VERITAS™

VERITAS NetBackup™ 5.1

System Administrator's Guide, Volume II

for UNIX

N12314B

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 © 1993-2004 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS Software, the VERITAS logo, VERITAS NetBackup, and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation.VERITAS, the VERITAS Logo, VERITAS NetBackup Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

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

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000 Fax 650–527–2908
www.veritas.com

Third-Party Copyrights

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

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

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

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

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

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

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

Contents

Preface . . . . . **xix**

What Is In This Manual xix

Getting Help xx

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

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

NetBackup Manuals xxi

Glossary xxii

▼ *To access the NetBackup online glossary* xxiii

Accessibility Features xxiii

Using the Keyboard to Navigate in NetBackup xxiii

Navigating in a NetBackup Tree View xxiv

Using Accelerator Keys xxv

Using Mnemonic Keys xxv

Using the Keyboard in Dialogs xxv

Accessing Online Documentation xxvii

Conventions xxvii

Chapter 1. Access Management **1**

NetBackup Access Management Components 2

VxSS Components 2

Root Broker 2

Authentication Brokers 3

Security Administrator 3

Installation Overview 4

Order of Installation or Upgrade 4
VxSS Component Distribution 4
Installing and Configuring Access Control for Master Servers 5
Installing and Configuring Access Control for Media Servers 9
Installing and Configuring Access Control for Clients 12
Installing the Authentication Service Root Broker (Root + AB) 14
Configuring Authentication on the Root Broker for Use with NetBackup 15
Installing the Authorization Server 17
Configuring the Authorization Server 17
Configuring Access Control Host Properties 19
Master Server (Root Broker) Host Properties 19
Access Control Host Properties Dialog 19
VxSS Tab 20
Authentication Domain Tab 20
Authorization Service Tab 22
Verifying Master Server Settings 22
Access Management Troubleshooting Guidelines 24
Windows Verification Points 24
Master Server Verification Points 26
Media Server Verification Points 28
Client Verification Points 29
UNIX Verification Points 31
Master Server Verification Points 32
Media Server Verification Points 34
Client Verification Points 35
Verification Points in a Mixed Environment with a UNIX Master Server 37
Master Server Verification Points 39
Media Server Verification Points 39
Client Verification Points 40
Verification Points in a Mixed Environment with a Windows Master Server 42

Master Server Verification Points 44
Media Server Verification Points 44
Client Verification Points 45
Other Troubleshooting Topics 47
Expired Credentials Message 47
Useful Debug Logs 47
If Uninstalling VxSS 47
Where Credentials Are Stored 47
VxSS Ports 48
Stopping VxSS Daemons 48
If You Lock Yourself Out of NetBackup 48
nbac_cron Utility 49
Using the Access Management Utility 50
Access Management Menus 50
Determining Who Can Access NetBackup 52
Individual Users 52
User Groups 54
Default User Groups 54
Additional User Groups 55
User Group Configuration 56
▼ *To create a new user group* 56
▼ *To create a new user group by copying an existing user group* 56
Renaming User Groups 57
General Tab 57
Users Tab 57
Defining Users Groups and Users 58
Defining a User Group 59
▼ *To add a new user to a user group* 59
Permissions Tab 60
Authorization Objects and Permissions List 60

Permissions for Default NetBackup User Groups 61
Backup, Archive, and Restore (BAR) Client Interface 61
License Permissions 62
Jobs Tab in the Activity Monitor Permissions 62
Permissions in the Device Monitor 63
Daemon Tab Permissions in the Activity Monitor 64
Reports Permissions 65
Policy Permissions 65
Storage Units Permissions 66
Storage Unit Groups Permissions 66
Catalogs Permissions 67
Host Properties Permissions 68
Media Permissions 68
Volume Group Permissions 69
Volume Pools Permissions 69
Robots Permissions 70
Device Host Permissions 70

Chapter 2. Enhanced Authentication and Authorization 71
Common Configuration Elements 72
Configuration Files 72
methods.txt 72
methods_allow.txt 73
methods_deny.txt 74
names_allow.txt 75
names_deny.txt 76
authorize.txt 76
Library Files 78
Commands 78
bpauthorize 78

bpauthsync 78
vopie_util 79
Processes 79
vopied Daemon 79
Files 79
vopie Files 79
temp File 81
Enhanced Authentication 82
Using vopie Enhanced Authentication 82
▼ *To use the vopie enhanced authentication method* 82
vopie Enhanced Authentication Examples 83
Using noauth Rather than vopie Authentication 87
Troubleshooting Authentication 91
Enhanced Authorization 91
Enhanced Authorization Process 92
Gaining Access to a Server 92
Gaining Access to a Client 93
Configuring NetBackup Enhanced Authorization 94
Enabling NetBackup Enhanced Authentication 94
Adding an Authorized User 95
▼ *To create a list of authorized users* 95
Using the Administration Console to Specify Preferred Groups (Optional) . . . 95
▼ *To specify a preferred group* 96
Example Configuration 97

Chapter 3. Additional Configuration 99
Multiplexing 100
When to Use Multiplexing 100
How to Configure Multiplexing 101
Maximum Multiplexing Per Drive for Storage Unit 101

Media Multiplexing for a Schedule 101
Other Configuration Settings to Consider Using Multiplexing 104
Demultiplexing 105
Using Multiple NetBackup Servers 105
Configuring a Master and Media Server Grouping 106
Software on Each Server 109
NetBackup Catalogs 109
NetBackup and Media Manager Daemons 109
▼ *To add media servers* 110
Dynamic Host Name and IP Addressing 113
Setting up Dynamic IP Addresses and Host Names 114
Configuring the NetBackup Master Server 115
Configuring a Dynamic Microsoft Windows Client 117
Configuring a Dynamic UNIX NetBackup Client 117
Bandwidth Limiting 118
Read This First 118
How Bandwidth Limiting Works 119
Configuration 119
Rules for IP Address Ranges 120
Rules for Setting Bandwidth Values 121
Examples 122
Example 1 122
Example 2 122
Example 3 122
Busy-File Processing (UNIX Clients Only) 122
Getting Started 123
Modifying bp.conf 123
BUSY_FILE_PROCESSING 124
BUSY_FILE_DIRECTORY 124
BUSY_FILE_ACTION 124

Examples 125
Creating Action Files 125
Logs Directory 127
Modifying bpend_notify_busy 128
Configuring E-mail Notifications 129
Specifying the Locale of the NetBackup Installation 130
Adjusting Time Zones in the NetBackup-Java Console 131
▼ *To set the time zone and Daylight Savings Time* 132
NetBackup Configuration Options 134
Method for Specifying the Configuration Options 134
Syntax Rules for bp.conf Options 135
bp.conf Options for Master Servers 136
ALLOW_MEDIA_OVERWRITE 136
ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA 137
ALLOW_NON_RESERVED_PORTS 137
AUTHENTICATION_DOMAIN 137
AUTHORIZATION_SERVICE 138
BPBRM_VERBOSE 139
BPDBJOBS_COLDEFS 140
BPDBM_VERBOSE 142
BPRD_VERBOSE 143
BPSCHED_VERBOSE 144
BPTM_VERBOSE 144
BPEND_TIMEOUT 145
BPSTART_TIMEOUT 145
BPTM_QUERY_TIMEOUT 146
CHECK_RESTORE_CLIENT 146
CLIENT_CONNECT_TIMEOUT 146
CLIENT_PORT_WINDOW 146
CLIENT_READ_TIMEOUT 147

CLIENT_RESERVED_PORT_WINDOW 147
CONNECT_OPTIONS 148
DISABLE_JOB_LOGGING 149
DISABLE_STANDALONE_DRIVE_EXTENSIONS 150
DISABLE_SCSI_RESERVE 150
DISALLOW_BACKUPS_SPANNING_MEDIA 150
DISALLOW_CLIENT_LIST_RESTORE 150
DISALLOW_CLIENT_RESTORE 151
FAILOVER_RESTORE_MEDIA_SERVERS 151
FORCE_RESTORE_MEDIA_SERVER 152
GENERATE_ENGLISH_LOGS 152
INCOMPLETE_JOB_CLEAN_INTERVAL 152
INITIAL_BROWSE_SEARCH_LIMIT 153
KNOWN_MASTER 153
LIMIT_BANDWIDTH 153
MASTER_OF_MASTERS 154
MEDIA_ID_PREFIX 155
MEDIA_UNMOUNT_DELAY 155
MEDIA_REQUEST_DELAY 155
MEDIA_SERVER 156
MPX_RESTORE_DELAY 156
MUST_USE_LOCAL_DRIVE 156
QUEUE_ON_ERROR 156
RANDOM_PORTS 157
RE_READ_INTERVAL 157
REQUIRED_INTERFACE 158
SERVER 159
SERVER_PORT_WINDOW 160
SERVER_RESERVED_PORT_WINDOW 160
SKIP_RESTORE_TO_SYMLINK_DIR 161

