/2001 with a user backup. NetBackup did not restore these directories because they did not exist at the time of the incremental backup, which was the reference for the true-image restore.

Notes On True-Image Restores and Move Detection

- Because the additional information that NetBackup collects for incrementals is the same as for a full backup, incremental backups take much more disk space when you are collecting true-image restore information. Adding move detection requires even more additional space.
- You can set the period of time that NetBackup keeps the true-image restore information by setting **How Long to Keep TIR Information** on the Global NetBackup Attributes properties tab. (See “How Long to Keep TIR Information” on page 243.)
- Incremental backups are slower for a policy where true-image restore information is being collected.

- You can perform true-image restores only on directories that were backed up by a policy for which NetBackup is collecting true-image restore information.

  If you intend to restore an entire file system or disk by using a true-image restore, ensure that all the desired directories are backed up by a policy that is collecting true-image restore information.

- For true-image restores, you can list and select only directories. In true-image restore mode, the client-user interface does not show individual files or let you select them. The NetBackup user's guides explain this further and provide instructions for performing true-image restores.

- A true-image restore preserves files that are currently in the directory but were not present when the backup was done. In our previous example, assume you created a file named file5 after the incremental backup occurred on 12/04/2001, but before doing the restore. In this case, the contents of the directory after the restore is:

  ```
  file1
  file2
  file4
  file5
  ```

Exclude and Include Lists on UNIX Clients

Note Exclude and include lists do not apply to user backups and archives.

On UNIX clients, you create the exclude and include lists in the following files on the client:

```
/usr/openv/netbackup/exclude_list
/usr/openv/netbackup/include_list
```

The following topics explain the rules for creating these lists on UNIX clients.

Creating an Exclude List on a UNIX Client

If you create a `/usr/openv/netbackup/exclude_list` file on a UNIX client, NetBackup uses the contents of the file as a list of patterns to skip during automatic full and incremental backups.

The following types of files typically appear in an exclude list:

- `*.o` files
- `core` files
- `a.out` files

- Files prefixed or suffixed by ~ (backups for editors)
- Files and directories under `/tmp`, `/usr/tmp`
- Man pages
- Software that you can restore from original installation tapes
- Automounted directories
- CD-ROM file systems
- On Solaris 8 and 9, always add `/etc/mnttab` and `/proc` to the exclude list

Note VERITAS suggests that you always specify automounted directories and CD-ROM file systems in the exclude list. Otherwise, if they are not mounted at the time of a backup, NetBackup must wait for a timeout before proceeding.

Check with users before excluding any files from their backups.

Syntax Rules

The following syntax rules apply to exclude lists:

- Blank lines or lines beginning with a pound sign (#) are ignored.
- Only one pattern per line is allowed.
- The following special or wildcard characters are recognized:

  [ ]

  ?

  *

- To use special or wildcard characters literally (that is, as nonwildcard characters), precede them with a backslash (\). For example, assume the brackets in the following are to be used literally

  ```
  /home/abc/fun[ny]name
  ```

  In the exclude list, precede them with a backslash as in

  ```
  /home/abc/fun\[ny\]name
  ```

Note A backslash (\) acts as an escape character only when it precedes a special or wildcard character as in the above example. This means that NetBackup normally interprets a backslash literally and it is a legal character to use in pathnames.

- If you exclude all files in the file list by using / or *, NetBackup backs up only what is specified by full path names in the include list.

- Spaces are considered legal characters. Do not include extra spaces unless they are part of the file name.

  For example, if you want to exclude a file named

  `/home/testfile` (with no extra space character at the end)

  and your exclude list entry is

  `/home/testfile` (with an extra space character at the end)

  NetBackup cannot find the file until you delete the extra space from the end of the file name.

- End a file path with `/` to exclude only directories with that path name (for example, `/home/test/`). If the pattern does not end in `/` (for example, `/usr/test`), NetBackup excludes both files and directories with that path name.

- To exclude all files with a given name, regardless of their directory path, just enter the name without a preceding slash. For example:

  ```
  test
  ```

  rather than

  ```
  /test
  ```

  This is equivalent to prefixing the file pattern with

  ```
  /
  /*/
  /*/*/
  /*/*/*/
  ```

  and so on.

- Do not use patterns with links in the names. For example, assume `/home` is a link to `/usr/home` and `/home/doc` is in the exclude list. The file is still backed up in this case because the actual directory path, `/usr/home/doc`, does not match the exclude list entry, `/home/doc`.

Example of an Exclude List

In this example, an exclude list contains the following entries:

```
# this is a comment line
/home/doe/john
/home/doe/abc/
/home/*/test
```

```
/*/temp
core
```

Given the exclude list above, the following files and directories are excluded from automatic backups:

- The file or directory named `/home/doe/john`.
- The directory `/home/doe/abc` (because the exclude entry ends with `/`).
- All files or directories named `test` that are two levels below home.
- All files or directories named `temp` that are two levels below the root directory.
- All files or directories named `core` at any level.

Exclude Lists for Specific Policies or Schedules

NetBackup allows you to create an exclude list for a specific policy or a policy and schedule combination. To do this, create an exclude_list file with a *.policyname* or *.policyname.schedulename* suffix. The following are two examples for a policy named *wkstations* that contains a schedule named *fulls*:

```
/usr/openv/netbackup/exclude_list.wkstations
/usr/openv/netbackup/exclude_list.wkstations.fulls
```

The first file affects all scheduled backups in the policy named *wkstations*. The second file affects backups only when the schedule is named *fulls*.

For a given backup, NetBackup uses only one exclude list and that is the one with the most specific name. For example, if there are files named:

`exclude_list.wkstations` and `exclude_list.wkstations.fulls`

NetBackup uses only:

```
exclude_list.wkstations.fulls
```

Creating an Include List on a UNIX Client

To add back in files that you eliminate with the exclude list, create a `/usr/openv/netbackup/include_list` file. The same syntax rules apply as explained previously for the exclude list.

To illustrate the use of an include list, we use the example from the previous discussion. The exclude list in that example causes NetBackup to omit all files or directories named test from all directories beneath `/home/*/test`.

In this case, add back in a file named `/home/jdoe/test` by creating a `/usr/openv/netbackup/include_list` file on the client and adding the following to it:

```
# this is a comment line
/home/jdoe/test
```

To create an include list for a specific policy or policy and schedule combination, use a *.policyname* or *.policyname.schedulename* suffix. The following are two examples of include list names for a policy named *wkstations* that contains a schedule named *fulls*.

```
/usr/openv/netbackup/include_list.workstations
/usr/openv/netbackup/include_list.workstations.fulls
```

The first file affects all scheduled backups in the policy named workstations. The second file affects backups only when the schedule is named *fulls*.

For a given backup, NetBackup uses only one include list and that is the one with the most specific name. For example, assume there are files such as the following:

`include_list.workstations` and `include_list.workstations.fulls`

In such a case, NetBackup uses only the following:

```
include_list.workstations.fulls
```

Schedules for User Backups or Archives

To have NetBackup use a specific policy and schedule for user backups or archives of a UNIX client, add the following options to the `/usr/openv/NetBackup/bp.conf` file.

- `BPARCHIVE_CLASS`
- `BPARCHIVE_SCHED`
- `BPBACKUP_CLASS`
- `BPBACKUP_SCHED`

These options can also be added to a user's `$HOME/bp.conf` file on the client.

NetBackup Notify Scripts D

Note Windows NT systems must be running Windows NT 4.0 or higher to use these scripts

NetBackup provides the following scripts (batch files on Windows 2000 and NT) for collecting information and providing notification of events.

Scripts that run on a server:

`backup_notify.cmd`

`backup_exit_notify.cmd`

`dbbackup_notify.cmd`

`diskfull_notify.cmd`

`restore_notify.cmd`

`session_notify.cmd`

`session_start_notify.cmd`

`userreq_notify.cmd`

Scripts that run on clients:

`bpstart_notify (UNIX clients only)`

`bpend_notify (UNIX clients only)`

`bpstart_notify.bat (Microsoft Windows clients only)`

`bpend_notify.bat (Microsoft Windows clients only)`

The scripts that run on a server are installed during NetBackup server installation and are in:

install_path`\NetBackup\bin`

On a UNIX client, you can run only the `bpstart_notify` and `bpend_notify` scripts. Before using these scripts, you must copy them from

install_path`\NetBackup\bin\goodies\`

on the server to

```
/usr/openv/netbackup/bin
```

on the client.

On a Windows 2000 or NT client, you can run only the `bpstart_notify.bat` and `bpend_notify.bat` scripts. These scripts are not supplied with the software. You must create them on the client per the criteria in the "bpstart_notify.bat (Microsoft Windows clients only)." and "bpend_notify.bat (Microsoft Windows clients only)." discussions.

For further information, refer to the comments in the scripts.

backup_notify.cmd

The `backup_notify.cmd` script runs on the NetBackup server where the storage unit is located and is called each time a backup is successfully written to media. The parameters that NetBackup passes to this script are:

- The name of the program doing the backup
- The backup-image name or path

For example:

```
backup_notify.cmd bptm bilbo_0695316589
```

backup_exit_notify.cmd

The `backup_exit_notify.cmd` script runs on the master server. The NetBackup scheduler on the master server calls this script to do site specific processing when an individual backup has completed from the perspective of the client, Media Manager, and the image catalog.

NetBackup passes the following parameters to the script:

Parameter	Description
`clientname`	Name of the client from the NetBackup catalog.
`policyname`	Policy name from the NetBackup catalog.
`schedname`	Schedule name from the NetBackup catalog.
`schedtype`	One of the following: `FULL`, `INCR` (differential incremental), `CINC` (cumulative incremental), `UBAK`, `UARC`

Parameter	Description
exitstatus	Exit code for the entire backup job.

For example:

```
backup_exit_notify.cmd freddie production fulls FULL 0
backup_exit_notify.cmd danr production incrementals INCR 73
```

bpstart_notify (UNIX clients only)

Note Before using this script, ensure that it is executable by *other* on the client. Do this by running `chmod 755` *script_name*. Where *script_name* is the name of the script.

On UNIX clients, NetBackup calls the `bpstart_notify` script each time the client starts a backup or archive operation. To use this script, copy

install_path`\NetBackup\bin\goodies\bpstart_notify`

from the server to

`/usr/openv/netbackup/bin/bpstart_notify`

on the UNIX client. Then, modify the script as desired and ensure that you have permission to run the script.

The `bpstart_notify` script runs each time a backup or archive starts and initialization is completed (but before the tape positioning). This script must exit with a status of 0 for the calling program to continue and for the backup or archive to proceed. A nonzero status causes the client backup or archive to exit with a status of `bpstart_notify failed`.

If the `/usr/openv/netbackup/bin/bpstart_notify` script exists, it runs in the foreground and the `bpbkar` process on the client waits for it to complete before continuing. Any commands in the script that do not end with an & character run serially.

The server expects the client to respond with a `continue` message within the period of time specified by the NetBackup `BPSTART_TIMEOUT` option on the server.

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

NetBackup passes the following parameters to the script:

Parameter	Description
`clientname`	Name of the client from the NetBackup catalog.
`policyname`	Policy name from the NetBackup catalog.
`schedname`	Schedule name from the NetBackup catalog.
`schedtype`	One of the following: `FULL`, `INCR` (differential incremental), `CINC` (cumulative incremental), `UBAK`, `UARC`

For example:

```
bpstart_notify freddie cd4000s fulls FULL
bpstart_notify danr cd4000s incrementals INCR
bpstart_notify hare cd4000s fulls FULL
bpstart_notify freddie cd4000s user_backups UBAK
bpstart_notify danr cd4000s user_archive UARC
```

To create a `bpstart_notify` script for a specific policy or policy and schedule combination, create script files with a *.policyname* or *.policyname.schedulename* suffix. The following are two examples of script names for a policy named *production* that has a schedule named *fulls*:

```
/usr/openv/netbackup/bin/bpstart_notify.production
/usr/openv/netbackup/bin/bpstart_notify.production.fulls
```

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

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

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

```
BACKUPID
UNIXBACKUPTIME
BACKUPTIME
```

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

```
BACKUPID=freddie_0857340526

UNIXBACKUPTIME=0857340526

BACKUPTIME=Sun Mar 2 16:08:46 1997
```

In addition to the above, the following environment variables can be used for the support of multiple data streams:

`STREAM_NUMBER` indicates the stream number. The first stream started from a policy, client, and schedule will be 1. A value of 0, indicates that multiple data streams is not enabled.

`STREAM_COUNT` specifies the total number of streams to be generated from this policy, client, and schedule.

`STREAM_PID` is the pid (process ID) number of `bpbkar`.

bpstart_notify.bat (Microsoft Windows clients only)

For all Windows clients, you can create batch scripts that provide notification whenever the client starts a backup or archive. These scripts must reside on the client and in the same directory as the NetBackup client binaries:

install_path`\NetBackup\bin`

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

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

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

install_path`\netbackup\bin\bpstart_notify.bat`

Note On Windows 98 and 95 systems, use a `pif` suffix on the batch scripts. For example, `bpstart_notify.pif`. The `bat` suffix, as shown in the examples, applies only to Windows 2000 and NT systems.

To create a `bpstart_notify` script that applies only to a specific policy or policy and schedule combination, add a *.policyname* or *.policyname.schedulename* suffix to the script name.

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

  install_path`\netbackup\bin\bpstart_notify.days.bat`

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

  install_path`\netbackup\bin\bpstart_notify.days.fulls.bat`

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

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

`bpstart_notify.`*policy*`.`*schedule*`.bat`

`bpstart_notify.`*policy*`.bat`

`bpstart_notify.bat`

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

Note If you are also using `bpend_notify` scripts, they can provide a different level of notification than the `bpstart_notify` scripts. For example, if you had one of each, they could be `bpstart_notify.policy.bat` and `bpend_notify.policy.schedule.bat`.

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

Parameter	Description
`%1`	Name of the client from the NetBackup catalog.
`%2`	Policy name from the NetBackup catalog.
`%3`	Schedule name from the NetBackup catalog.
`%4`	One of the following: `FULL`, `INCR`, `CINC`, `UBAK`, `UARC`
`%5`	Status of the operation is always 0 for `bpstart_notify`.

Parameter	Description
%6	Results file that NetBackup checks for a return code from the script. NetBackup uses %6 to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named *install_path*\netbackup\bin\BPSTART_RES.*policy*.*schedule* If the script applies to a specific policy, the results file must be named *install_path*\netbackup\bin\BPSTART_RES.*policy* If the script applies to all backups, the results file must be named *install_path*\netbackup\bin\BPSTART_RES An echo 0> %6 statement is one way for the script to create the file. NetBackup deletes the existing results file before calling the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.

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

For Windows 2000 and NT clients, the bpstart_notify script can use the following environment variables for the support of multiple data streams:

STREAM_NUMBER indicates the stream number. The first stream started from a policy, client, and schedule will be 1. A value of 0, indicates that multiple data streams is not enabled.

STREAM_COUNT specifies the total number of streams to be generated from this policy, client, and schedule.

STREAM_PID is the pid (process ID) number of bpbkar.

bpend_notify (UNIX clients only)

Caution The bpend_notify script is run when the client is finished sending data, but the server has not yet completed writing to media.

Note Before using this script, ensure that it is executable by *other* on the client. Do this by running chmod 755 *script_name*. Where *script_name* is the name of the script.

For a UNIX client, if you need notification whenever the client completes a backup or archive operation, copy

install_path\NetBackup\bin\goodies\bpend_notify

from the server to

/usr/openv/netbackup/bin/bpend_notify

on the UNIX client. Then, modify the script as desired, and ensure that you have permission to run the script.

The bpend_notify script runs each time a backup or archive completes. For archives, it runs after the backup but before the files are removed.

If bpend_notify exists, it runs in the foreground and bpbkar on the client waits until it completes. Any commands that do not end with an & character run serially.

The server expects the client to respond within the period of time specified by the BPEND_TIMEOUT NetBackup configuration option on the server. The default for BPEND_TIMEOUT is 300.

If the script needs more than 300 seconds, set BPEND_TIMEOUT to a larger value. Avoid too large a value or you will delay the server from servicing other clients.

NetBackup passes the following parameters to the bpend_notify script:

Parameter	Description
clientname	Name of the client from the NetBackup catalog.
policyname	Policy name from the NetBackup catalog.
schedname	Schedule name from the NetBackup catalog.
schedtype	One of the following: FULL, INCR (differential incremental), CINC (cumulative incremental), UBAK, UARC
exitstatus	Exit code from bpbkar. This is only client status and does not mean that the backup is complete and successful. For example, the client can show a status 0 when, due to a failure on the server, the All Log Entries report shows a status 84.

For example:

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

To create a bpend_notify script for a specific policy or policy and schedule combination, create script files with a *.policyname* or *.policyname.schedulename* suffix. The following are two examples of script names for a policy named *production* that has a schedule named *fulls*:

```
/usr/openv/netbackup/bin/bpend_notify.production
```

```
/usr/openv/netbackup/bin/bpend_notify.production.fulls
```

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

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

If the UNIX client is running NetBackup 3.0 or later software, the bpend_notify script can use the following environment variables:

```
BACKUPID
UNIXBACKUPTIME
BACKUPTIME
```

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

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

In addition to the above, the following environment variables can be used for the support of multiple data streams:

STREAM_NUMBER indicates the stream number. The first stream started from a policy, client, and schedule will be 1. A value of 0, indicates that multiple data streams is not enabled.

STREAM_COUNT specifies the total number of streams to be generated from this policy, client, and schedule.

STREAM_PID is the pid (process ID) number of bpbkar.

bpend_notify.bat (Microsoft Windows clients only)

For Windows 2000, NT, 98, and 95 clients, you can create batch scripts that provide notification whenever the client completes a backup or archive. These scripts must reside on the client and in the same directory as the NetBackup client binaries:

install_path`\NetBackup\bin`

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

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

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

install_path`\netbackup\bin\bpend_notify.bat`

Note On Windows 98 and 95 systems, use a `pif` suffix on the batch scripts. For example, `bpend_notify.pif`. The `bat` suffix, as shown in the examples, applies only to Windows 2000 and NT systems.

To create a script that applies only to a specific policy or policy and schedule combination, add a *.policyname* or *.policyname.schedulename* suffix to the script name.

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

  install_path`\netbackup\bin\bpend_notify.days.bat`

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

  install_path`\netbackup\bin\bpend_notify.days.fulls.bat`

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

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

`bpend_notify.`*policy*`.`*schedule*`.bat`

`bpend_notify.`*policy*`.bat`

`bpend_notify.bat`

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

Note If you are also using `bpstart_notify` scripts, they can provide a different level of notification than the `bpend_notify` scripts. For example, if you had one of each, they could be `bpstart_notify.policy.bat` and `bpend_notify.policy.schedule.bat`.

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

Parameter	Description
`%1`	Name of the client from the NetBackup catalog.
`%2`	Policy name from the NetBackup catalog.
`%3`	Schedule name from the NetBackup catalog.
`%4`	One of the following: `FULL`, `INCR`, `CINC`, `UBAK`, `UARC`
`%5`	Status of the operation and is same as sent to the NetBackup server. This is 0 for successful backups and 1 for partially successful backups. If an error occurs, the status is the value associated with that error.
`%6`	Results file that NetBackup checks for a return code from the script. NetBackup uses `%6` to pass the file name and then expects the script to create the file in the same directory as the script. If the script applies to a specific policy and schedule, the results file must be named *install_path*`\netbackup\bin\BPEND_RES.`*policy*`.`*schedule* If the script applies to a specific policy, the results file must be named *install_path*`\netbackup\bin\BPEND_RES.`*policy* If the script applies to all backups, the results file must be named *install_path*`\netbackup\bin\BPEND_RES` An `echo 0> %6` statement is one way for the script to create the file. NetBackup deletes the existing results file before calling the script. After the script runs, NetBackup checks the new results file for the status. The status must be 0 for the script to be considered successful. If the results file does not exist, NetBackup assumes that the script was successful.

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

For Windows 2000 and NT clients, the bpend_notify script can use the following environment variables for the support of multiple data streams:

STREAM_NUMBER indicates the stream number. The first stream started from a policy, client, and schedule will be 1. A value of 0, indicates that multiple data streams is not enabled.

STREAM_COUNT specifies the total number of streams to be generated from this policy, client, and schedule.

STREAM_PID is the pid (process ID) number of bpbkar.

dbbackup_notify.cmd

The dbbackup_notify.cmd script runs on the master server and is called each time NetBackup completes an attempt to back up its catalogs. NetBackup passes the following parameters to this script:

Parameter	Description
device	Device type the backup was written to.
vsn_or_path	Volume serial number (for tape) or path (for disk) used for the backup.
status	Specifies whether the backup was successful and must have a value of either SUCCESS or FAIL.