SERVER_CONNECT_TIMEOUT 162
SPC_SERVER 162
TIMEOUT_IN_QUEUE 162
UNLINK_ON_OVERWRITE 162
USE_VXSS 163
VERBOSE 164
VXSS_NETWORK 164
WAIT_IN_QUEUE 165
bp.conf Options for UNIX Clients 166
ALLOW_NON_RESERVED_PORTS 167
AUTHENTICATION_DOMAIN 167
BPARCHIVE_POLICY 167
BPARCHIVE_SCHED 168
BPBACKUP_POLICY 168
BPBACKUP_SCHED 168
BUSY_FILE_ACTION 168
BUSY_FILE_DIRECTORY 169
BUSY_FILE_NOTIFY_USER 169
BUSY_FILE_PROCESSING 170
CLIENT_NAME 170
CLIENT_PORT_WINDOW 170
CLIENT_READ_TIMEOUT 170
CLIENT_RESERVED_PORT_WINDOW 171
COMPRESS_SUFFIX 171
CRYPT_CIPHER 171
CRYPT_KIND 172
CRYPT_OPTION 172
CRYPT_STRENGTH 173
CRYPT_LIBPATH 173
CRYPT_KEYFILE 174

DISALLOW_SERVER_FILE_WRITES 174
DO_NOT_RESET_FILE_ACCESS_TIME 174
GENERATE_ENGLISH_LOGS 175
IGNORE_XATTR 175
INFORMIX_HOME 175
INITIAL_BROWSE_SEARCH_LIMIT 175
KEEP_DATABASE_COMM_FILE 176
KEEP_LOGS_DAYS 176
LIST_FILES_TIMEOUT 176
LOCKED_FILE_ACTION 176
MEDIA_SERVER 176
MEGABYTES_OF_MEMORY 177
NFS_ACCESS_TIMEOUT 177
RANDOM_PORTS 177
RESTORE_RETRIES 177
REQUIRED_INTERFACE 177
SERVER_PORT_WINDOW 178
SERVER 178
SYBASE_HOME 178
USE_CTIME_FOR_INCREMENTALS 179
USE_VXSS 179
USEMAIL 179
VERBOSE 180
VXSS_NETWORK 180
UNIX Client Examples 180
Example /usr/openv/netbackup/bp.conf File 180
Example $HOME/bp.conf File 180
Restricting Administrative Privileges of Media Servers 181

Chapter 4. Using bpadm 183
Starting bpadm 184
Defining and Managing Storage Units 185
Adding a Removable or Robotic Storage Unit 185
▼ *To add a removable or robotic storage unit* 187
Adding a Disk Type Storage Unit 189
▼ *To add a disk type storage unit* 189
Displaying and Changing Storage Unit Configurations 190
▼ *To use the Storage Unit Management menu* 191
Defining and Managing Storage Unit Groups 192
Adding a Storage Unit Group 192
▼ *To add a storage unit group* 193
Displaying and Changing Storage Unit Group Configurations 193
▼ *To view or change storage unit group configurations* 193
Defining and Managing Policies 194
Adding a Policy 195
▼ *To add a policy to the configuration* 195
Displaying and Changing Policy Configurations 199
▼ *To view or change policy configurations* 199
Defining and Managing the Client List for a Policy 199
Adding Clients to a Policy 200
▼ *To add clients to a policy* 200
Displaying Client Lists and Deleting Clients from a Policy 202
▼ *To view client lists or delete clients from a policy* 202
Defining and Managing the Selections List for a Policy 203
Adding to a Selections List 203
▼ *To add entries to a selections list* 203
Displaying and Changing a File List 204
▼ *To view file lists or delete files from a policy* 204
Defining and Managing Schedules for a Policy 205

Adding a Schedule 205
▼ *To add either an automatic or user-directed schedule* 205
Displaying and Modifying a Schedule 210
▼ *To view or modify schedules* 210
Defining NetBackup Global Attributes 210
▼ *To list or modify Global attributes* 211
Installing NetBackup Software on All Trusting Client Hosts 214
Displaying Reports 215
▼ *To view reports or change report parameters* 215
▼ *To view media reports or change report parameters* 217
Managing bprd (NetBackup Request Daemon) 218
▼ *To manage the request daemon* 219
Redefining Retention Levels 219
▼ *To redefine retention levels* 220
Performing Manual Backups 221
▼ *To perform manual backups* 221
Backing Up the NetBackup Databases (Catalogs) 222
Listing Database Backup Settings 223
Modifying Database Backup Settings 226
Deleting Database Backup Media ID 229
Performing Manual Database Backups 229
Adding Database Backup File Paths 229
▼ *To add database backup paths* 230
Removing Database Backup File Paths 231

Chapter 5. Reference Topics 233
Rules for Using Host Names in NetBackup 234
Qualifying Host Names 234
How NetBackup Uses Host Names 234
Server and Client Name on UNIX Servers and Clients 234

Host Names on Windows Servers and PC Clients 235
Policy Configuration 235
Image Catalog 235
Error Catalog 236
Scheduler 236
Catalog Backup Information 236
How to Update NetBackup After Host Name Changes 236
Special Considerations For Domain Name Service (DNS) 237
Terminal Configuration on UNIX 238
Modifying the XKeysymDB File 238
Modifying the terminfo File 238
Changing X Resources for xbp 239
Reading Backup Images with tar 241
Effects of Using a Non-NetBackup tar 241
▼ *To restore files using a non-NetBackup tar* 242
Possible Files Generated By tar 244
Factors Affecting Backup Time 244
Total Data 245
Transfer Rate 245
Compression 246
Device Delays 246
Determining NetBackup Transfer Rate 246
Network Transfer Rate 246
Network Transfer Plus End-of-Backup-Processing Rate 246
Total Transfer Rate 247
Examples 247
How NetBackup Builds Its Automatic Backup Worklist 249
Building the Worklist (Queue) 249
Prioritizing the Worklist 251
Guidelines for Setting Retention Periods 252

Guidelines for Setting Backup Frequency 253
Determining Backup Media Requirements 253
Media Catalog 254
Planning Worksheets 255

Chapter 6. NetBackup Notify Scripts 267
backup_notify 268
backup_exit_notify 269
bpstart_notify (UNIX clients only) 269
bpstart_notify.bat (Microsoft Windows clients only) 271
bpend_notify (UNIX clients only) 273
bpend_notify.bat (Microsoft Windows clients only) 276
dbbackup_notify 278
diskfull_notify 279
restore_notify 279
session_notify 280
session_start_notify 280
userreq_notify 280

Chapter 7. Using NetBackup With AFS 283
Installation 283
System Requirements 283
Server and Client Installation 283
Configuration 283
General Policy Attributes 284
Client List 284
Backup Selections 284
Backup Selection List Directives 284
Regular Expressions 285
Exclude and Include Lists 286
Backups and Restores 286

Backups 286
Automatic Backup 286
Manual Backup 286
Restores 286
Restore From the NetBackup for AFS Client 287
Restore From the NetBackup Master Server 287
Notes About Restores 287
Troubleshooting 288
Troubleshooting Backups 288
Troubleshooting Restores 289

Chapter 8. Intelligent Disaster Recovery 291
Supported Windows Editions 292
Requirements for IDR 292
Overview of IDR Use 293
About the DR Files 294
Configuring NetBackup Policies for IDR 294
Backing Up the System to be Protected 295
Creating IDR Media 295
Choosing the Bootable Media 296
Creating Bootable Diskettes 297
▼ *To create bootable diskettes* 298
Modifying Diskette Sets for Use with Multiple Windows 2000 Computers . . 299
Creating a Bootable CD Image 299
▼ *To create a bootable CD image* 300
Creating IDR Diskettes 301
▼ *To create IDR diskettes* 301
Updating IDR Media 302
Updating a Bootable CD 302
Updating Bootable Diskettes 302

▼ *To update IDR bootable diskettes* 302
Updating IDR Diskettes Only 303
▼ *To update IDR diskettes using IDR Preparation Wizard* 303
Using drfile.exe to Create or Update a DR File 304
Recovering Your Computer 305
Step 1: Boot Your Computer 306
▼ *To boot a computer using a bootable diskette* 306
▼ *To boot from a bootable CD* 306
Step 2: Windows Setup in IDR Recovery 307
▼ *To use Windows setup in IDR recovery* 307
Step 3: Disaster Recovery Wizard 307
▼ *To use the Disaster Recovery Wizard* 308
Notes on Altering Hard Drive Partition Sizes 311
Notes on Recovering Specific Platforms 311
Recovering the Dell PowerEdge 6100/200 with RAID 311
▼ *Use the following steps with your IDR recovery diskette set* 312
Recovering IBM Computers 312
Recovering Compaq Computers 312
IDR Frequently Asked Questions 313

Index 315

Preface

This guide describes how to configure and manage the operation of VERITAS NetBackup Server and VERITAS NetBackup Enterprise Server for Windows and applies to all supported platforms and operating systems. See the *NetBackup Release Notes* for a list of the hardware and operating system levels that NetBackup supports.