For example:

```
dbbackup_notify.cmd DISK /disk1/bpsync1 SUCCESS
dbbackup_notify.cmd OPTICAL AA0001 FAIL
dbbackup_notify.cmd TAPE XYZ047 SUCCESS
```

You must be able to identify the most recent catalog backup. Therefore, consider modifying this script to produce a printed copy of the media ID to which the catalog backup was done.

diskfull_notify.cmd

The diskfull_notify.cmd script runs on the NetBackup server that has the storage unit. The disk-media manager (bpdm) calls this script if it encounters a disk full condition when writing a backup to a disk type storage unit. The default action is to sleep five minutes and retry the write (file being written is kept open by the active bpdm).

You can modify the script to send a notification to someone or to perform actions such as removing other files in the affected directory or file system. NetBackup passes the following parameters to this script:

Parameter	Description
`programname`	Name of the program (always `bpdm`).
`pathname`	Path to the file being written.

For example:

```
diskfull_notify.cmd bpdm /disk1/images/host_08193531_c1_F1
```

restore_notify.cmd

The `restore_notify.cmd` script runs on the server that has the storage unit. The NetBackup tape or disk manager (`bptm` or `bpdm`) calls the script when it is finished sending data to the client during a restore (regardless of whether data is actually sent). NetBackup passes the following parameters to this script:

Parameter	Description
`programname`	Name of the program doing the restore or other read operation.
`pathname`	Path to the backup.
`operation`	One of the following: `restore`, `verify`, `duplication`, `import`

For example:

```
restore_notify.cmd bptm bilbo_0695316589 duplication
```

session_notify.cmd

The `session_notify.cmd` script runs on the master server and is called at the end of a backup session if at least one scheduled backup has succeeded. NetBackup passes no parameters to this script. The scheduler is suspended until this script completes, thus no other backups can start until that time.

session_start_notify.cmd

The `session_start_notify.cmd` script runs on the master server. When a set of backups is due to run, NetBackup calls this script to do any site specific processing prior to starting the first backup. NetBackup passes no parameters to this script.

userreq_notify.cmd

The `userreq_notify.cmd` script runs on the master server and is called by NetBackup each time a request is made to:

- List files that are in backups or archives
- Start a backup, archive, or restore

You can alter this script to gather information about user requests to NetBackup. NetBackup passes the following parameters to this script.

Parameter	Description
`action`	Defines the action and can have the following values: `backup`, `archive`, `manual_backup`, `restore`, `list`
`clientname`	Defines the client name.
`userid`	Defines the user ID.

For example:

```
userreq_notif.cmd backup mercury jdoe
userreq_notify.cmd archive mercury jdoe
userreq_notify.cmd manual_backup mercury jdoe
userreq_notify.cmd restore mercury jdoe
userreq_notify.cmd list mercury jdoe
```

Intelligent Disaster Recovery E

Intelligent Disaster Recovery (IDR) for Windows is a separately-priced option for NetBackup BusinesServer. IDR software is provided with your NetBackup BusinesServer software, but to use it you must purchase a license from VERITAS and activate it on the master server.

Intelligent Disaster Recovery (IDR) for Windows NT / 2000 / XP is a fully-automated disaster recovery solution that allows you to quickly and efficiently recover your Windows computers after a disaster. The IDR wizards guide you in preparing for disaster recovery and in recovering your computer to its pre-disaster state.

All information in this appendix applies to both Windows NT, Windows 2000, and Windows XP unless otherwise specified.

This appendix contains the following sections:

- “Requirements for IDR” explains the prerequisites for using IDR.
- “Overview of IDR Use” explains the main steps involved in using the disaster recovery software.
- “About the DR Files” introduces the DR (Disaster Recovery) files and explains their importance in disaster recovery.
- “Configuring NetBackup Policies for IDR” explains how to configure policies that contain clients that are using IDR.
- “Preparing the IDR Bootable Media” explains how to use this wizard to prepare the bootable media that is used to recover your data.
- “Updating IDR Media” explains how and when to update the IDR media so it is always ready when you need it.
- “Recovering Your Computer” explains how to perform disaster recovery.
- “Notes on Recovering Specific Platforms” provide information on recovering data on specific types of platforms.
- “IDR Frequently Asked Questions” answers questions that are frequently asked about IDR.

Supported Windows Editions

IDR allows you to recover the following Windows platforms:

- Windows NT 4.0 Enterprise Server, Small Business Server, and Workstation editions with Service Pack 3 or later
- Windows 2000 Server, Advanced Server, and Professional
- Windows XP 32-bit versions

Requirements for IDR

- NetBackup 4.5 or later must be installed on the NetBackup server and clients that you are going to protect.
- The Intelligent Disaster Recovery software is installed automatically when NetBackup server or client software for Windows is installed. The software is not required and cannot be installed on UNIX master servers. For NetBackup BusinesServer, you must activate the license on the master server.
- Intel platform running Windows NT 4.0 (with Service Pack 3 or later), Windows 2000, Windows XP.
- At least 40 MB of hard drive space to hold the minimal recovery system.
- Sufficient space for the data that is being restored.
- Sufficient swap space to support your system's RAM.

  For example, if you have 128 MB of RAM, the minimum swap used is 128 MB. For a 2 GB partition storing 1.8 GB of data, the required hard drive space for that partition is 1.8 GB plus 128 MB plus 40 MB, for a total of 1.97 GB.
- The partition on the first physical drive must be the boot partition and must also be labeled `c:\`.
- A protected computer must use a network card that does not require a Windows NT/2000/XP service pack to be installed in order to work. For a list of cards that have passed Microsoft compatibility tests without service packs, see the "Network LAN Adapters" section of the "Hardware Compatibility List" that comes with the Microsoft Windows software.
- The driver required by the CD-ROM on a protected computer must be supported by Windows in order to use Intelligent Disaster Recovery. A possible workaround is to choose **Use SCSI Drivers Currently installed on this system** when prompted by the IDR preparation wizard about the SCSI Drivers (assuming that the CD-ROM driver in question is a SCSI miniport driver).

Overview of IDR Use

Using IDR involves the following steps:

- Installation:

  The IDR software is installed automatically upon the installation of 3.4 and 4.5 NetBackup server or client software for Windows. In order for IDR to be activated for backups, you must enter an IDR license key on the master server.

  The IDR software is not required (and cannot be installed) on UNIX master servers. For NetBackup BusinesServer, you must activate the license on the master server.

  NetBackup 3.3 clients may require that IDR be installed.

- Configuration. On the NetBackup master server, select the **Collect disaster recovery information** general attribute when setting up the policy configuration for protected clients. This causes NetBackup to collect disaster recovery information.
- Preparing the bootable media. The IDR preparation wizard guides you through the preparation of bootable media used to recover protected systems.
- Backup. Back up your data files frequently.
- Recovery. A wizard guides you through the steps for restoring data to a protected system.

The installation, configuration, preparation, and backup steps are prerequisites for successfully recovering a Windows system through a network connection to a NetBackup server.

About the DR Files

The DR files are mentioned frequently in this appendix and in the screens that you see in the wizards. A DR (Disaster Recovery) file contains specific information about the computer you are protecting, including:

- Hard disk partition information
- Network interface card information
- NetBackup configuration information required to restore data files

To fully automate the recovery of an IDR-protected computer, you need a copy of the DR file for that computer. If IDR software is installed on the server and client, NetBackup creates a DR file and stores a copy on the client and the master server after every:

- Full backup
- Incremental (differential or cumulative) backup

- User backup
- User archive

NetBackup stores the DR file for each client in the *install_path*`\NetBackup\Idr\data` directory on the client. The DR files generated after a backup are named in the format *netbackup_client_name* `.dr`. For example, if the client name is bison, the DR file is `bison.dr`.

Note IDR requires that the DR file name match the computer name of the client. That is, if the computer name is recognized by the network as bison, then the DR file must be named `bison.dr`. If the NetBackup client name is different for some reason, you must manually rename a DR file created after each backup to *`computer_name`*`.dr` before you can use it in a recovery.

If a full backup has been performed for a client, you can also run *install_path*`\NetBackup\bin\drfile.exe` on the client itself to create or update the client's DR file. In this instance the name of the resultant DR file always matches the computer name of the client (which is the name required by IDR), even if this name happens to be different than the one used in the NetBackup policy configuration. For more information on this method, see "Using drfile.exe To Create or Update a DR File" on page 706.

On the master server, the DR files for all clients are stored in the NetBackup catalogs on the server. However, you can run the IDR preparation wizard on the master server, a media server, or a NetBackup administration client, and choose the option that places all client DR files in the server's *install_path*`\NetBackup\Idr\data directory`. This allows you to easily obtain the latest copy of a DR file if a client fails and you did not get the latest DR file prior to the failure.

Other sections of this appendix and the wizards provide more information on using the DR files.

Configuring NetBackup Policies for IDR

Set up the policy configuration on the NetBackup master server as follows:

- For NetBackup BusinesServer, activate the license on the master server.
- Ensure that each protected client is in an MS-Windows-NT type policy.
- Select the **Collect disaster recovery information** policy attribute for at least one of the MS-Windows-NT policies that are backing up protected clients.
  - If the master server is running Windows, ensure that the IDR license key is installed on that server. Otherwise, you cannot select the **Collect disaster recovery information** attribute.

- Ensure that all the clients in this policy have IDR installed. If a client in a policy that is collecting disaster recovery information does not have IDR installed, backups performed for that client by this policy will never end with a status of 0. A successful backup in this instance shows a status of 1 (partially successful). This is a result of NetBackup not finding a DR file to store in its catalog after each backup.

  By default, all 3.4 and 4.5 clients should have IDR installed. If there are 3.3 clients being protected, IDR may need to be installed on those clients.

- Ensure that the client names used in the NetBackup policy configuration match the client's computer name. If these names do not match, you must manually rename the DR file that is created after each backup to *computer_name* `.dr` before you can use it in a recovery.

Preparing the IDR Bootable Media

The IDR preparation wizard guides you in creating the bootable media required for recovering a Windows computer. To use this wizard, you must have:

- The Windows installation CD for the version and language installed on the protected system.
- Administrative privileges for the protected system.
- Your choice of the following media for Windows NT, Windows 2000, or Windows XP:
  - CD-R (CD Recordable CD-ROM)
  - CD-RW (CD Rewritable CD-ROM)
  - Diskettes (not supported by Windows XP)

  More information on media is provided later in this appendix.

You must prepare your bootable media before a disaster. For CD-R or CD-RW, also try booting from the media before a disaster occurs to ensure that your hardware can boot from it. (See "Step 1: Boot Your Computer" on page 707.)

If an IDR-protected NetBackup client is available, you can prepare IDR bootable diskettes on an emergency basis. However, if the DR files are not available, it may be necessary to manually repartition your hard drives, manually install networking, and manually submit the restore request.

Choosing the Bootable Media

For Windows NT/2000, the IDR preparation wizard, can create both bootable diskettes and bootable CD-Recordable (CR-R) or CD-Rewritable (CR-RW) media.

When choosing between diskettes and CD-ROM media, consider the type of Windows system or systems you are protecting, the available hardware, and your system BIOS.

- Diskettes work on most systems but require more time for preparation and recovery. The Windows NT/2000/XP installation CD is also required during recovery.
- Diskettes will hold SCSI driver information for only one computer (due to space limitations).

  This means you must pick a computer that represents the set of computers to be protected, then create the bootable media for that computer. This works fine but if you have a variety of driver configurations it means creating a set of diskettes for each variation.

  CD media has enough space to add SCSI driver information for multiple systems, so you can use a single CD for multiple systems during disaster recovery.

  With both diskettes and CDs, you must prepare separate media for each operating system level and language being used.
- CDs require less time for preparation and recovery than diskettes. However, they also need:
  - BIOS that supports booting from a CD
  - Third party CD writing hardware and software for writing ISO 9660 CD images

Creating Bootable Diskettes

If you select diskettes for the bootable media, you need four (for Windows NT) or five (for Windows 2000) blank, formatted 1.44 MB diskettes for each set of disaster recovery diskettes. You do not need a separate set of disaster recovery diskettes for each computer. However, a separate set is required for each version and language of Windows that is used.

Note Windows XP does not support bootable diskettes.

In each set:

- One is the diskette that contains the computer specific information that is necessary to perform an actual disaster recovery. This diskette is *created* by the IDR preparation wizard.
- The rest are Windows Setup diskettes. These are initially created by a utility that is on the Windows installation CD. IDR modifies these setup diskettes for use specifically with NetBackup for Windows.

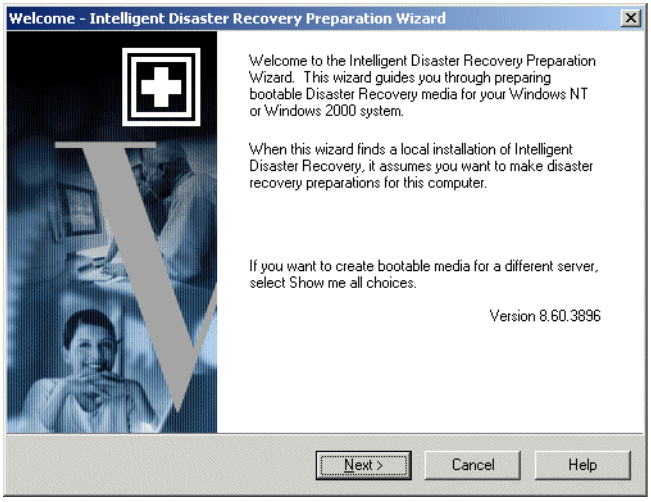
Note The Windows installation CD is needed both to prepare disaster recovery diskettes and for disaster recovery using those diskettes.

▼ To create bootable diskettes

1. Format the diskettes that you are going to use. (Windows NT requires four diskettes and Windows 2000 requires five. Windows XP does not support bootable diskettes.)

2. On the computer where you are going to prepare the diskettes, go to the *install_path*`\NetBackup\bin` folder and double-click `drprepwizard.exe` (*install_path* is `C:\Program Files\VERITAS` by default).

   The Welcome screen for the IDR preparation wizard appears.



3. Click **Next** to continue.

   The Create or Update IDR Boot Media screen appears.

4. Select **Diskettes to boot the Windows NT or Windows 2000 setup CD** and click **Next**.

   The Intelligent Disaster Recovery Preparation - Diskettes screen appears.

5. Read this screen and click **Next** to continue. The Create or Update IDR Boot Media screen appears.

6. Select **Yes** and click **Next** to continue. The Select Machine For Diskette Preparation screen appears.

7. Specify the name of the computer for which the disaster recovery diskettes are being created and click **Next**.

   The Enter Windows NT CD Path screen displays.

8. Place the Windows NT/2000 installation CD into the CD-ROM drive.

9. Enter the path of the install directory that is on the Windows installation CD (for example, `D:\i386`) and click **Next**.

The default path shown is the path from which you installed Windows on the computer where you are preparing the diskettes. To use a different path, click **Browse** and select a directory.

If you receive a message that an invalid path was specified, make sure the Windows installation CD is in the CD-ROM drive, and try again.

Note If you are creating the diskettes on a Windows NT computer perform step 10. If you are creating the diskettes on a Windows 2000 computer, proceed to step 11.

10. If you are on a Windows NT computer and entered the correct path in the previous step, the Windows NT Upgrade/Installation screen appears.

a. Click **Continue** and follow the Windows NT instructions for creating and labeling the setup diskettes.

b. During the SCSI device detection phase of this utility, if a SCSI driver version is detected on the selected computer that is different from the version on the Windows NT installation CD, you are prompted to use either the default SCSI drivers that are on the Windows NT installation CD or the SCSI drivers that are installed on the selected computer.

- If you are creating disaster recovery diskettes for multiple computers or for a computer other than the one you selected, select **Use Default SCSI drivers that are available on the inserted CD**.
- If you are creating disaster recovery diskettes for the selected computer, select the default, **Use SCSI Drivers currently installed on this system**. This option adds the drivers currently installed on the selected computer to the Setup diskettes.

Caution It is strongly recommended that you use the SCSI drivers currently installed on the computer being protected because the drivers contained on the Windows NT CD-ROM may not be up to date. If you have an IDE hard disk greater than eight GB you must select **Use SCSI Drivers currently installed on this system**.

After making your selection, click **Next** to continue.

c. You are now prompted to insert the Windows NT setup diskettes into the drive so information can be updated for the Disaster Recovery wizard. Insert them as prompted and click **Next**. After the last screen proceed to step 12.

11. If you are on a Windows 2000 computer and entered the correct path in the previous step, the Create Diskettes screen appears. Follow the prompts on this and subsequent Create Diskettes screens to create the Windows 2000 setup diskettes.

12. The last prompt tells you to label a blank formatted diskette as Intelligent Disaster Recovery Diskette, insert it into the drive, and click **Next**. Your next action depends on whether a DR file already exists on this computer:
    - If a DR file already exists on this computer, skip the remainder of this procedure because it does not apply. Instead, the wizard continues and updates the diskettes as explained in "Updating Disaster Recovery Diskettes" on page 704. Go to that procedure for more information.
    - If a DR file does not exist on this computer, when the IDR Preparation wizard has copied the necessary drivers and the Disaster Recovery wizard to this diskette, the Finished - Intelligent Disaster Recovery Preparation screen appears.

13. If there is still a diskette in drive A, remove it and store it with the rest of the disaster recovery diskettes.

14. Click **Finish**. The Disaster Recovery setup diskettes are now complete, except for adding the DR file.

15. Create a DR file for the target computer by running an initial full backup of the entire hard drive (not just the individual directories).

    If a full backup has already occurred, you can run the `drfile.exe` command to create a DR file without waiting for the next backup. (See "Using drfile.exe To Create or Update a DR File" on page 706 and "About the DR Files" on page 695.)

16. After the initial backup has been performed, run the IDR preparation wizard again to update the Disaster Recovery preparation diskettes with the DR file. (See "Updating Disaster Recovery Diskettes" on page 704.)

Creating a Bootable CD Image

The following are the requirements for using a bootable CD as your disaster recovery media:

- Computer(s) to be recovered must be able to boot from a CD.
- Writable (or re-writable) CD device.
- Third party software that will burn an ISO 9660 image.
- Windows NT/2000/XP installation CD. The Windows NT/2000/XP operating system version and language on this CD must match those on the computers being protected. If there is more than one operating system level or language, you must create a CD for each variation.

The IDR preparation wizard guides you through the creation of the CD image. You must use your CD writing system to burn a CD.

To recover your computer with the bootable CD, you need:

- The bootable CD
- The latest copy of the DR file for the computer (required for automated recovery)
- The latest backup images

▼ To create a bootable CD image

1. On the system where you are preparing the media, go to the *install_path*`\NetBackup\bin` folder and double-click `drprepwizard.exe` (*install_path* is `C:\Program Files\VERITAS` by default).

   The Welcome screen for the IDR preparation wizard appears.

2. Click **Next** to continue. The Intelligent Disaster Recovery Preparation Options screen appears.

3. Select **CD Image for use with CD Writers** and click **Next**.

   The Intelligent Disaster Recovery Preparation - Writable CD screen appears.

4. Read this screen and click **Next**. The Select Machine(s) to Protect screen appears.

5. Select the computers for which the bootable CD image is being created. The wizard will gather the SCSI driver information from these computers.

Note All computers selected must be running the same version of Windows NT / 2000 / XP.

6. Click **Next**. If there are different driver versions on the selected computers, the Driver Versions Do Not Match screen appears.

   a. Select which driver version is to be put into the bootable image. Options include:

      - First version found. Hardware installation diskettes may be required for the highlighted computers.
      - Latest date time stamp. The newest drivers may not work on older hardware.
      - Only drivers from Windows NT / 2000 / XP setup media. Hardware installation diskettes can be required for some computers.

   b. Click **Next**. The Select Location for CD Image screen appears.

7. Select the directory where the ISO 9660 CD image file is to be placed.

Note Most CD writer software requires that the image be placed on the same computer as the CD writer software to prevent data underrun problems during burn.

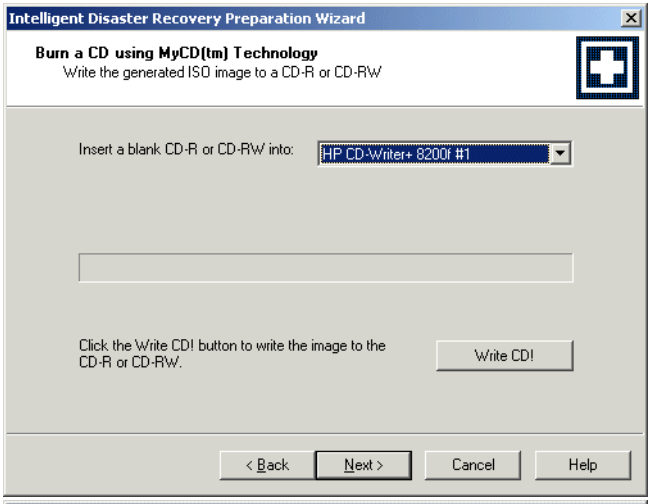
8. Click **Next**. The Windows NT Installation Media screen appears.

9. Insert the Windows NT installation CD and specify the drive.

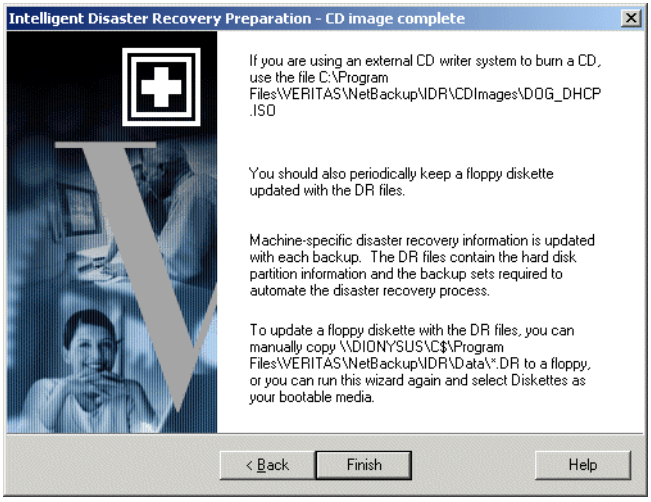
10. Click **Next**. The Creating Disaster Recovery Image screen appears. When the creation of the bootable image is complete, a Done status and a **Next** button appears.

11. Click **Next**. The Burn a CD using MyCD Technology screen appears.

    Click **Write CD!** to burn the CD or click **Next** to proceed to the next screen.



    If you click **Next**, the Intelligent Disaster Recovery Preparation - CD Image Complete screen appears.



12. Click **Finish**.

    If you did not burn a CD in the previous step, you must now use your CD writing system to burn a CD. Many popular CD-RW systems

ship with both Adaptec Direct CD and Easy CD Creator. Easy CD Creator handles ISO 9660 image files.

Caution Test your bootable CD to ensure that your system can boot from it. (See "Step 1: Boot Your Computer" on page 707.)

Updating IDR Media

Update your IDR media in the following instances:

- If your hardware configuration changes.
- If you are using bootable diskettes, update them after the first full backup that is performed after you created them. This is necessary to add the DR file. It is also recommended that you update them on a periodic basis in order to maintain the latest DR file.

Updating Disaster Recovery Diskettes

You can update disaster recovery diskettes with the latest DR file by using the IDR preparation wizard. If this is the first time the DR file has been created, use the wizard to ensure that all disks get updated that need to be updated.

If this is not the first time the DR file has been created, you may prefer to run `drfile.exe` from a command prompt and copy the DR file to the diskette. (See "Using drfile.exe To Create or Update a DR File" on page 706.)

The following explains how to use the wizard.

▼ To update diskettes by using the IDR Preparation Wizard

1. Start NetBackup.
2. Run a full backup of the target computer (or wait until NetBackup has completed a scheduled automatic backup).
3. Go to the *install_path*`\NetBackup\bin` folder and double-click `drprepwizard.exe` (*install_path* is `C:\Progam Files\VERITAS` by default).
4. Click **Next** in the **Welcome** screen. The Create or Update IDR Boot Media screen appears.
5. Select **Diskettes to boot the Windows NT or Windows 2000 setup CD** and click **Next**.

The Intelligent Disaster Recovery Preparation - Diskettes screen appears.

6. Click **Next**. The Create or Update IDR Boot Media screen appears.

7. Click **No, I want to update my existing diskettes**, then click **Next**. The Update Disks screen appears.

   This window displays the names of the computers that have had a DR file generated by NetBackup during a backup of the computer's hard disk.

8. Select the computer(s) whose DR file you want to store on this set of disaster recovery diskettes and click **Next**.

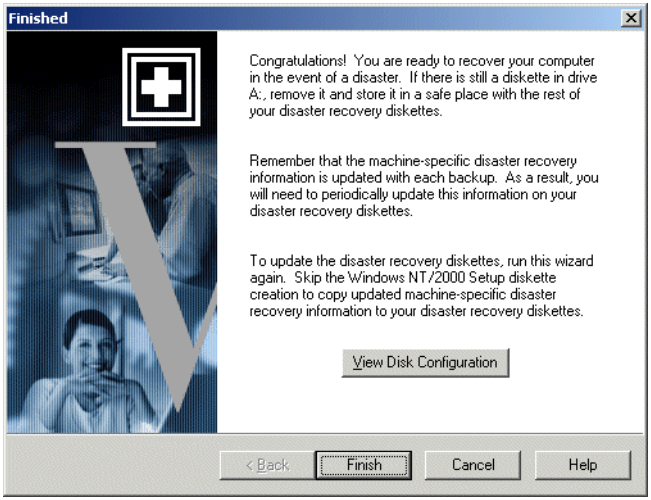
   The Create Diskettes screen displays.

9. Insert the Windows Setup boot disk and click **Next**. This diskette is updated and the Update Disk screen appears.

10. Insert the Intelligent Disaster Recovery diskette into drive A and click **Next**. The DR file(s) are written to the diskette.

Note You can store the DR files for all the protected computers on one diskette. You can also store the DR files on a diskette other than the Intelligent Disaster Recovery diskette. In this instance, insert the other diskette when prompted for the DR file during disaster recovery. When you are done, label the diskette and keep it with your set of disaster recovery diskettes.

When the writing is done, the Finished screen appears.



11. Click **Finish**.

    Disaster recovery preparation is now complete.

    For subsequent disaster recovery, you will need the disaster recovery diskettes, the Windows installation CD, and the latest backups on the NetBackup server.

Updating a Disaster Recovery CD

If you install a new SCSI card that is not supported by the Windows installation CD, create a new bootable CD as explained in the previous procedure, “Creating a Bootable CD Image” on page 701.

Using drfile.exe To Create or Update a DR File

If at least one full backup has been performed, you can run `drfile.exe` to create or update the DR file on your computer.

1. Go to the *install_path*`\NetBackup\bin` folder and double-click `drfile.exe` (*install_path* is `C:\Program Files\VERITAS` by default).

   This creates (or updates) the DR file that is located in the *install_path*`\NetBackup\Idr\Data` directory on your computer. Note that the `Data` directory must exist on the client or the `drfile.exe` command will fail.

   The DR file name is of the form *computer_name*`.dr` as in `bison.dr`. The name of the resultant DR file always matches the computer name of the client (which is the name required by IDR), even if this name happens to be different than the one used in the NetBackup policy configuration.

2. Insert the Intelligent Disaster Recovery diskette into your drive and copy the DR file to it or use the wizard as explained earlier.

Note You can also copy the DR file to a diskette other than the Intelligent Disaster Recovery diskette. In this instance, insert the other diskette when prompted for the DR file during disaster recovery.

Recovering Your Computer

Restoring the NetBackup client to its pre-disaster status with IDR includes the following steps:

- Booting the computer by using previously prepared IDR bootable media.
- On Windows NT, using the Windows NT Setup program and its **Express Setup** option to install a minimal version of Windows NT on the system. This step does not apply to Windows 2000.
- Using the NetBackup IDR Disaster Recovery wizard to restore your system to its pre-disaster state and restore your data files.

Step 1: Boot Your Computer

You can recover a Windows system by using the bootable diskettes or CD created during disaster preparation. The computer being recovered must have a storage device capable of booting from the bootable media.

Note If you have not previously prepared bootable media for a failed client, you can create bootable diskettes on an emergency basis as described in "Preparing Emergency IDR Bootable Diskettes" on page 712.

▼ To boot a computer using a bootable diskette

1. Insert the bootable diskette.
2. Follow screen instructions.

   You will need the Windows installation CD that was used during the preparation of the disaster recovery diskettes.

Note Windows 2000 will require you to log in prior to the time that the disaster recovery wizard appears. For this login, type administrator for the user name. A password is not required.

3. See "Step 2: Run Windows NT Setup (applies only to Windows NT)" on page 707 for additional steps.

▼ To boot from a bootable CD

1. Insert the bootable CD.
2. Follow screen instructions.

Note If you are testing your bootable media, do not continue when the magenta colored NetBackup Intelligent Disaster Recovery Bootstrap screen appears. Instead, remove the CD and press Escape.

3. Press Enter to begin the Windows NT Setup. (See "Step 2: Run Windows NT Setup (applies only to Windows NT)" on page 707 for additional steps.)

Step 2: Run Windows NT Setup (applies only to Windows NT)

Note This step does not apply to Windows 2000.

Windows NT Setup installs a minimal operating system and also can reformat or repartition your hard drive to prepare space for the recovery system. The Windows NT Setup process is similar for both bootable diskettes and CD.

▼ To use Windows NT setup

1. If using diskettes for the recovery:

   a. Replace the preparation diskettes as prompted.

   b. Place the Windows NT installation CD in the computer's CD-ROM drive when prompted, then press **Enter**.

2. When the Windows NT setup instructions appear, press Enter to choose **Express Setup**.

Note **Express Setup** is usually the best choice. Use **Custom Setup** if the following conditions exist:
- SCSI drivers are not present on the boot media.
- You have RAID hardware that needs to be reconfigured.

---

3. If a new hard drive is detected on your system, select a file system (FAT or NTFS) to format it, then press **Enter**.

Note When asked to create a partition on a replacement disk, be sure to select FAT format for the C drive. IDR cannot repartition to the old layout if you build the partition as NTFS.

---

4. Ensure no diskettes or CDs are in the drives and press Enter to reboot the system.

   After the reboot, the Disaster Recovery Wizard automatically starts.

Step 3: Run the Disaster Recovery Wizard

To fully automate the recovery with the Disaster Recovery wizard, you need:

- A NetBackup server that can restore the latest backups to the computer being recovered.
- The latest DR file for the machine you are recovering.

  If you booted from a bootable CD, the DR file on that media was created when you ran the IDR Preparation Wizard and can contain out-of-date hard disk partition, network-interface-card driver, or backup set information.

The DR file can also be out of date on bootable diskettes, unless you recently updated it.

The latest DR files (required to fully automate the recovery) are stored on both the client and on the NetBackup server that did the last backup. (See "About the DR Files" on page 695.) If necessary, you can copy either of these DR files to a diskette and use it for automated recovery. The other option is to not use a DR file and perform a manual recovery as explained in the procedure.

▼ To use the Disaster Recovery Wizard

1. When the wizard appears , insert the diskette that contains the latest DR file into drive A and click **Next**. If you do not intend to use a DR file, just click **Next**.

2. If you have a DR file, select the DR file for the computer you are recovering and click **Next.**

   The name of a DR file matches the computer for which it was created. For example, if the computer is named carrot look for a file named `carrot.dr`.

Note If you do not have a DR file, click **Next** anyway to proceed. A message stating that the recovery file was not selected appears. Click **Yes** to continue in manual mode.

3. For Windows NT (not Windows 2000), if your hard disk partition layout changed, the wizard prompts you to either replace the current hard drive partition with the partition information contained in the DR file or to keep the current hard drive partitions.

   a. The next wizard screen allows you to run the Windows NT Disk Administrator program. Disk Administrator allows you to make additional changes to your partition information, if necessary (for more information on Disk Administrator and fault tolerant configurations, refer to the Windows NT Server 4.0 Resource Kit).

   b. To make partition changes, click **Run Disk Administrator**. (See "Notes on Altering Hard Drive Partition Sizes" on page 712.) Otherwise, click **Next** to continue the recovery process.

4. Select either **Automatic Restore** or **Manual Restore**.

   - If you selected **Automatic Restore**, click **Finish** to complete the network installation and go to step 12 to continue the recovery.
   - On Windows NT, if you selected **Manual Restore**, select **Wired to the Network**, click **Next**, and proceed to step 5.

- On Windows 2000/XP, if you selected **Manual Restore**, a message box appears instructing you to manually configure the network connection. To do this, click the **Start** button on the Windows 2000/XP task bar and the **Network and Dial-Up Connections** command on the menu that appears. Then, select the Local Area Connection icon for your network card and configure the properties for that connection according to the requirements for your network. When the network connection is configured, click the **OK** button in the IDR message box and proceed to step 12.

5. To select your network adapter, do one of the following:
   - If your network adapter requires a manufacturer supplied setup diskette, click **Select from list**, then click **Have Disk**.
   - If your network adapter does not require a manufacturer supplied setup diskette, either click **Select from list** or **Start search**.

   A list of network adapters appears.

Note If your network adapter is not listed on the screen that appears, click **Select from list**, then click **Have Disk add an adapter to the Network Adapter List**. For automatic network installation to succeed, the Windows NT setup program must be able to recognize the network interface card being used.

6. The next screen lists the default network protocols. Select the networking protocols used on your network and click **Next**.

7. Windows NT is ready to install the networking components. Insert your Windows NT installation CD or the IDR bootable CD into the CD-ROM drive and click **Next** to continue.

Note If additional setup screens that specifically address your network interface card appear, follow the prompts.

8. If TCP/IP is selected as the network protocol, you are prompted to use DHCP. If you do not want to use DHCP, enter a TCP/IP number.

   The Windows NT Networking Installation dialog displays.

9. Click **Next** to start the network and complete the installation of the networking components.

10. Enter the name of the workgroup or domain for your computer and click **Next**.

Note VERITAS recommends that you enter the name of a temporary workgroup, rather than the name of a domain. When the recovery is complete, the system will be restored to its original workgroup or domain.

11. Click **Finish** to complete the network installation and continue with recovery.

12. Select either **Automatic** or **Manual**:
    - If you selected **Automatic**, click **Next** and proceed to step 13.
    - If you select **Manual**, click **Next** and proceed to step 14.

13. Select the server from which you want to restore files, then:

    a. Click **Start Restore** to submit the restore request to the selected server. You can view the progress of the restore after the server has acknowleged the request.

    b. After the restore is complete, the **Next** button becomes available. Click **Next** and proceed to step 15.

14. Select **Start NetBackup Interface** to start the NetBackup client interface.

    Using this interface, you can make changes to the NetBackup configuration and you also have more control over the restore. The following steps provide basic instructions. (See the *NetBackup User's Guide* for more information on using the interface.)

    a. Display a restore window and search the NetBackup server of your choice for files and folders to restore.

    b. Select the files and folders to restore.

    c. Submit the restore request. Before submitting the restore request, make sure that **Overwrite Existing Files** is checked. If it is not, the system may be in an unstable state upon restart.

    d. View the progress of the restore.

    When the restore is complete, close the progress viewer and the NetBackup client interface. If the restore is complete, the **Next** button is now available. Click **Next** and proceed to step 15.

15. Remove any diskettes from drive A and click **Finish** to reboot the computer.

Preparing Emergency IDR Bootable Diskettes

If you do not have IDR bootable diskettes for a protected client that has failed, you can prepare a set of diskettes on an emergency basis in either of the following ways:

- Run the IDR Preparation wizard on the server that has been backing up the client.
- Copy the failed client's DR file from the server to another similarly configured client. Then, run the IDR preparation wizard on the other client.

Note Either of the above methods creates a set of diskettes that will usually work on the client you are trying to recover. However, to increase your chances of successfully recovering a client, always prepare IDR bootable media in advance as explained in "Preparing the IDR Bootable Media" on page 697.

Notes on Altering Hard Drive Partition Sizes

Note This section applies only to Windows NT. Reformatting and repartitioning is not supported on Windows 2000/XP.

IDR defaults to restoring the hard drive partition to the same sizes they were before the disaster. There may be unused and unallocated space. If the hard drive in the target computer is larger than the hard drive that was in place before the disaster occurred, run Windows NT's Disk Administrator program (within the IDR Recovery Wizard) to alter the partition sizes to reflect the larger hard drive size.

An example of why you might want to resize your hard drive partitions: If the pre-disaster computer hardware contained a 4 GB hard drive with two 2 GB partitions, and you have replaced it with a 9 GB model, IDR (using the DR file) will rebuild the hard disk partition table using the partition information found on the original 4 GB hard drive. As a result, only 4 GB of space will be allocated on the new 9 GB hard drive, with a partition map consisting of two 2 GB partitions.

To include additional space, use the Disk Administrator program to repartition the hard drive. For information regarding and fault tolerant configurations, please refer to the Windows NT Server 4.0 Resource Kit.

Notes on Recovering Specific Platforms

Recovering the Dell PowerEdge 6100/200 with RAID

Note Although this section specifically deals with restoring a Dell system, the steps outlined can be used with any system requiring the use of third party drivers.

Recovering a Dell PowerEdge 6100/200 with RAID configuration is different than recovering a regular system with one hard drive.

In order to load Windows on this type of machine, you must manually load the PowerRaid II driver, which is not bundled with the Windows operating system.

After loading the PowerRaid II driver, you must manually load the Adaptec controller driver. Failure to follow these steps results in Windows not recognizing any hard drive partitions on the system.

▼ Use the Following Steps With Your IDR Recovery Diskette Set

1. When the Windows blue Setup screen appears after booting with the IDR boot diskette, press and hold down the **F6** key.

   Windows prompts for IDR diskette 2.

2. Insert IDR diskette 2 and press and hold the F6 key again.

   After loading additional drivers, a Setup screen appears, allowing you to specify additional devices.

3. Release the F6 key and press the **S** key.

4. Follow the on-screen instructions to load the PowerEdge RAID II controller software.

5. After loading the PowerEdge RAID software, press **S** again to specify loading another device.

6. Follow the on-screen instructions to load the Adaptec controller software next.

7. After loading both pieces of third party software, press Enter and proceed as normal to recover your system.

Recovering IBM Computers

If you are using an IBM computer and the drive containing the system's configuration information fails, you must reconfigure the system using the IBM Reference Diskette prior to running recovery.

Recovering Compaq Computers

If you are using a Compaq computer and the drive containing the System Configuration Partition fails, Intelligent Disaster Recovery will recreate the partition on the new hard disk; however, you must use the Compaq SmartStart utilities to update the system partition.

IDR Frequently Asked Questions

1. Can I restore boot managers such as System Commander or OS/2 Boot Manager with Intelligent Disaster Recovery for Windows?

   No, because boot managers usually are installed at a very low level that NetBackup cannot protect.

   For example, the OS/2 boot manager resides in its own hard drive partition that NetBackup cannot access. In fact, because of the many different boot managers on the market, an Intelligent Disaster Recovery restore may render your system unbootable, even though your operating system has been restored. In this case, re-installing the boot manager should fix the problem.

2. I ran a full backup of my system but when I run the IDR Preparation Wizard again, I don't see a disaster recovery file. What happened?

   For some reason, the DR file was not generated automatically. Generate it manually as explained in "Using drfile.exe To Create or Update a DR File" on page 706.

3. During recovery, the Windows install fails when attempting to load SCSI drivers. When creating the recovery diskettes, I picked **Use SCSI Drivers Currently installed on this system** when the IDR Preparation Wizard prompted me to choose drivers.

   It could be that Windows NT/2000/XP does not support your drivers. A possible solution is to run the IDR Preparation Wizard on another system in order to create a new set of recovery disks and this time when prompted to choose drivers, pick Use **Default SCSI drivers that are available on the inserted CD**.

4. Why does the recovery wizard keep complaining that one or more of my hard drives are smaller than the originals?

If this isn't actually the case, the reason may be because the minimal version of Windows NT/2000/XP that runs the recovery wizard has detected the hard drives in a different order than what was originally configured under the original version of Windows NT/2000/XP did.

Be sure that your hard drive and controller configuration matches the original configuration before a disaster occurs.

If the original configuration does not match, then to a certain extent, you can control the hard drive numbering scheme that Windows NT /2000/XP devises. The following chart lists the normal order that Windows NT/2000/XP uses to assign disk drive numbers. Keep in mind that this chart can change if third party drivers are used.

Windows NT/2000/XP Hard Drive Numbering Scheme

Primary IDE	Master Server Media Server
Secondary IDE	Master Server Media Server
SCSI Adapter 0 (In order of the lowest I/O port address)	SCSI ID 0 SCSI ID 1 ... SCSI ID 7 (or 15 is wide SCSI)
SCSI Adapter 1	SCSI ID 0 SCSI ID 1 ... SCSI ID 7 (or 15 is Wide SCSI)
SCSI Adapter *n*	SCSI ID 0 SCSI ID 1 ... SCSI ID 7 (or 15 is Wide SCSI)

Other types of mass storage controllers are usually seen as SCSI controllers by Windows.