What Is In This Manual

- Chapter 1, "Access Management," discusses how to install the VERITAS Security Subsystem (VxSS) component and configure your system to use NetBackup access control. Permission to perform specific actions within the NetBackup Administration Console is granted to defined user groups.
- Chapter 2, "Enhanced Authentication and Authorization," discusses configuring your system to use the enhanced authentication and authorization available in this release.
- Chapter 3, "Additional Configuration," explains how to configure features and parameters that seldom, if ever, require changing.
- Chapter 4, "Using bpadm," explains the tasks that can be performed with the `bpadm` interface.
- Chapter 5, "Reference Topics," provides further information about configuration that applies specifically to UNIX servers and clients.
- Chapter 6, "NetBackup Notify Scripts," provides information about scripts that collect information and provide notification of events.
- Chapter 7, "Using NetBackup With AFS," provides information about using NetBackup to back up AFS clients.
- Chapter 8, "Intelligent Disaster Recovery," explains how to use Intelligent Disaster Recovery for Windows.

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Technical Support Web Site

The VERITAS Support Web site allows you to:

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

The address for the VERITAS Technical Support Web site follows:

- http://support.veritas.com

Subscribing to VERITAS Email Notification Service

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

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

Accessing VERITAS Telephone Support

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

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

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

Accessing VERITAS E-mail Support

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

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

Contacting VERITAS Licensing

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

NetBackup Manuals

The following manuals, along with the online help, comprise the NetBackup documentation set. The manuals are provided in Adobe Portable Document Format (PDF) on the NetBackup CD-ROM.

- *NetBackup Release Notes for UNIX and Windows*

  Provides important information about NetBackup Server and Enterprise Server 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 Installation Guide for UNIX*

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

- *VERITAS Security Services Installation Guide*

  Explains install and configure the VERITAS Security Services. This manual is found on the VERITAS Security Services CD-ROM.

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

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

- *NetBackup Backup, Archive, and Restore Getting Started Guide*

  Explains how to use the NetBackup Backup, Archive, and Restore interface to perform basic backup and restore operations for UNIX and Windows systems.

- *VERITAS Security Services Administrator's Guide*

  Explains how to configure and manage core security mechanisms, including authentication, protected communications, and authorization. This manual is found on the VERITAS Security Services CD-ROM.

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

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

- *NetBackup Vault Operator's Guide for UNIX and Windows*

  Describes procedures for sending tapes offsite, receiving tapes on site, and running reports on offsite media and vault jobs.

- *NetBackup Commands for UNIX*

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

- *NetBackup Troubleshooting Guide for UNIX and Windows*

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

Glossary

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

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

▼ **To access the NetBackup online glossary**

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

Use the scroll function to navigate through the glossary.

Accessibility Features

The NetBackup interface can be used by people who are vision impaired and by people who have limited dexterity. Accessibility features include the following:

- Using the Keyboard to Navigate in NetBackup
- Accessing Online Documentation

Note Text that appears in the NetBackup 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 in the NetBackup interface:

- Press window navigation keys to move from one window element to another. For example, press **Tab** to move from one pane to another.
- Perform common actions quickly using accelerator keys. Accelerator keys let you initiate actions without first accessing a menu. For example, press **Ctrl+n** to create a new policy.
- Press mnemonic keys to select items using only the keyboard. Mnemonic keys are indicated by an underlined letter. For example, press **Alt+h** to access the **Help** menu.
- You can also use the keyboard to select control options in a dialog.

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**	Moves to the next (right or down) pane in the active NetBackup window.
Shift+Tab or **Shift+F6**	Moves to the previous (left or up) pane in the active NetBackup window.
Ctrl+Tab or **Ctrl+F6**	Moves to the next (right or down) NetBackup window.
Ctrl+Shift+Tab or **Ctrl+Shift+F6**	Moves to the previous (left or up) NetBackup window.
Plus Sign (**+**) on the numeric keypad	Expands the highlighted item.
Minus Sign (**–**) on the numeric keypad	Collapses the highlighted item.
Asterisk (*) on the numeric keypad	Expands the entire tree below the first item in the active NetBackup 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	Selects the next item up in the pane.
Shift+Down Arrow	Selects the next item down in the pane.
Page Up	Moves to the top item visible in a pane.
Page Down	Moves to the bottom item visible in a pane.
Home	Moves to the first item (whether visible or not) in a pane.
End	Moves to the last item (whether visible or not) in a pane.
Right Arrow	Expands the highlighted item. If the highlighted item does not contain hidden items, using the **Right Arrow** has the same effect as using the **Down Arrow**.

Keyboard Input	Result
Left Arrow	Collapses the highlighted item. If the highlighted item does not contain expanded items, using the **Left Arrow** has the same effect as using the **Up Arrow**.
Alt+Right Arrow	Moves to the next (right or down) option control in the interface.
Alt+Left Arrow	Moves to the previous (left or up) option control in the interface.
Alt+Spacebar	Displays the NetBackup window menu.

Using Accelerator Keys

Accelerator keys let you use NetBackup from the keyboard, rather than using the mouse. 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 refresh the information in the window, press **F5**.

Using Mnemonic Keys

A mnemonic key is a keyboard equivalent for a mouse click that is used to activate a component such as a menu item. To select a menu item, press the **Alt** key to initiate menu pull-down mode, then press a mnemonic key to open a menu, and another mnemonic key to select a menu item.

Mnemonics are case-insensitive. Keys can be pressed either sequentially or simultaneously.

For example, to change the Master Server, press and hold the **Alt** key then press the **f** key to pull down the File menu, and press the **c** key to invoke the **Change Server** menu option.

Using the Keyboard in Dialogs

To select or choose controls that have an underlined letter in their titles, type **Alt+***underlined_letter* at any time when the dialog is active. For example, typing **Alt+O** is the same as clicking the OK button in a dialog.

To move forward (right or down) from one control to the next, press **Tab**. To reverse the direction (for example, from moving right to moving left), press **Tab** and **Shift**.

To move within a list box, groups of option controls, or groups of page tabs, press the arrow key that points the direction you want to move.

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 carries out the command you have chosen, using the information supplied in the dialog. This button is generally labeled **OK**. Other command buttons let you cancel the command or choose from additional options.

- Command buttons containing an ellipsis (...)

  Command buttons containing 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 outlined by a dark border

  A dark border around a button initially indicates the default button. Press **Enter** or the **Spacebar** at any time to choose the button with a dark border. Press **Tab** to move the keyboard focus to the next control. When you change focus to a command button, it temporarily has the dark border. If the focus is not on a control, the dark border returns to the default command button in the pane.

- Check boxes

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

  Press **Tab** to move from one checkbox to another and the **Spacebar** to change the check box to the next state. Typing the mnemonic key for a check box also moves the focus to the box and changes its state.

- Option controls (also known as radio buttons)

  Option controls are used to select only one option from a group of options. (Option buttons may represent two or three states, as checkboxes do.) Press **Tab** to move to an option button and press the **Spacebar** to initiate the option. Type the mnemonic key for an option control to move the focus to the control and select it.

- Page series

  A series of 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. Press **Tab** to move to the name of the page, then use right and left arrows to highlight a different page name. Press **Return**.

Accessing 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 (or as an option for downloading if the release is available from the Web). For a complete list of NetBackup documents, see the NetBackup release notes.

Conventions

The following conventions apply throughout the documentation set.

Product-Specific Conventions

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

- Microsoft Windows, Windows

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

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

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

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the **Password** field.

Conventions (continued)

Convention	Description
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces. This font is also used to highlight NetBackup server-specific or operating system-specific differences. For example: *This step is only applicable for NetBackup Enterprise Server.*
`Code`	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

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

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

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

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

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

Command Usage

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

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

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

`command` *`arg1`*`|`*`arg2`*

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

Navigating Multiple Menu Levels

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

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

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

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

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

Access Management 1

Access to NetBackup can be controlled by defining user groups and granting explicit permissions to these groups. Configuring user groups and assigning permissions is done using **Access Management** in the NetBackup Administration Console.