Note On Windows NT (not Windows 2000), if you cannot get the IDR Recovery Wizard to properly detect the hard drive order, you can still manually set up hard drive partitions by using the Windows NT Disk Administrator option within the Disaster Recovery Wizard. After this is done, you can continue with automated restore of your backup media.

If you have drives greater than eight gigabytes and the recovery wizard reports them as being only eight gigabytes, you must create bootable diskettes with the option **Use SCSI drivers currently installed on this system**.

Using the Backup Exec Tape Reader Option F

With the Backup Exec Tape Reader for NetBackup option, NetBackup 4.5 can read Backup Exec media written by Backup Exec 7.0 and above, and convert on-disk catalogs of Backup Exec 7.3 and above to NetBackup catalogs.

NetBackup makes use of the Backup Exec engine to restore and catalog Backup Exec media. Backup Exec uses NetBackup Media Manager to mount and manage Backup Exec media. Backup Exec forwards all device-related requests to NetBackup Media Manager.

Once Backup Exec is upgraded to NetBackup, Backup Exec on-disk catalogs need to be converted to NetBackup catalogs. This enables Backup Exec files to be browsed and restored using the NetBackup restore interfaces. NetBackup image files (.f) are not created at catalog conversion time, but are obtained at run time when a Backup Exec image is browsed. To obtain the file list, NetBackup queries the Backup Exec catalogs. Once the Backup Exec files are selected for restore, the Backup Exec engine is made to perform the restore.

Note NetBackup stores the information / data on tape in tar format (when not using multiplexing) while Backup Exec stores the data in MTF format.

Determining if Your Configuration can Use the Backup Exec Tape Reader Option Effectively

- Are you upgrading to NetBackup 4.5 from Backup Exec 7.3 or later? The BE Tape Reader option can be used to convert on-disk Backup Exec catalogs of version 7.3 and later. The BE Tape Reader will not recognize a Backup Exec install version earlier than 7.3. (See “Backup Exec Tape Reader and Typical Backup Exec Installations” on page 719.)
- Are you currently using Backup Exec and backing up to hard disk? The BE Tape Reader option does not support using NetBackup to restore Backup Exec data that was backed up to hard disk.
- Is Backup Exec currently backing up to media and / or devices that are unsupported by NetBackup 4.5? See the NetBackup device support matrix at `www.support.veritas.com`

- Are you currently using Backup Exec to back up and restore any of the following data:
  - Windows NT 4.0
  - Windows 2000
  - UNIX
  - Netware
  - Exchange (5.5 and 2000)
  - SQL (6.5, 7.0 and 2000)

  Data backed up using some of the Backup Exec options or agents is not eligible for restore by NetBackup 4.5. For example, Backup Exec Oracle Agent.
- Are you currently restoring data from foreign media and/or MTF media written by an application other than Backup Exec NT 7.0 or above? For example: NT Backup Applet, Backup Exec for NetWare, ArcServe, and so forth. The BE Tape Reader option can only restore data written on media by Backup Exec NT 7.0 and above.
- Is Backup Exec currently backing up data using the RAIDirector or IBM ADSM options?

  Using the BE Tape Reader option, restoring from media previously created by Backup Exec's RAIDirector or IBM ADSM feature is not supported.

Installing the Backup Exec Tape Reader Option

The BE Tape Reader option allows NetBackup to restore or catalog data backed up by Backup Exec. The option is included with NetBackup 4.5.

The option must be installed on a NetBackup Windows NT 4.0 or Windows 2000 media server. The master server can be UNIX, Windows NT 4.0 or Windows 2000.

Uninstalling the BE Tape Reader option removes all Backup Exec application files but retains Backup Exec user data files. A fully functional Backup Exec cannot be installed over the version of Backup Exec provided with the Backup Exec Tape Reader for NetBackup option.

Note NetBackup and Backup Exec cannot coexist on the same system. Installing the BE Tape Reader option does not preserve a pre-existing Backup Exec installation.

Before Upgrading to NetBackup

Before upgrading to NetBackup, the Backup Exec user interface should be used to attach to all the clients which may be restored from Backup Exec backups. This includes NT/2000 machines which cannot be accessed by the user account under which the Backup Exec services are running, Netware machines, UNIX machines, the Exchange databases and mail boxes and SQL databases. Backup Exec will be able to restore file system backups to all those NT/2000 machines which can be accessed by the user account under which the Backup Exec services are running.

Before upgrading to NetBackup, back up and save the contents of the DATA directory, CATALOG directory and `pvl.mdb` (`pvl_sql.mdb` if applicable). These can be used later in case a normal version of Backup Exec is installed.

Obtain the location of the `pvl.mdb` (or `pvl_sql.mdb` if applicable) from the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Adamm\ODBC Driver Connection
String
```

Obtain the location of the DATA folder from the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup Exec\Engine\Misc\Data
Path
```

Obtain the location of the CATALOG folder from the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup
Exec\Engine\Misc\Catalog Path
```

Backup Exec Tape Reader and Typical Backup Exec Installations

Backup Exec installations of version 7.3 and later will be detected by the NetBackup install, and only their catalogs will be eligible for conversion. The NetBackup install will not detect Backup Exec versions earlier than 7.3. If the Backup Exec version is earlier than 7.3, it needs to be manually upgraded to Backup Exec 7.3 or later as indicated by Backup Exec documentation. Once Backup Exec is at 7.3 or later, rerun the NetBackup 4.5 custom install with the BE Tape Reader option enabled.

If NetBackup finds that Backup Exec 7.3 or later has been installed, the installation process defaults to the custom NetBackup installation dialog. Only the custom installation (not the typical installation) allows users to install the BE Tape Reader option.

The user can install Backup Exec remote agents on machines that may be restored from Backup Exec images. The user can either install remote agents on such machines at the time NetBackup is being installed with the BE Tape Reader option, or at a later point of time.

The user is allowed to install Backup Exec remote agents on machines only if the NetBackup install is running on a machine that has the BE Tape Reader option installed.

Note When the BE Tape Reader option is installed, it should be of the same locale as the NetBackup master and media servers. The existing Backup Exec installation should also be of the same locale as the NetBackup 4.5 to which it will be upgraded.

Differing locales between Backup Exec and NetBackup are not supported. The following configuration would not be supported, for example: One machine containing a Japanese Backup Exec installation, being upgraded to an English NetBackup 4.5 media or master server.

Note Before installing NetBackup with the BE Tape Reader option enabled, exit (close) the Backup Exec user interface.

Backup Exec Tape Reader Option and Complex Backup Exec Installations

The NetBackup installation process detects complex Backup Exec installations. Complex installations are those that include Network Storage Edition (NSE), Backup Exec installed with the SAN Shared Storage Option (SSO), or cluster-aware Backup Exec.

Upon installation of the BE Tape Reader option over a complex Backup Exec install, NetBackup informs the user to manually uninstall the complex Backup Exec install, retain the Backup Exec catalogs and Advanced Device and Media Management (ADAMM) database, and rerun the NetBackup installation with the BE Tape Reader option enabled.

Note It is necessary that the Backup Exec catalogs and ADAMM database be preserved when uninstalling Backup Exec. If the Backup Exec catalogs and the ADAMM database are not preserved while uninstalling Backup Exec, it is possible to install the BE Tape Reader option, but all the Backup Exec media need to be imported.

Once the BE Tape Reader option is installed on the necessary machines, only one such machine should refer to the Backup Exec catalogs and ADAMM database (Backup Exec catalogs for such complex installs are stored on one host). Only the media server that refers to the Backup Exec catalogs and ADAMM database can perform the restore operations on Backup Exec media.

In case Backup Exec media need to be restored from another NetBackup media server, the Backup Exec media must be imported on that media server.

Backup Exec Tape Reader Option Installation where Backup Exec is Not Present

The NetBackup install does not detect the presence of Backup Exec data files, in case Backup Exec is not installed.

If the BE Tape Reader option is installed on a machine containing Backup Exec catalogs and data files from a previous uninstall of Backup Exec, perform the steps in

Associating Backup Exec Catalogs and Data Files with NetBackup

In case NetBackup 4.5 is installed with the BE Tape Reader option on a machine which does not have Backup Exec currently installed, but does contain Backup Exec catalogs left over by a previous uninstall of Backup Exec, NetBackup needs to be associated with Backup Exec leftover catalogs and data files. The following methods may be used to accomplish this:

▼ To associate Backup Exec catalogs and data files with NetBackup

Leave the Backup Exec catalog and data files in the present location. Install the BE Tape Reader option and point the tape reader components to the data files:

1. Stop the Backup Exec services.

2. Change the registry:

   a. Set the registry value:
   `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup Exec\Engine\Misc\Catalog Path`
   to the location of the `CATALOG` directory.

   b. Set the registry value:
   `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup Exec\Engine\Misc\Data Path`
   to the location of the `DATA` directory.

   c. Set the registry value:
   `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Adamm\ODBC Driver Connection String`
   to point to `pvl.mdb` (or `pvl_sql.mdb` if applicable).

d. Set the registry value:
`HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup Exec\User Interface\Data Path Remote`
to point to the location of the `DATA` folder. The path to the DATA directory should be entered in UNC format. For example:
`\\ADAJ\C$\Program Files\VERITAS\Backup Exec\NT\Data`

3. Restart the Backup Exec services.

Move the original Backup Exec data files to the location where the tape reader components can find them.

1. Stop the Backup Exec services.

2. Copy and save `pvl.mdb` (`pvl_sql.mdb`, if applicable) and the entire contents of the `DATA` and `CATALOGS` folders into the corresponding BE Tape Reader folders. After BE Tape Reader option has been installed, the location `pvl.mdb` (or `pvl_sql.mdb` if applicable), `DATA` and `CATALOG` folders can be obtained as follows:

   a. The location of the `pvl.mdb` (or `pvl_sql.mdb` if applicable) can be obtained from the following registry value:
   `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Adamm\ODBC Driver Connection String`

   b. The location of the `DATA` folder can be obtained from the following registry value:
   `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup Exec\Engine\Misc\Data Path`

   c. The location of the `CATALOG` folder can be obtained from the following registry value: `HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\Backup Exec\Engine\Misc\Catalog Path`

3. Restart the Backup Exec services.

Backup Exec Tape Reader Option Install Examples

BE Tape Reader Option Installed Over Existing Backup Exec (7.3 or later)

The NetBackup installation defaults to the custom installation dialog. Exit (close) the Backup Exec user interface. Select the Backup Exec Tape Reader for NetBackup option and continue the installation.

Installing BE Tape Reader Option on a Host Not Having an Existing Backup Exec Installation

Select the custom installation. Select the Backup Exec Tape Reader for NetBackup option and continue installation. After the installation is over, if existing Backup Exec catalogs left over from a previous uninstall of Backup Exec need to be associated with NetBackup, see

BE Tape Reader Option in a Complex Backup Exec Configuration

In the following scenario, a complex Backup Exec configuration is being upgraded to consist of one NetBackup master and two NetBackup media servers:

The current configuration consists of three Backup Exec NSE servers:

- BE_Server_A
- BE_Server_B
- BE_Server_C

BE_Server_C is the NSE master on which the Backup Exec catalogs and the ADAMM database are stored.

Since the Backup Exec catalogs and `ADAMM` database are present on BE_Server_C, install the Backup Exec Tape Reader for NetBackup option on BE_Server_C.

The NetBackup installation, when run on any of the machines, warns the user that a complex installation has been detected and Backup Exec must be manually uninstalled. Manually uninstall Backup Exec from all three machines, however, the Backup Exec catalogs and `ADAMM` database must be preserved on BE_Server_C.

Run the NetBackup installation on BE_Server_C with the BE Tape Reader option enabled. Once the NetBackup installation is finished, the old Backup Exec catalogs and `ADAMM` database (from the previous uninstall of Backup Exec) must be associated with the Backup Exec Tape Reader for NetBackup components.

Uninstalling the Backup Exec Tape Reader Option

Once the Backup Exec Tape Reader for NetBackup option is installed, the user can uninstall Backup Exec, or both Backup Exec and NetBackup.

In case Backup Exec is being uninstalled as a result of a NetBackup uninstall, the NetBackup uninstall preserves the Backup Exec catalogs and data files.

▼ **To uninstall Backup Exec, but not NetBackup:**

1. Select **Start > Settings > Control Panel > Add/Remove Programs**.
2. Select Backup Exec to uninstall from the program list.

Converting Backup Exec Catalogs to NetBackup Catalogs

In order for NetBackup to restore Backup Exec backups, Backup Exec catalogs need to be converted to NetBackup catalogs.

Since NetBackup Media Manager manages Backup Exec media, Backup Exec media records should also be converted to NetBackup Media Manager records. The catalog converter utility (`beconv`) converts the Backup Exec on-disk catalogs to NetBackup image files and Backup Exec media records to NetBackup Media Manager records. `beconv` usage is described in Appendix A.

How beconv Updates the Media Manager Volume Database

Backup Exec media are converted only if an appropriate drive (robotic or standalone drive whose Media Manager media type matches the media type of the Backup Exec media) is available.

`beconv` tries to associate Backup Exec media with existing NetBackup media records, first on the basis of barcode and then on the basis of a globally unique identifier (GUID). It does so by comparing the barcode and GUID in the Backup Exec ADAMM database with entries in the Media Manager volume database. It is therefore recommended that in case Backup Exec media are barcoded, a NetBackup inventory update be performed on the robot in which the Backup Exec media are present. This updates the Media Manager volume database with the barcodes of the Backup Exec media, thus enabling `beconv` to associate Backup Exec media records with existing records in the Media Manager volume database.

For a particular Backup Exec media, `beconv` builds a Media Manager volume database host list (in which to search for barcodes and GUIDs) based upon the Backup Exec media type as specified in the Backup Exec ADAMM database. `beconv` builds a list of all locally configured drives, whose base drive type matches the Backup Exec media type of the media. For each drive, the Media Manager volume database of the robot to which it belongs (or the Media Manager standalone drive volume database, if the drive is standalone) is added to the list.

If for a Backup Exec media, no match based upon the barcode or GUID is found in any of the Media Manager volume databases, `beconv` adds records to the NetBackup Media Manager volume database on the basis of Backup Exec `ADAMM` database information.

For robotic Backup Exec media, in case there is conflicting media residence information between the Backup Exec ADAMM database and Media Manager volume database, the Media Manager volume database information takes precedence (if the `-tbs` command line option to `beconv` is not specified)

For example: The Backup Exec ADAMM database says that Backup Exec media *BE-Media* is in slot 5 of Backup Exec robot Exabyte-210. Backup Exec robot Exabyte-210 corresponds to Media Manager robot 0. The Media Manager volume database of robot 0 (on host whale) contains a media record A00000 belonging to slot 5 of robot 0.

If a barcode or GUID match for *BE-Media* could not be found (and `-tbs` is not specified), `beconv` would create a non robotic record in the Media Manager volume database of whale corresponding to Backup Exec media *BE-Media*.

If there was no record in the Media Manager volume database on host whale belonging to slot 5 of robot 0, `beconv` would create a robotic record in the Media Manager volume database on whale belonging to slot 5 of robot 0, which would correspond to *BE-Media*.

If the `-tbs` command line option is specified, `beconv` will associate robotic Backup Exec media records with existing Media Manager volume database records by comparing the slot information from the Backup Exec ADAMM database with the slot information in the Media Manager volume database.

For example: The Backup Exec ADAMM database says that Backup Exec media *BE-Media* is in slot 5 of Backup Exec robot Exabyte-210. Backup Exec robot Exabyte-210 corresponds to Media Manager robot 0. The Media Manager volume database of robot 0 (on host whale) contains a media record A00000 belonging to slot 5 of robot 0.

If a barcode or GUID match for *BE-Media* could not be found and `-tbs` is specified, `beconv` would associate Backup Exec media *BE-Media* with the Media Manager record A00000.

Note The `-tbs` option should only be specified when the Backup Exec ADAMM database is up-to-date, and a NetBackup inventory update has been done on the robot which contains the Backup Exec media. If the Backup Exec ADAMM database is not up-to-date, Backup Exec media will get associated with wrong Media Manager records, and the wrong media will get mounted at the time of restoring Backup Exec images.

The `-tbs` option is useful when the Backup Exec media are not barcoded and the ADAMM database is up-to-date. The advantage of `-tbs` is that the standard NetBackup robot inventory update can be used to create Media Manager records, and those records can then be associated with Backup Exec media records (as opposed to `beconv` creating Media Manager records corresponding to Backup Exec media, when `-tbs` is not specified).

For non robotic Backup Exec media, the Media Manager volume database in which the corresponding record will be created is decided on the basis of the matching configured Media Manager drive.

`beconv` compares the media type of the Backup Exec media with the drive type of all the standalone Media Manager drives. If a match is found `beconv` creates a corresponding Media Manager record in the standalone drive volume database. In case no match is found `beconv` compares the media type of the Backup Exec media with the drive type of all the robotic Media Manager drives. If a match is found, `beconv` adds a non robotic Media Manager record in the Media Manager volume database of the robot whose drives drive type had matched the Backup Exec media type.

Each Media Manager record that corresponds to Backup Exec media will have the ADAMM_GUID field updated with the GUID obtained from the Backup Exec database. The description field will contain the cartridge label of the Backup Exec media. The media will be assigned to NetBackup (if not already assigned), and its state will be set to FROZEN in the NetBackup media database. NetBackup image files are generated (if not already present) for the converted Backup Exec media.

Whenever new records are added to the Media Manager volume database, the media type of the record added depends upon the drive type of the drive that was associated with the Backup Exec media. In case there are multiple drives having the same basic type as the Backup Exec media type, the media type of the newly added record is determined based upon entries in the Media Manager configuration file, vm.conf, or the drive index.

For example: Backup Exec media having Backup Exec media type DLT needs to be added in slot 5 of Media Manager robot 0. If robot 0 has 2 drives configured, as DLT2 and DLT3, the media type of the added record will be determined based upon the vm.conf entries. If the vm.conf maps Backup Exec DLT type to DLT2 type for robot 0, the media type of the added record will be DLT2. In case there are no vm.conf entries corresponding to Backup Exec DLT for robot 0, the media type of the newly added record will be determined by the drive type of the drive (of robot 0) having the lowest drive index.

For all new media records added to the Media Manager volume database, the default media id prefix for Backup Exec media is *BE*. This behavior can be overridden by specifying the MEDIA_ID_PREFIX configuration entry in the `vm.conf` file.

Note If more than one Media Manager volume database is in use, this configuration entry must be set with a unique media id prefix for each of the Media Manager volume databases.

The volume pool of the unassigned Media Manager records associated with Backup Exec media will be changed to the *BackupExec* pool. If the *BackupExec* pool is not present, it is automatically created.

Note `beconv` will not be able to update the Media Manager volume database correctly when the Media Manager volume database is changed while `beconv` is running. This can happen when existing NetBackup commands, which update the database, are run while `beconv` is running.

`beconv` will always ask for confirmation before modifying the Media Manager volume database or creating NetBackup catalogs.

`beconv` can be run to:

- Convert all Backup Exec media
- Convert Backup Exec media in a specific robot
- Convert a single piece or a group of Backup Exec media
- Check database consistency for duplicate media ids or globally unique identifiers (GUIDs)
- Display the Backup Exec to NetBackup robot mappings

Note Before running `beconv`, the appropriate robots and drives should be configured. Use the Device Configuration Wizard or another device configuration interface in NetBackup. On UNIX media servers, refer to the *NetBackup Media Manager Device Configuration Guide* to configure devices on the relevant operating system before configuring them for use with NetBackup. On Windows media servers, ensure that the appropriate tape driver is loaded.

Converting All Media

In order to convert all Backup Exec catalogs to NetBackup catalogs use the `beconv -all` option.

The `-all` option should not be specified in case only some Backup Exec catalogs need to be converted. beconv can take a long time to run in case many Backup Exec catalogs are present.

The `-all` option can be used with the `-tbs` option.

Converting Media in a Specific Robot

In case media need to be converted for a specific robot, use `-rn` *robot_number*. *robot_number* should be the Media Manager robot number corresponding to the Backup Exec robot whose media needs to be converted.

If the media in the robot are barcoded, it is recommended that a NetBackup inventory update be done on the robot.

In case the media are not barcoded and the Backup Exec ADAMM database is up-to-date, the user can still perform a NetBackup inventory update and run `beconv` with the `-tbs` option. The `-tbs` option associates Backup Exec media records with Media Manager volume records on the basis of the slot information.

Converting a Single Piece of Media or a Group of Media

In case a single media or a family of Backup Exec media need to be converted, `beconv` can be run with the `-m` *media_id* or the `-m` *media_id* `-f` option. The `-f` option converts the catalogs of all the media belonging to the family of Backup Exec media specified by *media_id*.

media_id is the Media Manager media id of the Backup Exec media. In order to use `beconv` with the `-m` option, a record must exist in the Media Manager volume database that corresponds to the Backup Exec media. The ADAMM_GUID field of the Media Manager volume database should contain the GUID of the Backup Exec media. This can be achieved as follows:

A Media Manager record needs to be created corresponding to that media (using either `vmadd` or a NetBackup robot inventory). `bephyinv` can then be run with the `-m` *media_id* option, where *media_id* is the Media Manager media id just created. `bephyinv` mounts the media, reads the tape header and updates the ADAMM_GUID field of the media record corresponding to *media_id* in the Media Manager volume database.

After running `bephyinv`, `beconv` can be run with the `-m` *media_id* option where *media_id* is the Media Manager media id just created.

Note It was necessary to run `bephyinv` in order to update the ADAMM_GUID field in the Media Manager volume database with the GUID of the Backup Exec media. Once that has been done, either using `bephyinv` or by an earlier run of `beconv`, it is not necessary to run `bephyinv` again.

For example: The user upgrades an existing Backup Exec installation to NetBackup 4.5. The first time the user runs `beconv -all`, all Backup Exec catalogs are converted to NetBackup catalogs. After some time the NetBackup images corresponding to the Backup Exec media expire, and catalogs need to be generated again for a specific media. If a media id corresponding to the Backup Exec media is already present in the Media Manager volume database (generated by the initial run of `beconv`), and the ADAMM_GUID field contains the GUID of the Backup Exec media, `bephyinv` does not need to be run. `beconv -m` *media_id* should convert catalogs for the Backup Exec media corresponding to *media_id*.

Using beconv with the -auto_correct Option

`beconv` tries to associate Backup Exec media records with Media Manager volume records on the basis of barcode and GUID information. There may be situations where the barcode of a Backup Exec media matches with one Media Manager record, and the GUID of the same Backup Exec media matches with another Media Manager record. In such situations, `beconv` will detect the inconsistency and report it to the user. `beconv` will prompt the user to run `beconv` with the `auto_correct` option for `beconv` to correct the inconsistency.

If the `-auto_correct` option is specified, and `beconv` detects the inconsistency described above, `beconv` unassigns the Media Manager volume record whose GUID corresponds to the Backup Exec media and updates the ADAMM_GUID field of the Media Manager record whose barcode matches the barcode of the Backup Exec media.

If the `-auto_correct` option were not specified, `beconv` would have reported the inconsistency to the user.

Note If `-auto_correct` is not specified, `beconv` will never unassign Media Manager volume records.

For example: The Backup Exec ADAMM database that is not up-to-date says that Backup Exec media *BE-Media* is in slot 5 of Backup Exec robot Exabyte-210. Backup Exec media *BE-Media* has GUID *ABC* and barcode *EFG*. Backup Exec robot Exabyte-210 corresponds to Media Manager robot 0. The Media Manager volume database for robot 0 (on host whale) does not contain a record belonging to slot 5 of robot 0. Actually the Backup Exec media *BE-Media* is in slot 6 of robot 0 (the Backup Exec ADAMM database and the robotic library contents are out of sync).

The user does not perform a NetBackup inventory update of robot 0. The user runs `beconv -all`. Since the NetBackup robot inventory update was not done, `beconv` will not find a barcode match for Backup Exec media *BE-Media*. Since this is the first time `beconv` is being run and `bephyinv` was not run, `beconv` will not find a GUID match either. `beconv` will create a robotic record A00000 in the Media Manager volume database on host whale belonging to slot 5 of robot 0, corresponding to *BE-Media*. The ADAMM_GUID field of A00000 just created will have the value *ABC*.

The user now runs a NetBackup inventory update on robot 0. The NetBackup robot inventory update creates a media record EFG001 in slot 6 having barcode *EFG*. This record actually corresponds to the Backup Exec media *BE-Media*. The user now runs `beconv` –all. `beconv` will find that the ADAMM_GUID field of Media Manager record A00000 matches with the GUID of *BE-Media* but the barcode of EFG001 matches with the barcode of “BE-Media”. `beconv` will report the inconsistency to the user and suggest that `beconv` be run with the `-auto_correct` option.

If `beconv_-all -auto_correct` is now run, `beconv` will unassign A00000 if required, change the ADAMM_GUID of Media Manager record A00000 from “ABC” to NULL and change the ADAMM_GUID field of EFG001 to “ABC”.

Using beconv with the Show_mappings Option

Note Catalogs are not converted when `-show_mappings` is specified.

`beconv -show_mappings` displays the mapping of Backup Exec robots to NetBackup robots. If any of the mappings are found to be incorrect, corrective action, such as adding entries in the vm.conf file, can be taken.

The mapping between Backup Exec robots and NetBackup robots is done on the basis of:

- The serial number, if the robot is serialized.
- The robot mapping entry specified in the vm.conf file, if the robot is not serialized.
- The inquiry string of the robot, if the robot is not serialized and there is no entry present in the vm.conf file.

Using beconv with the -check_consistency Option

Note Catalogs are not converted when `-check_consistency` option is specified.

`beconv` when invoked with the `-check_consistency` option examines the Media Manager volume databases of locally configured drives. If duplicate media ids or GUIDs are found in different Media Manager volume databases, the list of the Media Manager records containing the duplicate media ids or GUIDs is displayed to the user.

The following is an example of a situation where an inconsistency may arise:

Backup Exec server (whale) is being upgraded to a NetBackup master server. Attached to whale are two robots BE_Changer1 and BE_Changer2, both without barcode readers. After upgrading to NetBackup, Media Manager robots are configured such that BE_Changer1 corresponds to robot number 0 and BE_Changer1 corresponds to robot number 1. Robot 0 and robot 1 are configured such that the Media Manager volume database host of robot 0 is A and the Media Manager volume database host of robot 1 is B.

After running a NetBackup inventory update on robot 0 and robot 1, the Media Manager volume databases on hosts A and B will contain the following records:

Media Manager volume database on host A

Media Id	Robot Number
A00000	0
A00001	0
A00002	0

Media Manager volume database on host B

Media Id	Robot Number
A00000	1
A00001	1
A00002	1

The above case, where the same media ids are present in different Media Manager volume databases of robots attached to the same host, is not a correct configuration. `beconv`, when run with the `-check_consistency` option will detect such inconsistencies and report them to the user.

`beconv` when run with the `-check_consistency` option will also detect cases where the same GUIDs are present in different Media Manager volume databases. In the configuration below, the same GUIDs are present for different media ids in volume databases on different Media Manager hosts.

Media Manager volume database on host A:

Media Manager volume database on host A

Media Id	GUID
A00000	ABC
A00001	EFG

Media Manager volume database on host A

Media Id	GUID
A00002	KLM

Media Manager volume database on host B

Media Id	GUID
B00000	ABC
B00001	EFG
B00002	KLM

`beconv` will detect the inconsistent configuration above and report the inconsistency to the user.

Importing Uncataloged Backup Exec Media Using NetBackup

NetBackup can be used to import fresh Backup Exec media (Backup Exec media which are not known to Backup Exec) only if the Backup Exec Tape Reader for NetBackup option is installed. Importing a Backup Exec media involves two main operations:

- Making the fresh Backup Exec media known to Backup Exec and NetBackup.
- Generating Backup Exec catalogs and then converting them to NetBackup catalogs.

Making Fresh Backup Exec Media Known to Backup Exec and NetBackup

Use `bephyinv` on the Backup Exec media to make fresh Backup Exec media known to Backup Exec and NetBackup.

A Media Manager record needs to be created corresponding to that media (using either vmadd or a NetBackup robot inventory). `bephyinv` can then be run with the `-m` *media_id* option, where *media_id* is the Media Manager media id just created. `bephyinv` will mount the media, read the tape header and update the ADAMM_GUID field in the Media Manager volume database.

Generating and Converting Backup Exec Catalogs to NetBackup Catalogs

Once `bephyinv` has been run, Backup Exec catalog generation and the subsequent conversion of Backup Exec catalogs to NetBackup catalogs can be performed by running `bpimport -create_db_info -id` *media_id*, where *media_id* is the Media Manager media id specified when running `bephyinv` in the previous step.

Once the Backup Exec on-disk catalogs are generated successfully, `bpimport` internally calls `beconv` to convert the Backup Exec catalogs to NetBackup catalogs. The operations involved (generation of Backup Exec catalogs and their conversion to NetBackup catalogs) when importing Backup Exec media are shown in the following progress log.

Progress Log:

```
Import phase 1 started 07/16/01 18:16:54
18:16:54 INF - Create DB information for media id BE0000.
18:16:54 INF - Initiation of bptm process to read media id BE0000 was
successful.
18:16:54 INF - Waiting for mount of media id BE0000 on server SHARK.
18:17:16 INF - Backup Exec catalog generation started successfully.
18:17:59 INF - Backup Exec catalog generation completed successfully.
18:17:59 INF - Starting catalog conversion...
18:17:59 INF - Catalog conversion completed successfully.
```

Importing Backup Exec Media Belonging to a Spanned Set Where all the Media Belonging to the Spanned Set are Present

In case Backup Exec media belonging to a spanned set need to be imported, `bephyinv` needs to be first run for each of the Backup Exec media belonging to the spanned set. After running `bephyinv` for each of the Backup Exec media, `bpimport` should be run for each of the Backup Exec media belonging to the spanned set. The order in which `bephyinv` or `bpimport` is run for each of the media does not matter.

For example: Three Backup Exec media *BE-Media1*, *BE-Media2*, and *BE-Media3*, belonging to spanned media set need to be imported through NetBackup. `bephyinv` should first be run for each of the media *BE-Media1*, *BE-Media2*, and *BE-Media3*. After that `bpimport` should be run for each of the media *BE-Media1*, *BE-Media2*, and *BE-Media3*. It does not

matter whether `bpimport` is first run on *BE-Media3* or on *BE-Media1*. It is however necessary that `bephyinv` be run on all the media, and then `bpimport` be run on all the media.

Importing Backup Exec Media Belonging to a Spanned Set Where all the Media Belonging to the Spanned Set are not Present

In case all the Backup Exec media belonging to a spanned set are not present, `bephyinv` needs to be first run for each of the available Backup Exec media belonging to the spanned set. After running `bephyinv` for each of the available Backup Exec media, `bpimport` should be run for each of the available Backup Exec media belonging to the spanned set. The order in which `bephyinv` or `bpimport` is run for each of the media does not matter. After running `bpimport` for each of the available media belonging to the spanned set, `beconv` should be run with the `-m` *media_id* `-f` option, where *media_id* should be the Media Manager media id of any of the Backup Exec media belonging to the spanned set.

Updating the Media Manager Volume Database with Respect to Backup Exec Media

When to Run bephyinv

`bephyinv` can be used to update the Media Manager volume database with respect to Backup Exec media. This may need to be done when catalogs need to be converted for a single Backup Exec media, when fresh Backup Exec media need to be imported or when Backup Exec media are misplaced and the Media Manager volume database does not reflect the physical locations of Backup Exec media. `bephyinv` usage is described in Appendix A.

How bephyinv Works

The list of media on which `bephyinv` operates can be specified by any of the following:

- Media Manager Robot number
- Media Manager Robot number and range of slots
- Media Manager Volume pool
- Media Manager Volume group

- Media Manager Media ID

It is necessary that the Media Manager volume records be present when calling `bephyinv` with the corresponding option. For example, if `bephyinv` is called with the `-rn` *robot_number* parameter, there should be Media Manager records corresponding to Media Manager robot_number in the Media Manager volume database corresponding to robot_number.

`bephyinv` mounts each of the media specified by the above criterion and reads the tape header. If `bephyinv` discovers that the media is not Backup Exec media, the media is unmounted and the next media is mounted.

If the media is Backup Exec media, `bephyinv` obtains the Backup Exec GUID from the tape header and searches the Media Manager volume database to see if the GUID is present in the ADAMM_GUID field of any of the records of the Media Manager volume database. If the GUID is present in the Media Manager volume database, the Media Manager record having the GUID will be updated accordingly. In case the GUID read off the tape header is not present in any of the records of the Media Manager volume database, `bephyinv` will create a new Media Manager record corresponding to the Backup Exec media.

For each Media Manager record (added or updated) corresponding to the Backup Exec media, `bephyinv` will update the ADAMM_GUID field with the GUID obtained from the tape header and the Description field with the Backup Exec Cartridge Label read off the tape header. Each record will be assigned to NetBackup (if not already assigned) and its state will be set to FROZEN in the NetBackup media database of the local host. (Each NetBackup master or media server has a media database that is distinctly separate from the Media Manager volume database.)

The volume pool of the unassigned Media Manager volume records associated with Backup Exec media will be changed to the “BackupExec” pool. If the “BackupExec” pool is not present, it is automatically created.

`bephyinv` makes decisions on when and how to modify Media Manager records based upon the following principles:

- `bephyinv` changes the residence and description of any Media Manager record if required, regardless of whether it is assigned or not.
- If `-auto_correct` is not specified, `bephyinv` never changes the volume pool, media type, and ADAMM_GUID of an assigned record. `bephyinv` never unassigns an assigned Media Manager record if `-auto_correct` is not specified.
- If `-auto_correct` is specified, `bephyinv`, only if found necessary, may unassign an assigned Media Manager record so that the pool, media type or ADAMM_GUID may be changed.

`bephyinv` reports inconsistencies in the following situations:

- Whenever `bephyinv` finds that an assigned Media Manager record needs to be unassigned.
- Whenever the media type of an assigned Media Manager record needs to be changed.
- Whenever the GUID of an assigned Media Manager record needs to be changed.

When `bephyinv` finds an inconsistency, `bephyinv` displays the inconsistency to the user (provided `-auto_correct` was not specified). The user can either manually resolve the inconsistency, or run `bephyinv` with the `-auto_correct` option.

Note Running `bephyinv -auto_correct` may unassign Media Manager records and could lead to loss of data.

behyinv will always ask for confirmation before modifying the Media Manager volume database.

When bephyinv is Unable to Update the Media Manager Volume Database Correctly

There may be cases during which `bephyinv` is unable to update the Media Manager volume database correctly. `bephyinv` operates under the assumption that if a media has been mounted, the location where the media was mounted is the same as that indicated by the Media Manager record used to issue the mount.

Example:

In this example, host tumbleweed contains two robots, Robot 0 and Robot 1 whose Media Manager volume database hosts are A and B respectively. If the user runs the following:

```
bephyinv -m A00000 -h A
```

Media Manager volume database on hosts A and B

	Volume Database on A	Volume Database on B
Media Id	A00000	A00000
Robot Number	1	1
Robot Slot	5	6

It is possible that the media, which gets mounted by Media Manager, is the media specified by media id A00000 from Media Manager volume database B.

`bephyinv` would then operate as if media id A00000 had been mounted in slot 5, while it was actually mounted in slot 6. This may cause `bephyinv` to make incorrect decisions and update wrong Media Manager records with incorrect values.

Such problems can arise when multiple media ids are present in different Media Manager volume databases. Running `beconv -check_consistency` tells the user which Media Manager volume databases associated with locally configured drives have the same media ids present in them. **These problems can be avoided by centrally tracking all volumes in a single volume database, for example, on the NetBackup master server.**

Another case where `bephyinv` will not be able to update the Media Manager volume database correctly is when the Media Manager volume database has been changed while `bephyinv` has been running. This can happen when existing NetBackup commands, which update the Media Manager volume database, are run while `bephyinv` is running.

Running bephyinv for a Single Piece of Media

In case a single Backup Exec media needs to be physically inventoried, a corresponding Media Manager record needs to be added either using vmadd or the NetBackup robot inventory update.

The newly added record should correctly reflect the location of the Backup Exec media. Once the Media Manager record has been added, `bephyinv` can be run with the `-m` *media_id* `-h` *voldb_host* option where *media_id* is the media id of the Media Manager record which was just added and *voldb_host* is the Media Manager volume database host in which the Media Manager record was added.

Note For Backup Exec media in standalone drives, if the GUID on the tape header is not present in the ADAMM_GUID field of the corresponding Media Manager record which is being mounted, the mount request will have to be manually assigned using either vmoprcmd or the Device Monitor.

Examples

The user runs the following:

```
bephyinv -m A00000 -h tumbleweed
```

If media id A00000 is not present in the Media Manager volume database of host tumbleweed, `bephyinv` exits.

If media id A00000 is present in the Media Manager volume database of tumbleweed, `bephyinv` mounts media id A00000 and reads the tape header. In case the media mounted by media id A00000 is not a Backup Exec media, the media is unmounted and `bephyinv` exits.

If the media was a Backup Exec media, and the GUID and cartridge label read from the tape header was the following:

```
GUID: AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Cartridge label: "Backup Exec media"
```

`bephyinv` queries the Media Manager volume database on host tumbleweed for the GUID:

```
AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB.
```

The examples below show how `bephyinv` updates the Media Manager volume database of host tumbleweed, depending upon the initial state of the database.

Example 1

Media Manager volume database of host Tumbleweed:

	Volume Database on A	Volume Database on B
Media Id	A00000	A00000
Robot Number	1	1
Robot Slot	5	5
ADAMM_GUID	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	---	Backup Exec media
Volume Pool	test_pool	BackupExec
Assigned	---	06/16/2001 01:24:59 PM

`bephyinv` finds that in the Media Manager volume database of tumbleweed, media id A00000 has ADAMM_GUID AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB. Since the ADAMM_GUID is unique in the Media Manager volume database, there can be no other record in the Media Manager volume database of host tumbleweed having ADAMM_GUID: AAAAAAAA-1234-1234-1234 BBBBBBBBBBBB.

Since the mounted media id A00000, has the ADAMM_GUID: AAAAAAAA-1234-1234-1234 BBBBBBBBBBBB on its tape header, and the Media Manager volume database also shows that media id A00000 has the ADAMM_GUID: AAAAAAAA-1234-1234-1234 BBBBBBBBBBBB, this means that the Media Manager volume database is up-to-date with respect to the ADAMM_GUID.

`bephyinv` then changes the media description of media id A00000 to the Cartridge Label read off the tape header: *Backup Exec media*. `bephyinv` assigns the media to NetBackup, and sets its state as FROZEN in the NetBackup media database of host tumbleweed. Doing so ensures that NetBackup will never mount this media for NetBackup backups.

Refer to the table above to see how the Media Manager volume database changes after running `bephyinv`.

Example 2

Media Manager volume database of host Tumbleweed:

	Before running bephyinv	After running bephyinv
Media Id	A00000	A00000
Robot Number	1	1
Robot Slot	5	5
ADAMM_GUID	---	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	---	Backup Exec media
Volume Pool	test_pool	BackupExec
Assigned	---	06/16/2001 01:24:59 PM

No media record in the Media Manager volume database of tubleweed has the ADAMM_GUID equal to AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB.

Since the mounted volume A00000 is unassigned, it implies that no images corresponding to media id A00000 are present, the media record is treated much like scratch media. `bephyinv` changes the ADAMM_GUID of media id A00000 to AAAAAAAA-1234-1234-1234 BBBBBBBBBBBB, as shown in the table above.

`bephyinv` then changes the media description of media id A00000 to the Cartridge Label read off the tape header: *Backup Exec media*. `bephyinv` assigns the media to NetBackup, and sets its state as FROZEN in the NetBackup media database of host tumbleweed. Doing so ensures that NetBackup will never mount this media for NetBackup backups.

Refer to the table above to see how the Media Manager volume database changes after running `bephyinv`.

Example 3

Media Manager volume database of host Tumbleweed before running `bephyinv`:

Media Id	A00000
Robot Number	1
Robot Slot	5
ADAMM_GUID	---
Media Description	---
Volume Pool	test_pool
Assigned	06 / 16 / 2001 01:24:59 PM

Media Manager volume database of host Tumbleweed after running `bephyinv`:

Media Id	A00000	BE0000
Robot Number	-1	1
Robot Slot	0	5
ADAMM_GUID	---	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	---	Backup Exec media
Volume Pool	test_pool	BackupExec
Assigned	06 / 16 / 2001 01:24:59 PM	07 / 19 / 2001 02:38:23 PM

No media record in the Media Manager volume database of tumbleweed has the ADAMM_GUID equal to AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB.

Since the mounted media id A00000 is assigned, it may be a valid NetBackup media record that may have NetBackup images present. This case may arise when the user has misplaced a media by removing a NetBackup media from slot 5, and putting in a Backup Exec media instead.

`bephyinv` makes media id A00000 non-robotic, since, in any case, a NetBackup media is not actually present in slot 5. The media that was mounted from slot 5 (A00000) was found to be a Backup Exec media.

`bephyinv` creates a new Media Manager volume record belonging to Robot 1, slot 5, and generates a media id (based upon the media id prefix specified in the vm.conf file of Media Manager volume database tumbleweed). `bephyinv` then sets the ADAMM_GUID field of the newly created media id BE0000 to AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB (the GUID read off the tape header) and the "Media description" of BE0000 to Backup Exec media (the Cartridge Label read off the tape header).

`bephyinv` places the newly created media id in the Backup Exec volume pool, assigns it to NetBackup and set its state to be FROZEN in the local NetBackup database. Doing so provides that NetBackup will never mount this media for NetBackup backups.

Refer to the tables above for the Media Manager volume database of tumbleweed before and after running `bephyinv`. The right column of the second table shows the newly generated media id based upon the media id prefix specified in the `vm.conf` file of host tumbleweed.

Note If MEDIA_ID_PREFIX is not specified in the `vm.conf` file, *BE* is the default prefix used for Backup Exec media.

Example 4

Media Manager volume database of host Tumbleweed before running `bephyinv`:

Media Id	A00000	A00001
Robot Number	1	1
Robot Slot	5	6
ADAMM_GUID	XXX[a]	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	XXX[a]	Backup Exec media
Volume Pool	XXX[a]	BackupExec
Assigned	XXX[a]	06/16/2001 01:24:59 PM

a. The state of the field is inconsequential in this example.

Media Manager volume database of host Tumbleweed after running `bephyinv`:

Media Id	A00000	A00001
Robot Number	-1	1
Robot Slot	0	5
ADAMM_GUID	XXX[a]	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	XXX[a]	Backup Exec media
Volume Pool	XXX[a]	BackupExec
Assigned	XXX[a]	06/16/2001 01:24:59 PM

a. The state of the field is inconsequential in this example.

`bephyinv` finds that in the Media Manager volume database on tumbleweed, media id A00001 has ADAMM_GUID AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB.

Since media id A00001 is assigned and has a matching ADAMM_GUID, `bephyinv` changes the residence of media id A00000 to standalone, and changes the residence of media id A00001 from Robot 1, slot number 6, to Robot 1, slot number 5.

Refer to the tables above for the Media Manager volume database of tumbleweed before and after running `bephyinv`.

Example 5

Media Manager volume database of host Tumbleweed before running `bephyinv`:

Media Id	A00000	A00001
Media Type	dlt2	4mm
Robot Number	1	2
Robot Slot	5	6
ADAMM_GUID	XXX[a]	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	XXX[a]	Backup Exec media
Volume Pool	XXX[a]	BackupExec
Assigned	XXX[a]	06/16/2001 01:24:59 PM

a. The state of the field is inconsequential in this example.

Media Manager volume database of host Tumbleweed after running `bephyinv`:

Media Id	A00000	A00001
Media Type	dlt2	dlt2
Robot Number	-1	1
Robot Slot	0	5
ADAMM_GUID	XXX[a]	AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB
Media Description	XXX[a]	Backup Exec media
Volume Pool	XXX[a]	BackupExec
Assigned	XXX[a]	06/19/2001 03:56:33 PM

a. The state of the field is inconsequential in this example.

bephyinv finds that in the Media Manager volume database of tumbleweed, media id A00001 has ADAMM_GUID AAAAAAAA-1234-1234-1234-BBBBBBBBBBBB.

Media ID A0000 needs to be made non-robotic. Media ID A00001 needs to be moved to robot number 1, slot 5, and its media type changed to dlt2. However, since the media type of assigned records should not be changed, bephyinv will report the inconsistency to the user.

This inconsistency may be resolved in the following ways:

- Expire (unassign) A00001 and run bephyinv. This time bephyinv will change the media type of media id A00001 to dlt2 since it is no longer assigned.
- Run bephyinv with the -auto_correct option. bephyinv will automatically expire media id A00001 and change its media type to dlt2.

See the tables above to view the Media Manager volume database on tumbleweed before and after running bephyinv. The second table shows the Media Manager volume database on tumbleweed after running bephyinv with the -auto_correct option.

Browsing Backup Exec Files for Restore

Backup Exec file list requests can be generated by the NetBackup NT client interface (Backup, Archive and Restore), the NetBackup Java client (Backup, Archive and Restore) interface, the NetBackup Administration Console, the NetBackup SQL client interface, the NetBackup Netware client interface or the bplist command.

The NetBackup Database Manager daemon/service, bpdbm, running on the NetBackup master server, processes these file list requests. If files from a Backup Exec image are requested, bpdbm sends the file list request to the host on which the Backup Exec catalogs were converted to NetBackup catalogs (either by beconv or by bpimport).

The following steps describe what happens when bpdbm receives a file list request for files belonging to Backup Exec images:

1. bpdbm launches bpcd on the target host (the host on which the Backup Exec catalogs were converted to NetBackup catalogs, either by beconv or by bpimport) to obtain the list of files corresponding to the Backup Exec image.

2. bpcd launches bptm to obtain the Backup Exec media GUID corresponding to the Media Manager media id. The media id, which is stored in the Backup Exec image was passed to bpcd by bpdbm)

3. bptm obtains the Backup Exec GUID from the media id (which was passed over to it by bpcd), by querying the Media Manager volume database hosts of all the robots that have locally configured drives and the Media Manager standalone drive volume database host.

4. bpcd queries Backup Exec to obtain the Backup Exec file list corresponding to the Backup Exec GUID and the backup set number (which is stored in the keyword field of the Backup Exec image, and which was passed on to bpcd by bpdbm.)

Restoring Backup Exec Files

Backup Exec file restore requests can be generated by the NetBackup NT client interface (Backup, Archive and Restore), the NetBackup Java client (Backup, Archive and Restore) interface, the NetBackup Administration Console, the NetBackup SQL client interface, the NetBackup Netware client interface or the bprestore command.

These restore requests are processed by the NetBackup Request daemon/service, bprd, running on the NetBackup master server. If files from a Backup Exec image are submitted for restore, bprd sends the restore request to the host on which the Backup Exec catalogs were converted to NetBackup catalogs (either by beconv or by bpimport).

Note If the NetBackup device configuration is changed, and the NetBackup Device Manager service is restarted, the Backup Exec 8.x Device and Media Service on the same host should also be restarted (after the NetBackup Device Manager service been restarted). If this is not done, Backup Exec restore jobs may not run, or all the available drives may not be used for Backup Exec restore jobs.

The following steps describe what happens when bprd receives a restore request for Backup Exec images:

1. bprd launches bpcd on the target host (the host on which the Backup Exec catalogs were converted to NetBackup catalogs, either by beconv or by bpimport) to restore the Backup Exec files.

2. bpcd launches bptm to obtain the Backup Exec media GUID corresponding to the Media Manager media id. The media id, which is stored in the Backup Exec image was passed to bpcd by bprd.

3. bptm obtains the Backup Exec GUID from the media id (which was passed over to it by bpcd), by querying the Media Manager volume database hosts of all the robots that have locally configured drives and the Media Manager standalone drive volume database host.

4. bpcd launches the Backup Exec restore job by specifying the file list and Backup Exec family GUID that is derived from the Backup Exec media GUID.

5. bpcd sends the restore job progress information and completion status to bprd.

Each Backup Exec backup set is converted to one NetBackup image. Depending upon the files selected and the date range, multiple Backup Exec restore jobs may get launched corresponding to a single NetBackup restore job.

Example 1

User selects directory: C:\temp\foo.txt

Date range: 08/05/2001 through 08/12/2001 (MM/DD/YYYY date format)

Backup Exec took three backups between 08/05/2001 and 08/12/2001 that contain the directory C:\temp\foo.txt:

```
Backup Set: B1, Backup Date: 08/06/2001
Backup Set: B2, Backup Date: 08/07/2001
Backup Set: B3, Backup Date: 08/08/2001
```

The Backup Exec restore job launched corresponds to the latest backup set containing the file for restore, in this case Backup Set B3.

Note In case the user selects a directory, which belongs to multiple backup sets, a separate Backup Exec restore job is launched for each of the Backup Exec images.

When a user selects a directory for restore, for Backup Exec images, NetBackup does not expand the directory to obtain the file list, and then determine which files need to be restored from which Backup Exec images. (This is unlike the case for NetBackup images.)

Example 2

User selects directory: C:\temp

Date range: 08/05/2001 through 08/12/2001 (MM/DD/YYYY date format),

Backup Exec made three backups between 08/05/2001 and 08/12/2001, which contain the directory C:\temp\:

```
Backup Set: B1, Backup Date: 08/06/2001
Backup Set: B2, Backup Date: 08/07/2001
Backup Set: B3, Backup Date: 08/08/2001
```

Three restore jobs are launched corresponding to each of the backup sets.

If the Overwrite existing files option was selected, the Backup Exec restore jobs would run in the following order: B1, B2, B3. In the Overwrite existing files option was not selected, the Backup Exec restore jobs would run in the following order: B3, B2, B1.

This ensures that at the end of the NetBackup restore job, the client will get restored with the files of the latest backup.

Backup Exec Restore Options

The Backup Exec Tape Reader for NetBackup option will enable restoring the following types of files backed up by Backup Exec:

- Windows NT/2000 files
- UNIX and Netware files
- SQL 6.5/SQL 7.0/SQL 2000 databases
- Exchange 5.5, 2000 databases
- Windows 2000 system state

Mixed restores (a restore containing both Backup Exec and NetBackup images) of Exchange and SQL databases are not permitted. Consequently, only Backup Exec Exchange/SQL images or NetBackup Exchange/SQL images can be browsed in the same screen.

Browsing and/or restoring a mix of both NetBackup and Backup Exec images of Windows NT/2000, UNIX and Netware file systems is permitted. Therefore, it is possible to restore a full backup image backed up by Backup Exec and a differential/incremental backup image backed up by NetBackup, in one NetBackup restore job.

Access to Restore Target

Backup Exec restore jobs may fail, if prior to upgrade, the Backup Exec services did not have access to the target being restored. This may include Windows NT/2000 machines which cannot be accessed by the user account under which the Backup Exec services are running, Netware machines, UNIX machines, the Exchange databases and mail boxes and SQL databases. In such cases, it may be possible to grant access to the Backup Exec services by performing the following steps:

1. Launch the Backup Exec user interface (`bkupexec.exe`).
2. Attach to the target which needs to be restored. A user name and password for the target must be supplied when prompted by the Backup Exec user interface.
3. Close the Backup Exec user interface.

Limitations

The following sections are limitations to consider when using the Backup Exec Tape Reader for NetBackup option.

General Limitations

- The Backup Exec Tape Reader for NetBackup option does not convert or migrate Backup Exec job history, job schedules, or job descriptions to NetBackup.
- The Backup Exec Tape Reader for NetBackup option does not convert Backup Exec application setup or configuration information to NetBackup.
- The Backup Exec Tape Reader for NetBackup option does not support performing an Intelligent Disaster Recovery (IDR) operation using the NetBackup IDR wizard and Backup Exec media. This includes both local and remote IDR restores.
- NetBackup does not currently support standalone drives under Removable Storage Manager (RSM). To restore media written by Backup Exec using an RSM-controlled standalone drive or robot, the media must be put in a compatible non-RSM standalone drive or a library.

Client Restore Limitations

- Backup Exec file browse and restore operations are slower than NetBackup file browse and restore operations.
- All Backup Exec restore options are not supported when launching a Backup Exec restore job from the NetBackup Administration Console or from the command line.

Glossary

access control list (ACL)

Security information associated with files on some file systems.

ACS

Automated Cartridge System. ACS can refer to any of the following:

- A type of Media Manager robotic control. This robot type is supported only by NetBackup DataCenter servers.
- The StorageTek (STK) system for robotic control.
- The highest-level component under STK's ACS library software, which refers to a specific standalone robotic library or to multiple libraries connected with a media passthru mechanism.

active job

A job for which NetBackup is currently processing backup or restore data.

activity logs

See "debug logs."

activity monitor

A NetBackup administration utility that displays information about NetBackup jobs and provides limited control over them.

administration client

See "remote administration console."

administrator

A user that is granted special privileges to install, configure, and manage the operation of a system, network, or application.

AIT

Sony Advanced Intelligent Tape, a type of tape drive or media type.

alternate-client restore

See “redirected restore (different client).”

alternate-target restore

See “redirected restore (different target).”

alternate path restore

See “redirected restore (different path).”

alternate read server

A server used to read a backup image which was originally written by a different media server. The media server specified as Alternate Read Server must have access to the media containing the backup image or images it is configured to read.

archive

A special kind of backup where NetBackup backs up the selected files, and if the backup is successful, deletes the files from the local disk. In this manual, references to backups also apply to the backup portion of archive operations except where otherwise noted.

archive bit

A file-status bit that the Microsoft based operating system sets when it writes a file, thereby indicating that the file has changed.

attributes for a policy

Configuration parameters that control the behavior of NetBackup during operations involving this policy.

autochanger

See “robotic library.”

autoloader

See “robotic library.”

automatic backup

A scheduled backup by the master server.

back up

The act of copying and saving files and folders to storage media.

backup

Refers to the process of copying and saving files and directories to storage media. For example, *the backup is complete*. This term can also refer to the collection of data that NetBackup saves for a client during a backup or archive. For example, *duplicate the backup*.

Backup is two words when used as a verb. For example, *back up the file*.

backup, archive, and restore interface

The name of the NetBackup Microsoft Windows and Java based user interfaces for clients. On servers these interfaces can be started through the NetBackup Administration Console.

backup window

The period of time during which backups can begin.

block size

The number of bytes in each block of data written on the media during a backup.

bp

A backup, archive, and restore utility for users on NetBackup UNIX clients. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bpadm

An administrator utility that runs on NetBackup UNIX servers. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bp.conf file

A NetBackup configuration file on UNIX servers and also on UNIX, Macintosh, and OS/2 clients.

bp.ini file

NetBackup initialization file for Novell NetWare target clients.

bpcd

NetBackup Client service on Windows and the NetBackup Client daemon on UNIX.

bprd

NetBackup Request Manager service on Windows and NetBackup Request daemon on UNIX.

cancel a job

Terminating a job and removing it from the job queue.

carousel

See “robotic library.”

catalogs

Internal NetBackup and Media Manager databases. These catalogs contain information about configuration, media, devices, status, errors, and the files and directories in the stored backup images.

CDF

Context-dependent file, which is a type of directory structure on a Hewlett-Packard system.

changer

See “robotic library.”

class

See “policy.”

client

The system with the files to back up, archive, or restore.

client-user interface

See “user interface.”

cluster

See master and media server cluster.

command lines

Commands that users can execute either from the system prompt or in scripts.

compression

The process of compacting data to enable more efficient transmission and storage.

configuration

The parameters that govern the behavior of an application. This term can also refer to the manner in which a network or system is laid out or connected (for example, a network configuration).

consolidated eject

A process of ejecting media for more than one Vault session at a time. A Consolidated Eject can be performed for one or more logical vaults at one time.

consolidated report

A process of generating reports for more than one Vault session at a time. A Consolidated Report can be performed for one or more logical vaults at one time. Consolidated reports are organized by report title, not by vault.

cpio

A UNIX command that can be used for copying files to or from a cpio archive on disk or tape.

ctime

The time that a UNIX inode was changed.

cumulative-incremental backup

A backup that is scheduled by the administrator on the master server and backs up files that have changed since the last successful full backup. All files are backed up if no prior backup has been done. Also see “differential-incremental backup.”

daemon

A program on a UNIX system that runs in the background and performs some task (for example, starting other programs when they are needed). Daemons are generally referred to as services or processes on Windows server systems.

database-agent clients

Clients with additional NetBackup software that is designed to back up relational databases.

database-extension clients

See “database-agent clients.”

debug logs

Logs that can be optionally enabled for specific NetBackup and Media Manager programs and processes and then used to investigate problems.

destination storage unit

A storage unit to which Vault sends the data from a duplication operation. If the duplicated backup images are to be vaulted, then the destination storage unit must correspond to the robotic volume group.

device delays

Delays caused by the device that are beyond the control of the storage application. An example is the time required to position tape under the read and write heads.

device host

A host (that has Media Manager installed) where a drive or robotic control is attached or is defined.

device monitor

A Media Manager administration utility that provides monitoring and manual control of Media Manager storage devices. For example, an administrator or computer room operator can use this utility to manually reset devices or set them to the UP or DOWN state.

DHCP

Dynamic host configuration protocol. This TCP/IP protocol automatically assigns temporary IP addresses to hosts when they connect to the network.

differential-incremental backup

Scheduled by the administrator on the master server and backs up files that have changed since the last successful incremental or full backup. All files are backed up if no prior backup has been done. Also see “cumulative-incremental backup.”

directory depth

The number of levels below the current directory level that the NetBackup interfaces show in their directory and file list displays.

directory tree

The hierarchical structure in which files are organized on a disk. Each directory lists the files and directories that are directly below it in the tree. On UNIX, the topmost directory is called the root directory.

disaster recovery

Recovering data from backups after a disk crash or other catastrophe.

disk

Magnetic or optical disk storage media.

disk-image backup

A bit-by-bit rather than a file system backup of a disk drive on a Windows platform.

DLT

Digital-linear tape or tape drive type.

Domain Name Service (DNS)

A program that handles name translation for network communications.

drive cleaning

The use of a special cleaning tape to clean the heads on a drive.

duplicate image

A copy of a backup image.

eject

Move media out of a robotic library.

encryption

Provides additional security by encrypting backup data on the client. This capability is available only with the NetBackup Encryption option.

entry and exit ports

See “media access port.”

exclude list

A list that designates files or directories to exclude from automatic backups.

expiration (image)

The date and time when NetBackup stops tracking a backup image.

expiration (volume)

The date and time when the physical media (tape) is considered to be no longer usable.

external media ID

This is an identifier written on a media cartridge or canister to help the operator identify the volume before inserting it into a drive or robot. For labeled media, the external media ID should be the same as the media ID recorded on the media.

EVSN

See “external media ID.”

FlashBackup

A special type of raw-partition backup that requires the NetBackup FlashBackup separately-priced option (this option is available only for NetBackup DataCenter).

flush level

Controls how often Netbackup clears its log files on a Novell NetWare or Microsoft Windows client platform.

fragment

A part of a backup or archive image. NetBackup can be configured to divide images into fragments when they exceed a certain size or span tapes.

frequency (backup)

How often NetBackup performs scheduled backups. For example, if the frequency is seven days then backups occur once a week.

FROZEN media state

If a volume is FROZEN, NetBackup keeps it indefinitely and can restore from it but not use it for further backups or archives.

full backup

A backup that copies, to a storage unit, all files and directories that are beneath a specified directory.

FULL media state

If this appears in a report or listing, it indicates the volume is FULL and cannot hold more data or be used for further backups.

global attributes

NetBackup configuration attributes that affect all policies.

GDM Dashboard

The name for the Global Data Manager interface. The Dashboard enables monitoring job and drive activity on multiple master servers, as well as providing alerts to problem conditions.

GDM Managed Server

A NetBackup master server that appears as a managed master server in the left pane of the GDM Dashboard.

GDM Server

A NetBackup master server that has the Global Data Manager license activated. When logging into this host, the user can monitor the activity on multiple master servers using the GDM Dashboard interface. If the host has installed the Advanced Reporter option, the reports show information on multiple master servers.

Global Data Manager (GDM)

A separately-priced option (for UNIX servers) that provides an interface with a tree view where the administrator can view and administer multiple master servers. The server where the option is installed is called a GDM Server.

Global Device Database

A single host that serves as the repository for global device configuration information. When you install NetBackup, by default the master server is configured as the global device database host.

GNU tar

A public domain version of the UNIX tar program.

goodies directory

A directory containing programs, scripts, and other files that are not formally supported.

GUI

Graphical user interface.

hard link

On UNIX, a hard link is a pointer to the inode for the data. On a Windows server, a hard link is a directory entry for a file. Every file can be considered to have at least one hard link. On NTFS volumes each file can have multiple hard links, and a single file can appear in many directories (or even in the same directory with different names).

heap level

A parameter for memory-heap debugging on a Novell NetWare or Windows NetBackup client.

hierarchical storage management

The process of automatically migrating selected files from a managed file system to specified migration levels on secondary storage, while maintaining transparent access to those files.

host

A computer that executes application programs.

host name

Name by which a host computer is identified by programs and other computers in the network.

HSM

See storage migrator.

image

The collection of data that NetBackup saves for an individual client during each backup or archive. The image contains all the files, directories, and catalog information associated with the backup or archive.

import

The process of recreating NetBackup records of images so the images can be restored.

include list

A list that designates files or directories to add back in from the exclude list.

incremental backup

See “cumulative-incremental backup” and “differential-incremental backup.”

inject

Move media into a robotic library.

inport

See “media access port.”

inode

A UNIX data structure that defines the existence of a single file.

install_path

Directory where NetBackup and Media Manager software is installed. The default on Windows servers is `C:\Program Files\VERITAS` and on UNIX it is `/usr/openv`.

jbpSA

The Java-based NetBackup interface for performing user backups, archives, and restores.

jnbSA

The Java-based NetBackup interface for administrators.

job

A parcel of work submitted to a computer. NetBackup jobs are backups, archives, or restores.

kernel

The nucleus of an operating system.

keyword phrase

A textual description of a backup.

kill a job

See “cancel a job.”

label

Identifier of a tape or optical disk volume. A recorded label includes a media ID.

A barcode label allows a barcode scanner to be used for media tracking.

library

See “robotic library.”

link

See “hard link” or “symbolic link.”

LMF - Library Management Facility

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

load

(noun) Amount of work that is being performed by a system or the level of traffic on a network. For example, network load affects performance.

(verb) Copy data to internal memory. For example, load the installation program.

(verb) Used to indicate tape drive initialization done when new media is being added.

logs

Files where a computer or application records information about its activities.

mailslot

See “media access port.”

man pages

Online documentation provided with UNIX computer systems and applications.

Master and media server cluster

A NetBackup master server and the remote media servers that it is using for additional storage. It is possible to configure clusters only with NetBackup DataCenter servers. NetBackup BusinesServer supports only a single server, the master.

Master of Masters

A NetBackup host where Global Data Manager software is installed. When logging into this host, the interface has a tree view where the administrator can view and administer multiple master servers.

master server

The NetBackup server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster. NetBackup BusinesServer supports only a single server and it is the master.

media

Physical magnetic tapes, optical disks, or magnetic disks where data are stored.

media access port

A slot or other opening in a robot where you can insert or remove a tape without having to access the interior of the robot. After inserting a tape, you move it to a slot by using an inject command. Prior to removing a tape, you move it to the port by using an eject command. The inject and eject commands are supported through the add and move screens in the Media Manager administration interface.

media host

NetBackup server to which the job (client) is sending the data.

media ID

An identifier that is written on a volume as part of the recorded label.

Media Manager

Software that is part of NetBackup and manages the storage devices and removable media.

Media Manager Host

Host where Media Manager is installed (may have devices attached).

media server

A NetBackup server that provides storage within a master and media server cluster. The master can also be a media server. A media server that is not the master is called a remote media server. NetBackup BusinesServer does not support remote media servers.

menu interface

A character-based interface for use on terminals that do not have graphical capabilities.

mount

Make a volume available for reading or writing.

mount point

The point where a file system on a disk logically connects to a system's directory structure so the file system is available to users and applications.

MPX

See “multiplexing.”

mtime

The point in time when a UNIX or NTFS file is modified.

multiplexing

The process of sending concurrent-multiple backups from one or more clients to a single storage device and interleaving those images onto the media.

multiplexed group

A set of backups that were multiplexed together in a single multiplexing session.

NDMP

Network data management protocol. NetBackup requires the NetBackup for NDMP separately-priced option to support NDMP.

NetBackup Client service

NetBackup Windows service that runs on clients and servers and listens for connections from NetBackup servers and clients in the network. When a connection is made, this service starts the necessary programs.

NetBackup configuration options

On UNIX servers and on UNIX and Macintosh, clients, these settings are made in the `bp.conf` file. On NetWare target and OS/2 clients, they are in the `bp.ini` file. On Windows servers and Windows clients, these settings are called properties and are made through the Backup, Archive, and Restore interface or the Host Properties dialog in the NetBackup Administration Console.

NetBackup databases

See catalogs.

NetBackup Database Manager service

NetBackup Windows service that runs on the master server and manages the NetBackup internal databases (called catalogs). This service must be running on the master server during all NetBackup administrative operations.

NetBackup Device Manager service

The NetBackup Windows service that runs on a NetBackup server and starts the robotic control processes and controls the reservation and assignment of volumes. This service runs only if the server has devices under Media Manager control. The process is `ltid`.

NetBackup properties

Same as NetBackup configuration options but are called NetBackup properties on Microsoft Windows platforms.

NetBackup Request Manager service

The NetBackup Windows service that runs on the master server and starts the scheduler and receives requests from clients.

NetBackup Volume Manager service

A NetBackup Windows service that runs on a NetBackup server, allows remote administration of Media Manager, and manages volume information. The process is `vmd`.

NIS

Network information service.

NLM

NetWare loadable module.

NFS

Network file system.

nonrobotic

See “standalone.”

ODL

Optical disk library. This robot type is supported only by NetBackup DataCenter servers.

offsite volume group

A volume group in which media will appear after having been ejected from the robot for vaulting. When Vault ejects media it is moved from the robotic volume group to the off-site volume group.

offsite volume pool

A volume pool that contains media that is to be ejected and vaulted. Backup images written to an off-site volume pool by an original NetBackup backup policy or by Vault's duplication feature will be ejected and vaulted. More than one off-site volume pool can be specified for the Eject step of a Vault profile.

original backup

A backup image created by a backup job. A single backup image or all backup images created by an Inline Tape Copy (multiple copy) configuration are considered original backups. A backup image created by a duplication job is not an original backup.

outport

See "media access port."

partitions

The logical partitions into which a magnetic disk is divided.

patch

A program that corrects a problem or adds a feature to an existing release of software.

path length

Number of characters in a pathname.

pathname

The list of directories in the path to a destination directory or file.

PC clients

NetBackup clients that have Microsoft Windows, Macintosh, or IBM OS/2 operating systems.

peername

The name by which a computer identifies itself when establishing connections to other systems.

policy

Defines the backup characteristics for a group of one or more clients that have similar backup requirements.

port

A location used for transferring data in or out of a computer.

Also see “media access port.”

primary copy

The copy of an image that NetBackup uses to satisfy restores. When NetBackup duplicates an image, the original is designated as the primary copy.

privileges

The tasks or functions that a user, system, or application is authorized to perform.

profile

A vault profile is a way to save configuration settings. Specific parameters for duplication, catalog backup, eject, and report or any combination of these steps, are configured within a profile.

progress report

Log where NetBackup records events that occur during user operations.

proxy restore

A proxy restore allows the user to restore files that he has write access to, on a machine other than his desktop. The files must be in a backup of the machine to which they are being restored.

QIC

Quarter-inch-cartridge tape.

queued job

A job that has been added to the list of jobs to be performed.

raw-partition backup

Bit-by-bit backup of a partition of a disk drive on UNIX. On Windows, this is called a disk-image backup.

rbak

The program that Apollo clients use to read data from tape during a restore.

recorded media ID

This is an identifier written as part of the label on a volume and used by Media Manager to ensure that the correct volume is mounted. The recorded media ID should match the external media ID.

redirected restore (different client)

Restoring files to your client when they were originally backed up from a different client. The administrator using the interface on the master server can direct a restore to any client (this variation is called a server directed restore).

redirected restore (different target)

On a Novell NetWare server platform running the NetBackup target version of client software, this operation restores files to a different target than the one from which they were backed up.

redirected restore (different path)

Restores files to a different directory than the one from which they were backed up.

registry

A Microsoft Windows database that has configuration information about hardware and user accounts.

remote administration console

A Windows NetBackup client that has the administration interface software installed and can be used to administer NetBackup servers.

remote media server

A media server that is not the master. Note that only NetBackup DataCenter supports remote media servers. NetBackup BusinesServer supports only a single server, the master.

residence

In Media Manager, information about the location of each volume is stored in a volume database. This residence entry contains information, such as robot number, robot host, robot type, and media type.

resource

A Novell NetWare term that refers to a data set on the target. For example, in DOS, resources are drives, directories, and files. Also see “target service.”

restore

(verb) The act of restoring selected files and directories from a previous backup or archive and returning them to their original directory locations (or to a different directory).

(noun) The process of restoring selected files and directories from a previous backup and returning them to their original directory locations (or to a different directory).

retention level

An index number that corresponds to a user-defined retention period. There are 10 levels from which to choose (0 though 9) and the retention period associated with each is configurable. Also see “retention period.”

retention period

The length of time that NetBackup keeps backup and archive images. The retention period is specified on the schedule.

robotic arm

The component of a robotic library that physically selects the media (tape or optical disk).

robotic library

Refers to a robot and its accompanying software. A robotic library includes a collection of tapes or optical platters used for data storage and retrieval. For example, a Tape Library DLT (TLD) refers to a robot that has TLD robotic control.

robotic volume group

A volume group from which media will be ejected and vaulted. When Vault duplicates backups, they are duplicated to media in the robotic volume group.

root

The highest level directory in a hierarchical directory structure. In MS-DOS, the root directory on a drive is designated by a backslash (for example, the root on drive C is C:\). On UNIX, the root directory is designated by a slash (/).

Also, a UNIX user name having administration capability.

RS-232

An industry-standard interface for serial communications and sometimes used for communicating with storage peripherals.

RSM Interface

Application in Windows 2000 used to manage Removable Storage Manager (RSM) devices.

RSM - Removable Storage Manager

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

Also, a component of the Windows 2000 operating system that manages storage devices.

RVSN

See “recorded media ID.”

schedules

Controls when backups can occur in addition to other aspects of the backup, such as: the type of backup (full, incremental) and how long NetBackup retains the image.

SCSI

Small computer system interface. This is a type of parallel interface that is frequently used for communicating with storage peripherals.

server-directed restore

Using the user interface on the master server to restore files to any client. Only the administrator can perform this operation.

server independent restore

Restoring files by using a NetBackup server other than the one that was used to write the backup. This feature is available only with NetBackup DataCenter.

server list

The list of servers that a NetBackup client or server refers to when establishing or verifying connections to NetBackup servers. On a Windows server and Microsoft Windows clients, you update the list through a dialog box in the interface. On a UNIX server and UNIX and Macintosh clients, the list is in the `bp.conf` file. On NetWare target and OS/2 clients, the list is in the `bp.ini` file.

service

A program on a Windows server system that runs in the background and performs some task (for example, starting other programs when they are needed). Services are generally referred to as daemons on UNIX systems.

session

An instance of NetBackup checking its schedules for backups that are due, adding them to its worklist, and attempting to complete all jobs in the worklist. For user backups and archives, a session usually consists of a single backup or archive.

Session (Vault)

A vault session consists of executing a particular profile or profiles.

shared drives

See “Shared Storage Option (SSO).”

Shared Storage Option (SSO)

A separately priced VERITAS software option that allows tape drives (standalone or in a robotic library) to be dynamically shared among multiple NetBackup and Storage Migrator servers.

This option is supported only on NetBackup DataCenter servers.

SMDR

Storage management data requestor, a Novell NetWare program that provides its services transparently to all SMS modules and lets remote and local modules communicate with one another.

SMS

Novell NetWare storage management services.

source volume group

A volume group from which Vault can select backups to duplicate. This parameter is used to restrict the list of backups from all backups that reside on media in any volume group to backups that reside on media in a single volume group. Where a volume group corresponds to a particular robot, the profile will duplicate only backups on media in that robot. The Source Volume Group is normally only specified if you have multiple robots attached to the same server, for example you want to duplicate backups that reside in robot 0 to media that reside in robot 1.

SSO

See “Shared Storage Option (SSO).”

stacker

Usually a small robotic library that contains one drive only. See “robotic library.”

standalone

A qualifier used with drives and media to indicate they are not associated with a robot. For example, a standalone tape drive is one where you must manually find and insert tapes before using them. A standalone volume is one that is located in a standalone drive or is stored outside of a drive and designated as standalone in the volume configuration.

status code

A numerical code, usually accompanied by a troubleshooting message, that indicates the outcome of an operation.