This chapter discusses how to set up and manage access to NetBackup. It contains the following sections:

- "NetBackup Access Management Components" on page 2
- "Installation Overview" on page 4
- "Installing and Configuring Access Control for Master Servers" on page 5
- "Installing and Configuring Access Control for Media Servers" on page 9
- "Installing and Configuring Access Control for Clients" on page 12
- "Installing the Authentication Service Root Broker (Root + AB)" on page 14
- "Installing the Authorization Server" on page 17
- "Access Management Troubleshooting Guidelines" on page 24
- "Using the Access Management Utility" on page 50
- "Determining Who Can Access NetBackup" on page 52

Note *Access Management* and *Enhanced Authorization and Authentication* (see Chapter 2) are independent methods of Access Control. Access Management is the newest and will be the preferred method in future NetBackup releases. If both Access Management and Enhanced Authorization and Authentication are configured, Access Management takes precedence.

NetBackup Access Management Components

NetBackup uses the VERITAS Security Services (VxSS) to help implement core security. VxSS is a set of shared VERITAS infrastructure services, installed from the VxSS installation CD. The CD is packaged as part of NetBackup.

Note NetBackup Access Management relies on the use of home directories. Please see the documentation for your operating system for more information on home directories.

VxSS Components

When you install VxSS, you're installing and configuring the following services and client software:

- Authentication (At Server, At Client)

  Authentication is the process of proving your identity to the VxSS system. Authentication is accomplished by communicating with the daemon which, in turn, validates your identity with the operating system.

  For more information on authentication or the authentication daemon (`vxatd`), see the *VERITAS Security Services Administrator's Guide* found on the VxSS installation CD.

- Authorization (Az Server, Az Client)

  Authorization is the process of verifying that an identity has permission to perform the desired action. NetBackup verifies permissions with the authorization daemon for most actions. In many cases, NetBackup alters what information is accessible from the command line and Administration Console.

  For more information on authorization or the authorization daemon (`vxazd`), see the *VERITAS Security Services Administrator's Guide* found on the VxSS installation CD.

Root Broker

A Root Broker is a NetBackup server that has VxSS Authentication Server and Authorization Server installed and is configured to be a Root Broker. There is always one Root Broker in every NetBackup Access Management configuration.

The Root Broker acts as the most trusted certification authority, implementing a registration authority for Authentication Brokers, as well as itself.

While a Root Broker can authenticate an Authentication Broker, an Authentication Broker cannot authenticate a Root Broker.

In many cases, the Root Broker will also be an Authentication Broker. This chapter describes installing VxSS services, then it describes configuring the NetBackup server to be a Root Broker and an Authentication Broker (Root Broker + AB). For more information on the authentication Root Broker, see the *VERITAS Security Services Administrator's Guide*.

Authentication Brokers

An Authentication Broker is a server that has VxSS Authentication Server and Authorization Server installed. This machine is part of the Root Broker's private Access Management domain. An Authentication Broker can authenticate clients, but not other brokers.

The member of the NetBackup Security Administrator user group can choose which Authentication Broker a client should contact for authentication. (See "Configuration Containing Windows Systems Only" on page 25 or "Configuration Containing UNIX Systems Only" on page 31 for a depiction of this configuration.)

For example:

- A Windows 2000 client uses a Windows Authentication Broker for authentication.
- A UNIX client uses a UNIX Authentication Broker for authentication.
- For more information on authentication brokers, see the *VERITAS Security Services Administrator's Guide*.

Security Administrator

The user who installs and configures VxSS software for use with NetBackup Access Management is, by default, a member of the *NBU_Security Admin* user group. This chapter will refer to a member of the *NBU_Security Admin* group as a Security Administrator. Users can be added to the group, but there are usually few members.

Members of the *NBU_Security Admin* user group are the only users who can view the contents of **Access Management** > **Users** and **Access Management** > **NBU User Groups** in the NetBackup Administration Console. Security Administrators are the only users allowed to create user groups, assign users to the groups, and define permissions for the groups. However, Security Administrators, by default, do not have permission to perform any other NetBackup administration activities. (See "Security Administrator (NBU_Security Admin)" on page 54.)

Note The administrator group (Windows) or `root` (UNIX) is always a member of the *NBU_Security Admin* group on the system where the Authorization daemon runs. See the *VERITAS Security Services Administrator's Guide* for information on this special identity.

Installation Overview

For a detailed installation description, see "Installing and Configuring Access Control for Master Servers" on page 5.

Order of Installation or Upgrade

1. Complete all NetBackup master server installations or upgrades.
   a. Complete Root + AB installation of VxSS Authentication server.
   b. Complete VxSS Authorization server installation.
   c. Configure master servers for NetBackup Access Control.
2. Complete all NetBackup media server installations or upgrades, then configure media servers for NetBackup Access Control.
3. Complete all NetBackup client installations or upgrades, then configure clients for NetBackup Access Control. See "Installing and Configuring Access Control for Clients" on page 12.

VxSS Component Distribution

The VxSS components can be distributed throughout a configuration, just as NetBackup can distribute master servers, media servers and clients.

Note Although the Authentication broker and Authorization broker can technically be placed on any machine, VERITAS currently recommends that the root Authentication broker and Authorization broker be placed on the NetBackup master server. At a minimum, the root Authentication broker must reside on the master server.

For specific VxSS installation information, refer to the *VERITAS Security Services Installation Guide*, found on the VxSS installation CD.

NetBackup Installation	Required Authentication Component	Required Authorization Component
Master server	At server	Az server
Media server	At client	Az client

NetBackup Installation	Required Authentication Component	Required Authorization Component
Client	At client	None
Windows Remote Administration Console (only)	At client	Az client
Java Windows Display Console (only)	None	None

The following sections describe some actions you can take to verify that the components are correctly installed in a mixed environment:

- "Windows Verification Points" on page 24
- "UNIX Verification Points" on page 31
- "Verification Points in a Mixed Environment with a UNIX Master Server" on page 37
- "Verification Points in a Mixed Environment with a Windows Master Server" on page 42
- "UNIX Verification Points" on page 31

Installing and Configuring Access Control for Master Servers

The following steps describe configuring NetBackup Access Control for the master server in a NetBackup configuration. A master server requires Authentication Server and Client software and Authorization Server and Client software.

Throughout this chapter, in the configuration examples we'll refer to the following host names:

	Windows	UNIX
Master Servers	win_master	unix_master
Media Servers	win_media	unix_media
Clients	win_client	unix_client

1. Complete all NetBackup master server installations or upgrades.

2. Using the VxSS installation CD, install both the VxSS Authentication Server and Client software on the master server. This master server will be a Root + AB (Authentication Broker).

   See "Installing the Authentication Service Root Broker (Root + AB)" on page 14 and the *VERITAS Security Services Installation Guide* on the VxSS installation CD.

3. Using the VxSS installation CD, install the VxSS Authorization Server and Client software on the master server. To do this, you must perform a custom installation.

   See "Installing the Authorization Server" on page 17 and the *VERITAS Security Services Installation Guide* on the VxSS installation CD.

4. Create a machine account for the master server. Make sure that the Authentication and the Authorization services are running. See "UNIX Verification Points" on page 31 or "Windows Verification Points" on page 24.

   The command in this step must be run as either `root` (UNIX) or as a member of the local Administrator group (Windows) on the Root+AB Authentication broker. For more information about this step, see "Configuring Authentication on the Root Broker for Use with NetBackup" on page 15.

   `bpnbat` is located in directory `/usr/openv/netbackup/bin/`

   ```
   bpnbat -addmachine
   Does this machine use Dynamic Host Configuration Protocol (DHCP)?
   (y/n) n
   Authentication Broker: win_master
   Authentication port[ Enter = default]:
   Machine Name: win_master
   Password: *******
   Password: *******
   Operation completed successfully.
   ```

5. Log in to the machine account for the master server.

   For more information about this step, see "Configuring Authentication on the Root Broker for Use with NetBackup" on page 15.

   ```
   bpnbat -LoginMachine
   Does this machine use Dynamic Host Configuration Protocol (DHCP)?
   (y/n) n
   Authentication Broker: win_master
   Authentication port[ Enter = default]:
   Machine Name: win_master
   Password: *******
   Operation completed successfully.
   ```

Note Repeat this step for each alias used by NetBackup.

6. Create the first Security Administrator (bootstrapping security).

   For more information about this step, see "Configuring the Authorization Server" on page 17.

   `bpnbaz` is located in directory `/usr/openv/netbackup/bin/admincmd`

```
bpnbaz -setupsecurity win_master
Please enter the login information for the first Security
Administrator other than root/Administrator. This identity
will be added to the security administrators group
(NBU_Security Admin), and to the netbackup administrators
group (NBU_Admin). It will also be used to build the initial
security information.

Authentication Broker: win_master
Authentication port[ Enter = default]:
Authentication type (NIS, NIS+, NT, vx, UNIXpwd: nt
Domain: domain1
Login Name: admin1
Password: ******
Processing - please be patient
Operation completed successfully.
```

7. Add the master server as a host authorized to perform Authorization checks.

   For more information about this step, see "Configuring the Authorization Server" on page 17.

```
bpnbaz -AllowAuthorization win_master
Operation completed successfully.
```

8. Configure the Access Control host properties of the master server.

   For more information about this step, see "Configuring Access Control Host Properties" on page 19.

   - Set VERITAS Security Services to **Automatic** or **Required**. (If some clients will not use NetBackup Access Control, set to **Automatic**.)
   - On the VxSS tab, add the host to the VxSS network (*win_master)*. (If the VxSS property is set to **Required**, this tab is not available.)
   - On the Authentication Domain tab, add authentication domain(s) and the host that will act as the broker for the domain (*domain1)*.

The broker is a machine using an operating system supporting the domain type that has the VxSS Authentication service installed on it.

- On the Authorization Service tab, specify the master server on which you installed the VxSS Authorization service (*win_master)*.

After changing the host properties, recycle the server daemons for the changes to take effect.

Installing and Configuring Access Control for Media Servers

The following steps describe configuring NetBackup Access Control for a media server in a NetBackup configuration. A media server requires Authentication Client software and Authorization Client software.

1. Complete all NetBackup media server installations or upgrades.

2. Using the VxSS installation CD, install Authentication Client software on the system.

3. Using the VxSS installation CD, install the Authorization Client software on the media server.

4. On the master server, create a machine account for the media server. Make sure that the Authentication and the Authorization services are running. See "UNIX Verification Points" on page 31 or "Windows Verification Points" on page 24.

   The command in this step must be run as either `root` (UNIX) or as a member of the local Administrator group (Windows) on the Root+AB Authentication broker. For more information about this step, see "Configuring Authentication on the Root Broker for Use with NetBackup" on page 15.

   `bpnbat` is located in directory `/usr/openv/netbackup/bin`

   On the master server, run:

   ```
   bpnbat -addmachine
   Does this machine use Dynamic Host Configuration Protocol (DHCP)?
   (y/n) n
   Authentication Broker: win_master
   Authentication port[ Enter = default]:
   Machine Name: win_media
   Password: *******
   Password: *******
   Operation completed successfully.
   ```

5. Log in to the machine account for the media server.

   For more information about this step, see "Configuring Authentication on the Root Broker for Use with NetBackup" on page 15.

   On the media server, run:

   ```
   bpnbat -LoginMachine
   Does this machine use Dynamic Host Configuration Protocol (DHCP)?
   (y/n) n
   Authentication Broker: win_master
   ```

```
Authentication port[ Enter = default]:
Machine Name: win_media
Password: *******
Operation completed successfully.
```

Note Repeat this step for each alias used by NetBackup.

6. Add the media server as a host authorized to perform Authorization checks.

   For more information about this step, see "Configuring the Authorization Server" on page 17.

   `bpnbaz` is located in directory `/usr/openv/netbackup/bin/admincmd`

   On the master server, run:

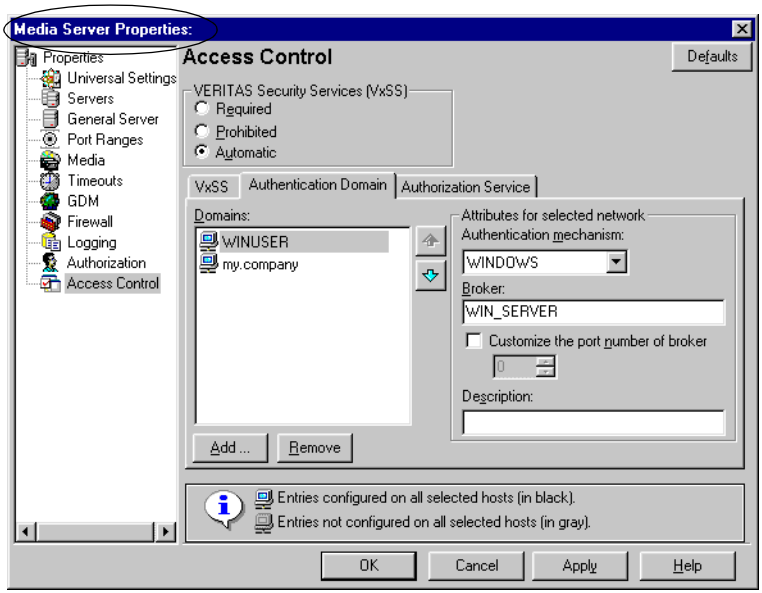
   ```
   bpnbaz -AllowAuthorization win_media
   Operation completed successfully.
   ```

7. Set up the proper Access Control host properties for the media server. The properties are described in "Configuring Access Control Host Properties" on page 19.

   a. Open Access Control host properties for the media server *(win_media)* through the master server. In the NetBackup Administration Console, select **NetBackup Management** > **Host Properties** > **Media Server** > *Select media server win_media* > **Access Control**.

      - Set VxSS mode to **Required**. If some clients will not use NetBackup Access Control, set to **Automatic**.

- Add authentication domains based on the systems where you have installed Authentication servers and the Authentication methods supported.
  For example, given a Windows system configured for Authentication using domain `WINUSER`, and a UNIX system configured for Authentication using the NIS domain `my.min.com`, the tab would look like the following:



- On the Authorization Services tab, indicate the host that will perform authorization for this media server.

b. Configure Access Control on the master server *(win_master)* for the media server:

On the VxSS tab, add win_media.min.com to the **VxSS Network** list as **Required**.

Installing and Configuring Access Control for Clients

The following steps describe configuring NetBackup Access Control for a client in a NetBackup configuration. A client requires Authentication Client software.

1. Install NetBackup client software on the system.

2. Using the VxSS installation CD, install Authentication client software on the system.

   Using `bpnbat`, register the client with the Authentication Broker, as described in step 2 on page 15.

   For example, if registering a machine *(win_client)* with the Authentication Broker *(win_master)*, run the following command on the At server *(win_master)*.

   a. **To add the client locally to the private domain, run the following command on the master server:**

```
bpnbat -AddMachine
Does the machine use Dynamic Host Configuration Protocol (DHCP)?
(y/n) n
Authentication Broker: win_master.min.com
Authentication Port: [Enter = Default]:
Name: win_client.min.com
Password:  [any password]
Password:  [enter password again]
Operation completed successfully.
```

   b. **To create a credential for the client, run the following command on the client:**

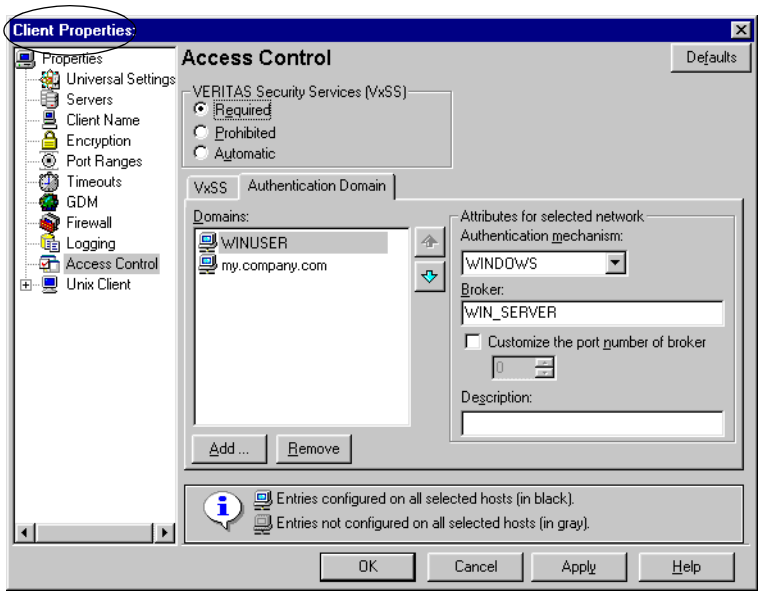
   Run the following command on the At client *(win_client)*.

```
bpnbat -loginmachine
Does this machine use Dynamic Host Configuration Protocol (DHCP)?
(y/n) n
Authentication Broker: win_master.min.com
Authentication port[ Enter = default]:
Name: win_client.min.com
Password: [same password as in step a]
Operation completed successfully.
```

3. Set up the proper Access Control host properties for the client. The properties are described in "Configuring Access Control Host Properties" on page 19.

a. Open Access Control host properties for the client *(win_client)* through the master server. In the NetBackup Administration Console, select **NetBackup Management** > **Host Properties** > **Clients** > *Select client win_master* > **Access Control**.