storage migrator

Refers to the VERITAS Storage Migrator line of hierarchical storage management products for UNIX and Windows. These products make extra room on a disk by transparently moving data to other storage and then transparently retrieving the data when it is needed by a user or application.

Storage Migrator is available only for NetBackup DataCenter servers.

storage unit

Refers to a storage device where NetBackup or Storage Migrator stores files. It can be a set of drives in a robot or consist of one or more single tape drives that connect to the same host.

SUSPENDED media state

If a volume is SUSPENDED, NetBackup can restore from it but cannot use it for backups. NetBackup retains a record of the media ID until the last backup image on the volume expires.

symbolic link

On a UNIX system, this is a pointer to the name of the file that has the source data.

TapeAlert

Allows reactive cleaning for most drive types and is a function of the tape drive.

tape format

The format that an application uses to write data on a tape.

tape marks

A mark that is recorded between backup images on a tape.

tape overhead

The space required for data that is not part of the backup images. For example, tape marks and catalogs of what are on the tape are considered overhead.

tape spanning

Using more than one tape to store a single backup image.

tar

Tape Archive program that NetBackup uses to extract backup images during a restore.

target

See “target service.”

target service

A Novell NetWare service that needs storage management. The SMS views all services (for example, print services, communication services, workstations) as targets.

Target Service Agent

A Target-service agent is a Novell NetWare agent that prepares the target's data for SMS during a backup and for the target during a restore.

TLD - Tape Library DLT

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TLH - Tape Library Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

TLM - Tape Library Multimedia

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

TL4 - Tape Library 4MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TL8 - Tape Library 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

timeout period

The period of time that an application has allotted for an event to occur.

TIR

See “true image restore.”

tpconfig

A Media Manager administration utility for configuring devices which is started from the command line. On UNIX, it has a character-based menu interface that can be run from terminals that do not have X Windows capabilities. tpconfig also has a command line interface.

transfer rate

The rate at which computer information is transferred between a source and a destination.

transport

See “robotic arm.”

true image restore

Restores the contents of a directory to what it was at the time of any scheduled full or incremental backup. Previously deleted files are ignored.

TS8 - Tape Stacker 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TSA

See “Target Service Agent.”

TSD - Tape Stacker DLT

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

TSH - Tape Stacker Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the VERITAS support web site.

This robot type is supported only by NetBackup DataCenter servers.

unassigned media

Media that contain no valid images. A piece of unassigned media has an entry in the volumes database but no entries in the images database. Unassigned Media do not have a “time assigned” in the Media section of the GUI.

user interface

The program used to perform user backups, archives, and restores.

user operation

A backup, archive, or restore that is started by a person on a client system.

Vault

Vault is a separately-priced NetBackup option that provides offsite backup management. Vault automatically duplicates specified backup images, and automates the process of offsite media rotation (a critical component of any backup or disaster recovery strategy). Vault manages offsite storage and retrieval of media for original backups, duplicate backups, and catalog backups. Additionally, NetBackup Vault generates reports to track the location and content of each piece of media.

vault

In the context of the NetBackup Vault, a vault is logical entity associated with a particular robot that acts as a designated holding place for backups that will eventually be sent to a physical offsite vault. The term ‘vault’ is used to refer both to the process, and to the physical storage location of a set of tapes offsite.

vault process

Vaulting is the process of choosing backup images to duplicate or eject, optionally duplicating backups, ejecting duplicate or original media, storing it at an offsite location, and later returning expired media to your robot. Vaulting is an integral part of the disaster recovery process.

verbose flag

Configuration file entry that causes a higher level of detail to be written in the logs.

verify

An operation that compares the list of files that are actually on a volume with what NetBackup has recorded as being on it. The data that is on the media is not verified.

vmadm

A Media Manager administrator utility for managing volumes. It runs on UNIX and has a character-based, menu interface that can be run from terminals.

vm.conf

A Media Manager configuration file with entries that include the servers that can manage local devices and default media ID prefixes for media that do not contain barcodes.

volume

Media Manager volumes are logical units of data storage or cleaning capability on media that have been assigned media IDs and other attributes, which are recorded in the Media Manager volume database.

volume configuration

Refers to configuration information that is stored in the Media Manager volume database.

volume database

An internal database where Media Manager keeps information about volumes. All hosts (where Media Manager is installed) have a volume database. However, the database is empty unless the host is designated as a volume database host.

volume database host

The host (where Media Manager is installed) that contains information about the volumes that Media Manager uses in a device. Because NetBackup BusinesServer supports only a single server, the volume database host is always on the same server.

volume group

A set of volumes that are configured within Media Manager to reside at the same physical location (for example, in a specific robot).

volume pool

A set of volumes that are configured within Media Manager to be used by a single application and are protected from access by other applications and users.

wakeup interval

The time interval at which NetBackup checks for backups that are due.

wildcard characters

A character that can be used to represent other characters in searches.

Microsoft Windows

(noun) Describes a line of operating systems developed by Microsoft, Inc.

For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`.

Windows

(adjective) Used to describe a specific product or clarify a term. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI.

Windows servers

A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and 2000.

Windows clients

A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE.

Windows Display Console

A NetBackup-Java interface program that runs on Windows 2000, NT, 98, and 95 computers. Users can start this interface on their local system, connect to a UNIX system that has the NetBackup-Java software installed, and then perform any user operations that their permissions allow.

WORM media

Write-once, read-many media for optical disks. NetBackup BusinesServer does not support WORM media.

xbp

The X Windows-based backup, archive, and restore program for users on NetBackup UNIX clients.

Index

A

Absolute Pathname to Directory box 31
Access
  license keys for a NetBackup server 317
Access control lists (ACLs) 94
ACL (see Access control lists)
Action taken on busy File 310
Activate policy 64
Active job 218, 224
Activity monitor
  cancel uncompleted jobs 220
  copy job information 221
  delete completed jobs 220
  detailed job status 220, 226
  disable job logging 276
  monitoring jobs 220
  specifying job filters 217
  using troubleshooting wizard 231
Adding
  catalog backup file paths 156
  clients to policy 75, 76
  files to policy 79, 80
  licenses 317
  new license key 318
  pathname 156
  paths to file list 77
  schedules 108, 113
  storage unit
    disk type 26
    media manager type 27
    NDMP type 26
Administrator
  definition xxxi
Administrator-defined streaming mode 101
All log entries report 200
Allow Frozen Image Clients 64
Allow media overwrite 274
Allow multiple data streams
  file-list directives 100
  set policy attribute 70
  tuning 73
  when to use 71
Allow multiple retentions per media 275
Allow non-reserved ports 251
Alternate client restores
  allowing 326
  host.xlate file 631
altnames file 326
Announce DHCP interval 306
ANSI format, allow overwrite 274
AOS/VS format, allow overwrite 274
Apollo Restore Timeout 277
Archive bit 304
Archives
  overview 6
Assistant, NetBackup 9
Attributes
  general for a policy 58
  NetBackup global (see Global Attributes)
Authentication
  commands 378
  configuration files 372
  enhanced
    configuring 383
  procedure 383
Authorization (see NetBackup authorization)
authorize.txt file 396
Auto-discover streaming mode 102

B

b 109
Backup end notify timeout 257
Backup Exec
  listing files 517
Backup frequency

effect on priority 112
guidelines for setting 640
setting 112
Backup migrated files (NetWare only) 311
Backup policy management window 40
Backup speed (see Transfer rate)
Backup start notify timeout 257
Backup windows
duration
examples 119
specifying 118
backup_exit_notify script 680
backup_notify script 680
Backups
across mount points 65
activating policy 64
automatic, introduction to 1
backup_exit_notify script 680
backup_notify script 680
balancing load 368
best times for user directed 139
bpend_notify script
UNIX client 686
windows client 688
bpstart_notify script
UNIX client 681
windows client 683
catalogs, NetBackup 145
diskfull_notify script 690
duplicating 178
estimating time required 633
frequency (see Backup frequency
full 110
import 184
incremental
overview 642
set on schedule 110
manual (see Manual backups)
media requirements 641
multiplexing (see Multiplexing)
offsite storage 640
raw partition 85
registry on Windows clients 86
session_notify script 691
session_start_notify script 692
status of backups report 197
types of 110
user directed
overview 1
schedules 138
verify 177
Bandwidth limiting
configuration overview 414
settings 269
beconv command 422
BE-MTF1 format, allow overwrite 275
bephyinv command 425
Boot managers and IDR 714
Booting a computer
with IDR bootable media 707
bparchive command 429
bpauthorize command 433
bpauthsync command 435
bpbackup command 438
bpbackupdb command 443
BPCD port setting on client 306
bpchangeprimary command 447
bpclassnew command 575
bpclclients command 537
bpclient command 451
bpclinclude command 553
bpclinfo command 544
bpclsched command 558
bpclschedrep command 569
bpconfig command 103, 453
bpdbjobs command 235, 463
bpdbjobs debug log 236
bpdown.exe 315
bpduplicate command 466
bpdynamicclient 413
bpend_notify script
UNIX client 686
windows client 688
bperror command 474
bpexpdate command 484
bpimagelist command 490
bpimmedia command 497
bpimport command 507
bplabel command 513
bplist command 515
bpmedia command 522
bpmedialist command 525
bpminlicense command 536
bpplclients command 537
bppldelete command 520
bpplinclude command 553
bpplinfo command 544
bppllist command 521

bpplsched command 558
bpplschedrep command 569
bppolicynew command 575
BPRD port setting on client 306
bprecover command 581
bprestore command 586
bpstart_notify script
    UNIX client 681
    Windows client 683
bpstuadd command 594
bpstudel command 600
bpstulist command 602
bpsturep command 606
BPTM query timeout 272
bpup.exe 315
bpverify command 611
Busy file
    action 310
    directory 309
    operator email address 309
    processing 283, 310
        Windows clients 283
    retry count 310

C

Cancel
    uncompleted jobs 220
Case sensitive exclude list 305
cat_convert utility 618
Catalog backup
    adding a pathname 156
    automatic 146
    caution for compressing 170
    changing a pathname 157
    compressing image catalog 170
    configuration 149
    delay to compress 245
    deleting a pathname 157
    disk path 153
    file paths
        adding 156
        NT master 157
    last media used 150
    manual backup 159
    media ID 151
    media type 150
    notification script 690
    overview 146
    precautions 147
    recovery 147
    setting media density 153
    setting schedules 154
    space required 166
Catalog indexing 173
Catalogs
    device 651
    media 651
    moving client images 171
    NetBackup
        managing 165
    volume 650
Cautions
    alternate client restores 326
    alternate path restore 329
    catalog backup 147
    database compression 170
    retention time 116, 139
    wildcards in UNIX raw backups 97
Changing
    catalog backup attributes 149
    licenses 317
    locale 418
    pathname 157
    policies, multiple 56
    policy properties 46, 53, 54
    retention period 247
    server
        for configuring storage units 320
        for reports 192
    storage unit group 36
Classes
    client list (see Clients, NetBackup)
    file list (see File List)
Client backups report 198
Client Connect Timeout 256
Client database 262
Client exclude and include lists 302
Client name 327
Client name property setting 281
Client port window
    setting on client 282
    setting on server 273
Client Read Timeout 250
Client reserved port window
    setting on client 283
    setting on server 273
Client sends mail 254
Client user

definition xxxi
Clients, NetBackup
adding to policy 75, 76
choosing policy type 58
definition 2
deleting from policy 55
exclude file list 106
exclude files list 674
include files list 677
maximum jobs 244
moving image catalog 171
setting host names 75
software 2
Codes, status 200
Collect disaster recovery information 70
Commands, NetBackup 421
Communications buffer size 305
Compaq Computers
recovering with IDR 714
Compress catalog after 245
Compression
advantages 68
disadvantages 68
specifications 68
Concurrent jobs
on client 244
per policy 62
Configuration
catalog backups 149
host names 630
intelligent disaster recovery 696
Policies 39
storage units 21
with NetBackup Assistant 9
Configure enhanced authentication
vopie method 383
Connect on nonreserved port 263
Copies, third-party 113, 181
Copy, primary 181
Core Frozen Images license 307
cpio format, allow overwrite 274
Creating a new storage unit group 35
Cross mount points
setting 65
Cumulative incremental
overview 643
select for schedule 110
Custom Setup, when to use in IDR 708
Customize
NetBackup Administration Console 14
reports window 193

D

Data streams
(see Allow multiple data streams)
Database-extension clients
add file paths for 92
Databases, NetBackup (see Catalog backup)
Dates, setting for locale 418
Datetime stamp 645
dbbackup_notify script 690
DBR format, allow overwrite 274
Deleting
clients from a policy 54
completed jobs 220
files from a policy 54
license keys 318
pathname 157
policies 54
schedules 54
storage unit group 37
Dell PowerEdge 6100/200 with RAID
recovering with IDR 713
Density, media 31
Detailed job status 220, 226
Device delays 634
Device Monitor 232
DHCP 408
Differential incremental
overview 642
select for schedule 111
Directives
for file list 98
templates 80
Disable Job Logging 276
Disable SCSI Reserve 276
Disable Standalone Drive Extensions 276
Disallow Backups Spanning Media 276
Disallow client browse and restore 257
Disallow client restore 257
Disallow Server File Writes 241, 250
Disaster recovery
catalogs 147
collect information for 70
diskettes
updating 704
procedure 706
Disk Administrator 712

Disk overhead, for catalogs 642
Disk storage units 26, 29, 113, 181
    Maximum fragment size 32
diskfull_notify script 690
DNS (see Domain Name Service)
Domain Name Service
    hostnames 631
Done job 218, 224
drfile.exe command 706
Drive, standalone (see Standalone drive)
Drives
    monitor 231
    monitoring 231
Duplicate backups
    creating 178
    restoring from 183
Duration
    of backup window
        examples 119
    to retain logs 243

E

Email
    send from client 254
    send from server 253
Email address for administrator of this client 254
EMC Fastrax 113, 181
Emergency IDR bootable diskettes 712
Encryption
    keys 293
    libraries 293
    permissions 292
    policy attribute 70
    strength 293
Encryption option 198, 207
End time, schedule 118
Enhanced authorization 252
Escape character 300
    on UNIX 93, 675
Exchange properties 280
Exclude files list 295, 674
    case sensitive 305
    example 676
    for specific policies and schedules 677
    overview 106
    UNIX 674
    Windows example 301
Exclude list, on client 302
Exclude tab 295
Expiration, backup (see Retention period)
Export
    license key 319
External media ID 651

F

Failover media server 270
Fastrax 113, 181
File action for busy files 310
File browse timeout 249
File list
    adding paths 77
    disk image on Windows 85
    extension clients 92
    links on UNIX 95
    Mac clients 91
    NetWare clients
        NonTarget 89
        Target 90
    OS/2 clients 89
    raw partitions 85
    raw partitions on UNIX 96
    standard clients 92
    unix files not backed up 93
    Windows clients 83
File-list directives 98
Files
    catalog space requirements 166, 642
    for catalog backup 156
    host.xlate 631
    linked, UNIX 94
    No.restrictions 327
    peername 328
    restoring to alternate client 329
    restrictions on restores 326
Filters, applying job 217
Firewalls
    vnetd 344
Format description
    tape 657
Fragment
    setting the size 32
    tape format 658
Free browse 264
Freeze media 652
Frequency (see Backup frequency)
Frozen Image 64
Frozen Image Configuration 307

Frozen, media state
definition 652
unfreezing 652
Full, media state 652

G

GDM (Global Data Manager) properties 267
Global attributes for NetBackup 242
Gravity stacker 656

H

Hard links
NTFS volumes 87
UNIX directories 95
Hashed file 380
Host names
changing server name 630
client peername 631
correct use 630
short 631
host.xlate file 631
How Long to Keep TIR Information 243

I

IBM computers, recovering with IDR 714
IDR (see Intelligent Disaster Recovery)
IDR preparation wizard
preparing bootable media 697
updating disaster recovery diskettes 704
Images
changing primary copy 183
duplicating 178
fragmentation 658
import 184
moving client catalog 171
on media report 206
restoring from duplicate 183
verify 177
Import backup images 184
Include files list 106, 297, 677
Include list, on client 302
Incremental backups (see Backups)
Incrementals based on archive bit 304
index_client command 173
Indexing, image catalog 173
Informix policy type 59
INI file, for lotus notes 294
Initial browse search limit 256
Inline Tape Copy option 113, 469
Intelligent disaster recovery
bootable media
choosing type 697
creating CD image 701
creating diskettes 698
preparing 697
collect information for 70
configuration 696
Custom Setup, when to use 708
DR files
obtaining from server 696
overview 695
update with drfile.exe 706
frequently asked questions 714
hard disk partition changes 709
hard drive partition, altering sizes 712
overview 695
preparation wizard 697
recovery wizard 708
requirements for using 694
supported Windows NT editions 694
updating IDR media
disaster recovery CD 706
recovery diskettes 704
using drfile.exe 706
when to update 704
using boot managers 714
Windows NT Disk Administrator 709
Windows NT Editions Supported 694
Windows NT Setup 708
wizard
disaster recovery 708
IDR preparation 697
Intelligent Disaster Recovery diskettes
emergency 712
preparing 697
updating 704
Internet Assigned Numbers Authority (IANA) 334
Interval for status reports 245

J

Java
interface 3
jbpSA (see Java)
jnbSA 3
Job filters
specify 217
Jobs
(see Activity monitor)

concurrent per disk storage unit 32
maximum per client 244
maximum per policy 62
priority for policy 63

K

Keep status property for user operations 282
keep_days 234
keep_hours 234
keep_successful_days 234
keep_successful_hours 234

L

Labeling media 655, 659
Last media used, catalog backups 150
License keys 317
accessing 317
adding 318
deleting 318
export 319
printing 318
viewing the properties of one key 319
Licenses
managing with bpminlicense command 536
Limit jobs per policy, setting 62
Links
UNIX hard-linked directories 95
UNIX symbolic 94
List restore permissions 263
Load balancing 368
Locale 418
Logging enabled for debug 258
logging, enabling 258
Logs
(see Reports)
progress, for user operations 6
setting retention period 243
Lotus Notes properties 294
Lotus-Notes policy type 59

M

Macintosh clients 295, 297
Mail notifications
administrator Email address 254
Email address for admin 245
Windows NT nbmail.cmd script 245
Manual backups
NetBackup catalogs 159
policy 143
Master server (see Server, NetBackup)
Maximum
concurrent jobs
disk storage unit 32
data streams for client 263
fragment size 32
jobs per client
BusinesServer 244
specifying 244
Maximum error messages for server 303
Maximum jobs per policy
(see Limit jobs per policy)
Maximum Restore Apollo arg Characters 278
Media
active 208
automatic suspend 660
backup fragmentation 658
density 31
determining requirements 641
format 657
freeze 652
ID 651
labeling 659
last used for catalog backup 150
media and device information 650
mount and unmount 659
nonactive 208
overwrite protection 274
reports (see Reports)
selection algorithm 653
spanning 654, 656
states 652
type for catalog backup 150
unfreeze 652
unsuspend 652, 660
Media 1 and Media 2, catalog backup 150
Media contents report 203
Media ID
for catalog backup 151
Media ID Prefix 276
Media list report 201
Media log entries report 208
Media Manager
overview 649
Media mount errors 232
Media mount timeout 243
Media request delay 277
Media summary report 208

Media unmount delay 277
Media written report 209
methods.txt file 372
methods_allow.txt file 373
methods_deny.txt file 374
Microsoft Exchange settings 280
mklogdir.bat 258
Monitoring
  NetBackup drives 231
  NetBackup processes 228
  NetBackup services 226
Mount media 659
Mount points and file systems 65
Move detection 65, 672
MS-Exchange policy type 59
MS-SQL-Server policy type 59
MS-Windows-2000 / NT policy type 59
MTF1 format, allow overwrite 274
Multiple copies 113
Multiple data streams
  (see Allow multiple data streams)
Multiple servers 408
Multiplexing (MPX)
  block sizes 659
  demultiplexing 407
  max jobs per client 406
  overhead 659
  schedule media multiplexing 403
  set for schedule 117
  storage unit max per drive 403
  tape format 658
Must use local drive 272
MySQL
  passwords 621

N

Names (see Host names)
names_allow.txt file 375
names_deny.txt file 376
nbdbsetport command 620
nbdbsetpw command 621
nbmail.cmd script 245
NDMP 29, 113, 181
  policy type 59
  storage units 22, 26
NetBackup administration - Java 3
NetBackup administration window 4
NetBackup Assistant 9
NetBackup authorization
  preferred group 252
  process description 391
NetBackup catalogs 170
  (see Catalog backup)
NetBackup Client service 316
  overview 316
NetBackup client service port (BPCD) 306
NetBackup configuration options
  configuring 9
NetBackup Database Manager service
  overview 315
NetBackup databases (see Catalogs)
NetBackup Device Manager service
  overview 315
NetBackup drives
  monitoring 231
NetBackup processes
  monitoring 228
NetBackup Request Manager service
  overview 315
NetBackup request service port (BPRD) 306
NetBackup services
  monitoring 226
NetBackup Vault 469
NetBackup Volume Manager service
  overview 316
NetWare NonTarget client 295, 297
NetWare policy type 59
Network file system
  (see Follow NFS mounts)
Network loading 244
NEW_STREAM, file list directive 101
NFS Access Timeout 278
No Callback 263
NO_STANDALONE_UNLOAD 656
Nonactive media 208
Notification scripts 679
Number of drives setting
  storage units 31

O

On demand only
  disk storage unit 29
  media manager storage unit 29
Online documents 18
Open files (see Busy file processing)
Open Transaction Manager (OTM) 283
Operator email address for busy files 309
Optical devices 113, 181

Oracle policy type 59
OS/2
clients 295, 297
policy type 59
OS/2 Boot Manager and IDR 714
OTM (see Open Transaction Manager)
Overhead, for catalogs 642
Override policy storage unit 114
Override policy volume pool 115
Overwrite protection 274

P

passwords
using nbdbsetpw to change password
for nbdbd database service 621
Path setting (Lotus Notes) 294
Pathname
catalog backup to disk 153
rules for class file list 79
rules for policy file list 83
PC NetLink files 94
Peername
client 631
file 328
Perform default search 305
Performance
measuring (see Transfer rate)
reducing search time 173
Permission
change NetBackup properties 240
Planning
policies 47
storage units 24
user schedules 138
worksheet 660
Policies
activating 64
adding (see Adding)
changing (see Changing)
configuration wizard 45
example 46
general attributes (see Attributes)
overview 6, 39
planning 47
setting priority 63
user 139
user schedules 138
Policy
volume pool 61
Policy storage unit 60
Policy type
Informix 59
Lotus-Notes 59
MS-Exchange 59
MS-SQL-Server 59
MS-Windows-2000/NT 59
NDMP 59
NetWare 59
Oracle 59
OS/2 59
Standard 59
Sybase 60
Vault 59
Pools (see Volume pools)
Power down NetBackup servers 314
Preferred group 252
specify 396
PREFERRED_GROUP 397
Prelabeling media 655
Preprocess interval 102
Primary copy
changing 183
definition 181
Print
job detail information 220
job list information 220
license key 318
report 196
Priority
for a policy 63
for jobs in worklist 639
for schedule 112
Problems report 199
Process busy files 310
Processes
monitor 228
monitoring 228
Progress logs, client 6
Properties
NetBackup, overview 238

Q

QIC 657
Queue on error 273
Queued job 218, 224

R

Random ports
setting on client 282

setting on server 272
Raw partition backups
on UNIX 96
when to use on UNIX 97
Raw partitions
backing up 85
restoring 85
Reboot
master server 314
Redirected restores 97
Registry
backup on Windows clients 86
restore on Windows clients 86
Remote Administration Console 324
Reports
(see Logs)
all log entries 200
client backups 198
copying from 196
customizing 193
images on media 206
interval for information 245
media contents 203
media list 201
media log entries 208
media summary 208
media written 209
printing 196
problems 199
running 192
saving 196
select server for 192
settings 195
status of backups 197
using the troubleshooting wizard 209
window description 192
Re-Queued job 218, 224
Required network interface 251
Re-read interval 272
restore_notify script 691
Restores
catalog backups 147
caution for alternate client 326
caution for alternate path 329
directed from the server 326
from duplicated backups 183
overview 3, 6
Raw partition 85
reducing search time 173
registry on Windows clients 86
restore_notify script 691
setting client permissions 263
symbolic links on UNIX 94
to alternate clients 326
Retention levels
(see Retention period)
default 116
Retention period
caution for setting 139
changing 247
guidelines for setting 640
mixing on media 117
precautions for setting 116
redefining 246
setting 115
user schedule 139
Retry
backups 242
restores 250
Retry count for busy files 310
Rmed media type 207
Robot numbers 31
RS-MTF1 format, allow overwrite 274

S

Save a report 196
Schedule
overview 44
adding to policy 108, 113
automatic, how processed 637
catalog backup 154
Dup button 120
examples, of automatic 125
frequency 112
naming 110
overview 6
priority 112
retention level 116
retention period
guidelines 640
setting 115
setting backup times 118
specify multiplexing 117
storage unit 114
type of backup 110
user backup or archive 138
volume pool 115
Schedule backup attempts 242

Scripts
backup_exit_notify 679
backup_notify 679
bpend_notify
UNIX 679
Windows 679
bpstart_notify
UNIX 679
Windows 679
dbbackup_notify 679
diskfull_notify 679
notification 679
restore_notify 679
session_notify 679
session_start_notify 679
userreq_notify 679
Search default 305
Sequent 397
Server and client speed 244
Server directed restore 326
Server independent restores 270
Server list
definition 254
on Servers tab 254
Server port window 274
Server reserved port window 267, 274
Server sends mail 253
Server, NetBackup
for manage storage units 320
host names, changing 630
multiple 408
power down 314
rebooting 314
select for reports 192
software 2
Servers tab 254
Services
monitoring 226
NetBackup Catalog Manager 315
NetBackup Client 316
NetBackup Device Manager 315
NetBackup Request Manager 315
NetBackup Volume Manager 316
overview 314
session_notify script 691
session_start_notify script 692
Source Copy Number 176
Spanning media
enabling 654, 656
tape format 658
Specify a preferred group 396
Stacker, gravity 656
Standalone drive
keeping in ready state 656
media selection 654
standalone extensions
disabling 655
enabling 654
using gravity stacker 656
Standard policy type 59
Start time, for schedule 118
Status bar 14
Status code 200
Status of Backups report 197
Stop / Restart Device Manager service 315
Storage unit group
change 36
create 35
delete 37
Storage units
overview 648
adding media manager type 27
adding NDMP type 26
changing server to manage 320
concurrent jobs (see jobs)
configure with the wizard 23
disk 113, 181
disk type, definition 22
example media manager type 24
for policy 60
for schedule 114
management window 22
media manager type, definition 22
NDMP 22, 26
next available 60
optical devices 113, 181
overview 7
QIC drive type 113, 181
rules for media manager type 23
Streaming (see Allow multiple data streams)
Sun PC NetLink 94
Suspend media 660
Suspended, media state 652, 653
Sybase policy type 60
Symbolic links
UNIX 94
System Commander and IDR 714
System_State

directive 99

T

Tape format
overview 657
fragmentation 658
multiplexed 658
non-QIC 657
QIC 657
Tape marks 642
Tape overhead, for catalogs 642
Tape spanning 654, 656
Tapes (see Media)
tar format, allow overwrite 274
Templates for directives 80
Third-party copies 113, 181
Throttling (see Bandwidth limiting)
Timeout
bpend 257
bpstart 257
bptm query 272
client connect 256
client read 250
overlap 305
Timeout in queue 272
Timeout in queue 272
Transfer rate 200, 633, 634
Traversing directories to back up a file 302
Tries, backup 242
Troubleshooting
general level setting 303
TCP level setting 303
Troubleshooting wizard
using in activity monitor 231
using in reports utility 209
True image restore
configuration 65, 671
move detection 65, 672
time to keep information 243
Type of backup 110

U

Uncompress
files before backing up (NetWare only) 311
Unfreeze media 652
Unhashed file 381
UNIX clients 297
Unmount media 659
UNSET, file list directive 105
UNSET_ALL, file list directive 105
Unsuspend media 652, 660
Updating IDR bootable media 704
User
backups, archives, restores 6
definition xxxi
schedules
planning 138
User directed timeout 292
userreq_notify script 692

V

Vault 219
configuring a policy 45
logical name 219
policy type 59
profile 219
vlteject command 142
vltrun command 142
Verbose Logging Level 260
Verify, backup images 177
Version, NetBackup
determining xxxi
View
properties of one license key 319
vlteject command 142
vltrun command 142
vnetd 262, 344
Volume database 650
Volume pool
for schedule 115
overview 650
policy 61
Volumes
allocation 650
assignments 650
scratch 650
vopie_util command 624
vopied 379
vopied command 622

W

Wait in queue 273
Wait time to clear archive bit 304
Wakeup Interval
specifying 242
Wildcard characters
escaping 300
escaping on UNIX 93, 675
in exclude files lists 300

in exclude lists 675
mac clients 92
UNIX file paths 93
windows clients 84
Wizard
backup policy 45
catalog backup 149
device configuration 23
disaster recovery 708
IDR preparation 697
starting from NetBackup Assistant 9
troubleshooter in activity monitor 231
troubleshooter in reports utility 209
Working directory for busy files 309
Worklist, prioritizing 639
Worksheet, planning 660