- Set VxSS mode to **Required**.
- Add authentication domains based on the systems where you have installed Authentication servers and the Authentication methods supported.
  For example, given a Windows system configured for Authentication using domain `WINUSER`, and a UNIX system configured for Authentication using the NIS domain `my.min.com`, the tab would look like the following:



b. Set up Access Control on the master server *(win_master)* for the client:

On the VxSS tab, add win_client.min.com to the **VxSS Network** list as **Required**.

Installing the Authentication Service Root Broker (Root + AB)

Before installing the VxSS services that will create a Root Broker that is also an Authentication Broker, check that the following conditions are true:

- Make sure that you are root on the system where you plan to install the VxSS Root Broker software. To become root, enter the following command:

  ```
  su -
  ```

- After becoming `root`, verify that root's home directory is correctly specified. Use the following command:

  ```
  echo $HOME
  ```

- If NetBackup is currently installed, shut down all NetBackup services before installing VxSS software.

Install the VxSS Root Broker software from the VxSS installation CD according to the instructions in the *VERITAS Security Services Installation Guide*. The manual is found on the VxSS installation CD.

NetBackup recommends placing the Root + AB broker on the NetBackup master server. This allows for more centralized administration of the NetBackup server and can facilitate upgrading to NetBackup Access Management.

After installing the Authentication Server software, configure the VxSS Root Broker as described in "Configuring Authentication on the Root Broker for Use with NetBackup" on page 15.

Configuring Authentication on the Root Broker for Use with NetBackup

Configure the Root Broker using the NetBackup command, `bpnbat` located in directory `/usr/openv/netbackup/bin/`

1. **Shut down NetBackup on the master server and start the At daemon, then the Az daemon:**

   To shut down NetBackup daemons, use

   ```
   NetBackup stop
   ```

   located in the `goodies` directory.

   To start the At daemon, enter `/opt/VRTSat/bin/vxatd`
   To start the At daemon, enter `/opt/VRTSaz/bin/vrtsaz`

2. **Allow the machines to communicate with one another:**

Note The steps below require a password that should not be a user or `root` password. The password must be at least five characters long, and match one another in both steps. However, it is not necessary to use the same password each time the two steps are run for a new machine in the domain.

   a. **To add a machine locally to the private domain:**

   In order for the NetBackup master servers, media servers, and clients to communicate, this machine needs to be added to the private database of the Authentication Broker or to the local disk by running the following command on the At server:

   ```
   bpnbat -AddMachine
   Does this machine use Dynamic Host Configuration Protocol (DHCP)?
   (y/n) n
   Authentication Broker: broker
   Authentication port[ Enter = default]: broker_port
   Name: machine_name
   Password: any_password
   Password: Re-enter password
   Operation completed successfully.
   ```

   Where:

   broker is the fully qualified name of the machine that will act as the Authentication Broker for this machine. In this case, since this machine is Root Broker + AB, enter the name of this machine.

broker_port is a specified port number. To use the default At port number (2821), press **Enter**.

machine_name is the fully qualified name of this machine.

any_password may be a unique password (at least five characters long) used only for the purpose of registering this machine. However, the same password *must* be used in both this step, when registering the machine locally in the private domain, *and* the next step, when registering the machine, but not in the private domain.

b. To create a credential for a machine:

In order to log the machine into the specified Authentication Broker, enter the following command on the machine that needs to be logged in:

```
bpnbat -loginmachine
Does this machine use Dynamic Host Configuration Protocol (DHCP)?
(y/n) n
Authentication Broker: broker
Authentication port[ Enter = default]: broker_port
Name: machine_name
Password: same password as in step a
You do not currently trust the server: server_name
Do you wish to trust it? (y/n) y
Operation completed successfully.
```

Continue to the next section for instructions on configuring authorization on the Root Broker.

Installing the Authorization Server

Install the VxSS Authorization software from the VxSS installation CD according to the instructions in the *VERITAS Security Services Installation Guide*.

NetBackup recommends installing the Authorization server on the master server. This ensures that the master and media servers are able to communicate with the Authentication server at all times.

Configuring the Authorization Server

The `bpnbaz` command is used during Authorization setup to perform two functions necessary for Access Management:

- Create the object hierarchy that appears in the NetBackup Administration Console under **Access Management**.
- Set up user groups and add the first identity to the security administration group (NBU_Security Admin).

`bpnbaz` is located in directory `/usr/openv/netbackup/bin/admincmd`

Before running `bpnbaz` commands, check that both the Authentication daemon (`vxatd`) and the Authorization daemon (`vxazd`) are running. If necessary, start the At daemon first, then the Az daemon.

Note The user named in the following command will be set up as the first NetBackup security administrator.

1. On the machine where the VxSS Authorization server software is installed and contains the Authorization server, run:

   `bpnbaz -SetupSecurity` *`master_server`* `[-server` *`AZ_server`*`]`

   Where:

   `master_server` is the fully qualified name of the NetBackup master server.

   `AZ_server` is the fully qualified name of the machine where Authorization server software is installed.

Note `bpnbaz -SetupSecurity` must be run by `root` (UNIX) or Administrator (Windows).

This process may take a number of minutes.

See step 6 on page 7 for an example of this command.

2. **Allow authorization:**

   Run the following command on the Authorization server. If configuring the Root Broker, the machine being added and the Az server will be the same:

   `bpnbaz -AllowAuthorization AZ_server`

Note `bpnbaz -AllowAuthorization AZ_server` must be run by `root` (UNIX) or Administrator (Windows).

   Where:

   AZ_server is the fully qualified name of the machine where Authorization server software is installed.

   If adding a different machine, the command would be run on the Az server, then a new machine would be named:

   `bpnbaz -AllowAuthorization AZ_client`

   AZ_client is the fully qualified name of the machine where Authorization client software is installed.

   This command must be run on the Az server for each master or media server that will utilize NetBackup Access Control.

3. **Start NetBackup daemons on the machine(s).**

4. Continue with "Configuring Access Control Host Properties" on page 19 for instructions on configuring NetBackup Access Control host properties for the master server (Root Broker).

Configuring Access Control Host Properties

Until host properties configuration on the master server is complete, NetBackup Access Control is not enforced. As such, UNIX users must temporarily load the Java NetBackup Administration Console (`jnbSA`) as `root` and Windows users must load the NetBackup Administration Console as Administrator.

Note VERITAS recommends setting master server VxSS property to **Automatic** until the clients are configured for Access Control. Then, if desired, change the VxSS property on the master server to **Required**.

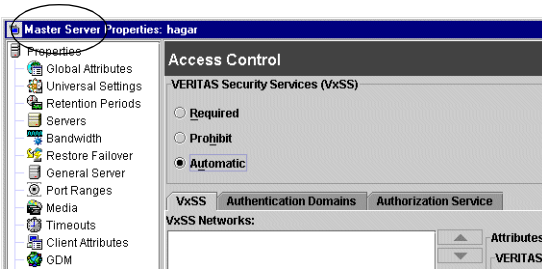
Master Server (Root Broker) Host Properties

The Access Control host properties are described fully in "Access Control Properties" on page 304, but here are some points to double-check.

Access Control Host Properties Dialog

Host properties of the master server (Root Broker):

Set the **VERITAS Security Services** to either **Required** or **Automatic**. A setting of **Automatic** takes into account that there may be hosts within the configuration that are not upgraded to NetBackup version 5.0 or higher. The server will attempt to negotiate the most secure connection possible when talking to other NetBackup systems.



Note VERITAS recommends setting the master server VxSS property to **Automatic** until the clients are configured for Access Control. Then, if desired, change the VxSS on the master server to **Required**.

When using **Automatic**, you may specify machines or domains requiring VxSS or **Prohibited** from using VxSS.

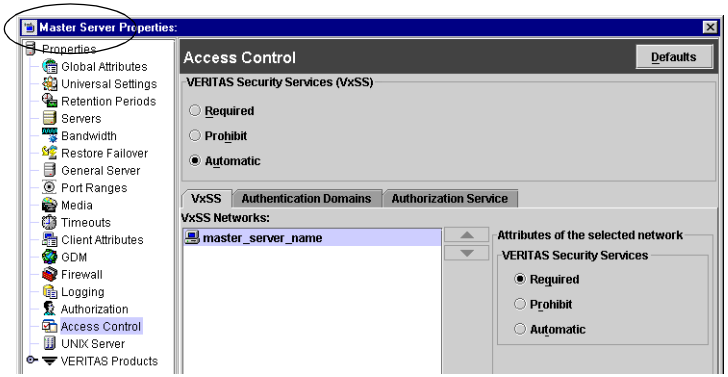
Host properties of the Az client:

Select the Az client in the host properties.
(On the master server, in the NetBackup Administration Console, open **NetBackup Management** > **Host Properties** > **Clients** > *Selected clients* > **Access Control**.

Set the **VERITAS Security Services** to **Required**.

VxSS Tab

Host properties of the master server (Root Broker):



Within the **Access Control** host properties, on the **VxSS** tab, add the master server to the VxSS Network list and set **VERITAS Security Services** to **Required**.

Each new NetBackup client or media server (version 5.0 or higher), added to the NetBackup master, needs to have the Access Control properties configured on both itself and the master. This can be done through the host properties on the master server.

Note VERITAS recommends setting the master server VxSS property to **Automatic** until the clients are configured for Access Control. Then, if desired, change the VxSS on the master server to **Required**.

Host properties of the Az client:

Select the Az client in the host properties. Set the **VERITAS Security Services** to **Required**.

Authentication Domain Tab

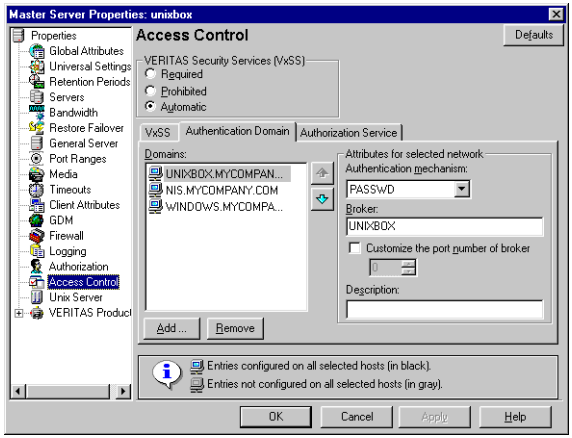
The Authenticaiton Domain tab is used to define the following:

- which Authentication servers support which authentication mechanisms, and
- what domains each supports.

The following examples contain three authentication domains and three authentication types, all hosted on the authentication server *UNIXBOX*.

A UNIX domain `UNIXBOX.MYCOMPANY.COM` on the Authentication server *UNIXBOX*.

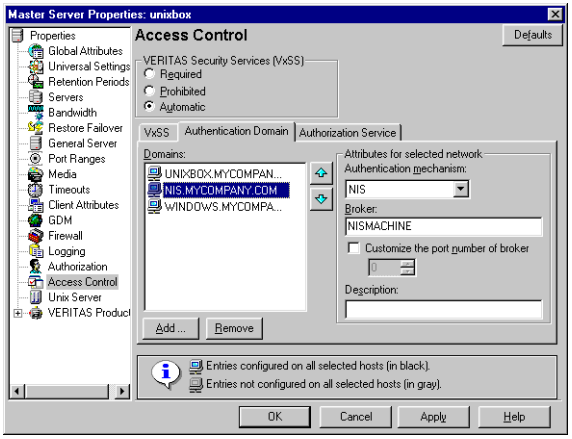
Notice that the authentication mechanism for this domain is PASSWD.



Note If using a UNIX authentication domain, enter the fully qualified domain name of the host performing the authentication.

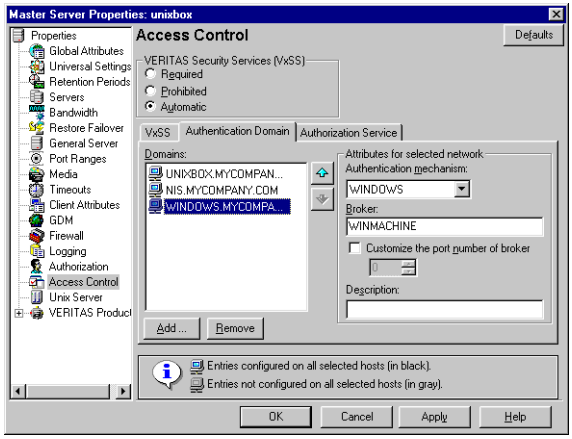
A NIS domain `NIS.MYCOMPANY.COM` on the Authentication server *NISMACHINE*.

Notice that the authentication mechanism for this domain is NIS.



A Windows AD/PDC (Active Directory/Primary Domain Controller) domain `WINDOWS.MYCOMPANY.COM` on the Authentication server *WINMACHINE*:

Notice that the authentication mechanism for this domain is WINDOWS.



Host properties of the master server (Root Broker):

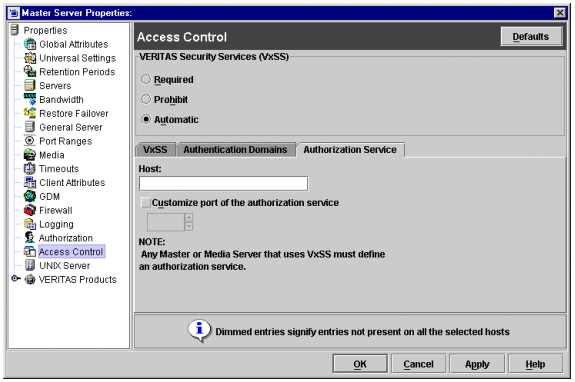
Within the **Access Control** host properties, on the **Authentication Domain** tab, add the domain in which the Authentication server resides and select the proper authentication mechanism.

Host properties of the Az client:

Within the **Access Control** host properties, on the **Authentication Domain** tab, add the domain in which the Az client resides and select the proper authentication mechanism.

Authorization Service Tab

Within the **Access Control** host properties, on the **Authorization Service** tab, complete the properties for the Authorization server. Specify the fully qualified domain name for the system running the Authorization daemon (typically the master). If needed, specify the alternate port for which this daemon has been configured. The default listening port for the Authorization daemon is 4032.



After making any changes to the host properties, restart the daemons.

Note If configuring this tab for a media server using Access Control, you must define the host that will perform authorization.

Verifying Master Server Settings

Running `bpnbat -whoami` tells in what domain a host is registered and the name of the machine the certificate represents (*win_master.min.com*).

```
bpnbat -whoami -cf
"e:\program
Files\veritas\netbackup\var\vxss\credentials\win_master"
Name: win_master
Domain: NBU_Machines@win_master.min.com
Issued by: /CN=broker/OU=root@win_master.min.com/O=vx
Expiry Date: Nov  5 20:17:51 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

If the domain listed is not NBU_Machines@win_master.min.com, consider running `bpnbat -addmachine` for the name in question *(win_master)* on the machine that is serving the NBU_Machines domain *(win_master)*.

Then, on the machine where we want to place the certificate, run:
`bpnbat -loginmachine`

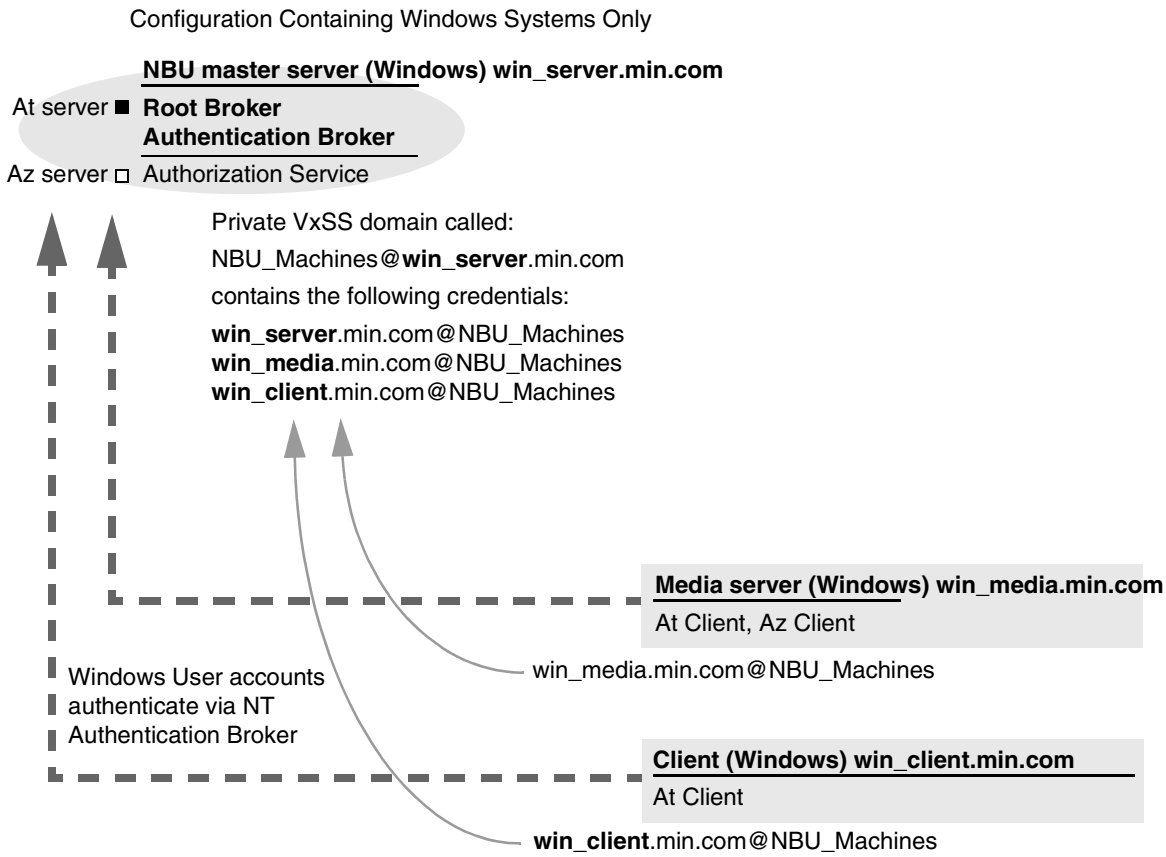
Access Management Troubleshooting Guidelines

In the configuration examples we'll refer to the following host names:

	Windows	UNIX
Master Servers	win_master	unix_master
Media Servers	win_media	unix_media
Clients	*win_client*	unix_client

Windows Verification Points

There are procedures that help you verify that the master server, media server and client are configured correctly for Access Control.



Note:
Each machine has a private domain account created for it. Using these accounts allows NetBackup to more reliably identify machines as they communicate with each other.

Master Server Verification Points

The following sections describe procedures for Windows master server verification.

Verify Windows Master Server Settings

To determine in what domain a host is registered (where the primary Authentication broker resides), and the name of the machine the certificate represents, run `bpnbat` with `-whoami`. For example:

```
bpnbat -whoami -cf
"e:\program
Files\veritas\netbackup\var\vxss\credentials\win_master"
Name: win_master.min.com
Domain: NBU_Machines@win_master.min.com
Issued by: /CN=broker/OU=root@win_master.min.com/O=vx
Expiry Date: Nov  5 20:17:51 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

If the domain listed is not NBU_Machines@win_master.min.com, consider running `bpnbat -addmachine` for the name in question *(win_master)* on the machine that is serving the NBU_Machines domain *(win_master)*.

Then, on the machine where we want to place the certificate, run:
`bpnbat -loginmachine`

Note When determining if a user's credentials have expired, keep in mind that the output displays the expiration time in GMT, not local time.

Note For the remaining procedures in this verification section, we assume that the commands are performed from an operating system window in which the user identity in question has run `bpnbat -login` using an identity that is a member of NBU_Security Admin. This is usually the first identity with which the security was set up.

Verify which Machines are Permitted to Perform Authorization Lookups

Logged in as a member of the Administrators group run the following command:

`bpnbaz -ShowAuthorizers`

This command shows that *win_master* and *win_media* (media server) are permitted to perform Authorization lookups. Note that both servers are authenticated against the same vx (VERITAS Private Domain) Domain, NBU_Machines@win_master.min.com.

```
bpnbaz -ShowAuthorizers
```

```
==========
Type: User
Domain Type: vx
Domain:NBU_Machines@win_master.min.com
Name: win_master.min.com
==========
Type: User
Domain Type: vx
Domain:NBU_Machines@win_master.min.com
Name: win_media.min.com
Operation completed successfully.
```

If a master or media server is missing from the list of Authorized machines, run `bpnbaz -allowauthorization` to add the missing machine.

Verify that the Database is Configured Correctly

To make sure that the database is configured correctly, run `bpnbaz -listgroups`:

```
bpnbaz -listgroups
NBU_User
NBU_Operator
NBU_Security Admin
Vault_Operator
NBU_Admin
Operation completed successfully.
```

If the groups do not appear, or if `bpnbaz -listmainobjects` does not return data, run `bpnbaz -SetupSecurity`.

Verify that the vxatd and vxazd Processes are Running

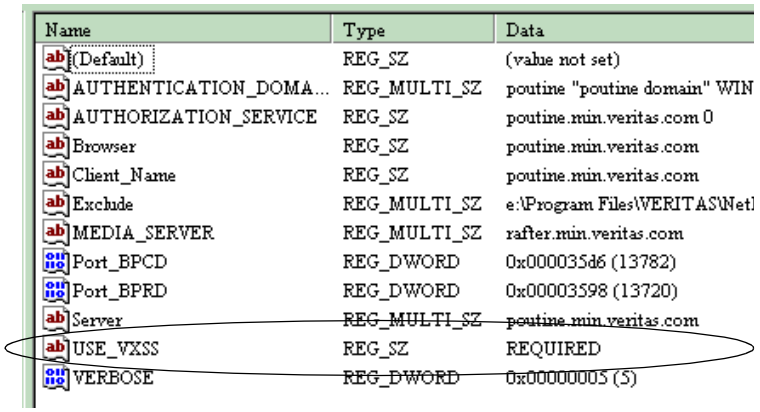
Use the Windows Task Manager to make sure that vxatd.exe and vxazd.exe are running on the designated host. If necessary, start them.

Verify that the Host Properties are Configured Correctly

In the Access Control host properties, verify that the **VERITAS Security Services** property is set correctly. (The setting should be either **Automatic** or **Required**, depending on whether all machines are using VxSS or not. If all machines are not using VxSS, set it to **Automatic**.

This can also be verified by viewing USE_VXSS in the registry at:

```
HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\config
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTHENTICATION_DOMA...	REG_MULTI_SZ	poutine "poutine domain" WIN
AUTHORIZATION_SERVICE	REG_SZ	poutine.min.veritas.com 0
Browser	REG_SZ	poutine.min.veritas.com
Client_Name	REG_SZ	poutine.min.veritas.com
Exclude	REG_MULTI_SZ	e:\Program Files\VERITAS\Net
MEDIA_SERVER	REG_MULTI_SZ	rafter.min.veritas.com
Port_BPCD	REG_DWORD	0x000035d6 (13782)
Port_BPRD	REG_DWORD	0x00003598 (13720)
Server	REG_MULTI_SZ	poutine.min.veritas.com
USE_VXSS	REG_SZ	REQUIRED
VERBOSE	REG_DWORD	0x00000005 (5)

In the Access Control host properties, verify that the authentication domains listed are spelled correctly and point to the proper servers (valid Authentication brokers). If all domains are Windows-based, they should point to a Windows machine running the At broker.

Media Server Verification Points

The following sections describe procedures for Windows media server verification.

Verify the Media Server

To determine which Authentication broker the media server is authenticated against, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf "c:\program
files\veritas\netbackup\var\vxss\credentials\win_media.min.com"
Name: win_media.min.com
Domain: NBU_Machines@win_master.min.com
Issued by: /CN=broker/OU=root@win_master.min.com/O=vx
Expiry Date: Nov  5 20:11:40 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the Server has Access to the Authorization Database

To make sure that the media server is able to access the Authorization database as it needs, run `bpnbaz -ListGroups -CredFile "`*`directory_containing_AZ_db`*`"`

For example:

```
bpnbaz -ListGroups -CredFile "C:\Program
Files\VERITAS\NetBackup\var\vxss\credentials\win_media.min.com"
NBU_User
NBU_Operator
NBU_Security Admin
Vault_Operator
NBU_Admin
Operation completed successfully.
```

If this command fails, run `bpnbaz -AllowAuthorization` on the master server that is the Authorization broker *(win_master.min.com).*

Unable to Load Library Message

Verifying the media server and verifying that the media server has access to the proper database indirectly informs us that the VxSS client libraries for both At and Az are properly installed. If either of these procedures fail with messages pertaining to "unable to load libraries," check to make certain the Authentication and Authorization client libraries are installed. See the *VERITAS Security Services Installation Guide* on the VxSS installation CD for proper installation procedures.

You may also verify that the Authentication domains are correct by viewing the Access Control host properties for this media server, or by using `regedit` directly on the media server.

Client Verification Points

The following sections describe procedures for Windows client verification.

Verify the Credential for the Client

To check that the credential for the client is indeed for the correct client and comes from the correct domain, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf "c:\program
files\veritas\netbackup\var\vxss\credentials\win_client.min.com"
Name: win_client.min.com
Domain: NBU_Machines@win_master.min.com
Issued by: /CN=broker/OU=root@win_master.min.com/O=vx
Expiry Date: Nov  5 20:11:45 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the VxSS Authentication Client Libraries are Installed

Run `bpnbat -login` on the client to verify that the VxSS authentication client libraries are installed.

```
bpnbat -login
Authentication Broker: win_master
Authentication port[ Enter = default]:
Authentication type (NIS, NIS+, NT, vx, UNIXpwd): NT
Domain: ENTERPRISE
Name: Smith
Password:
Operation completed successfully.
```

This can also be done by looking at the Windows Add/Remove Programs.

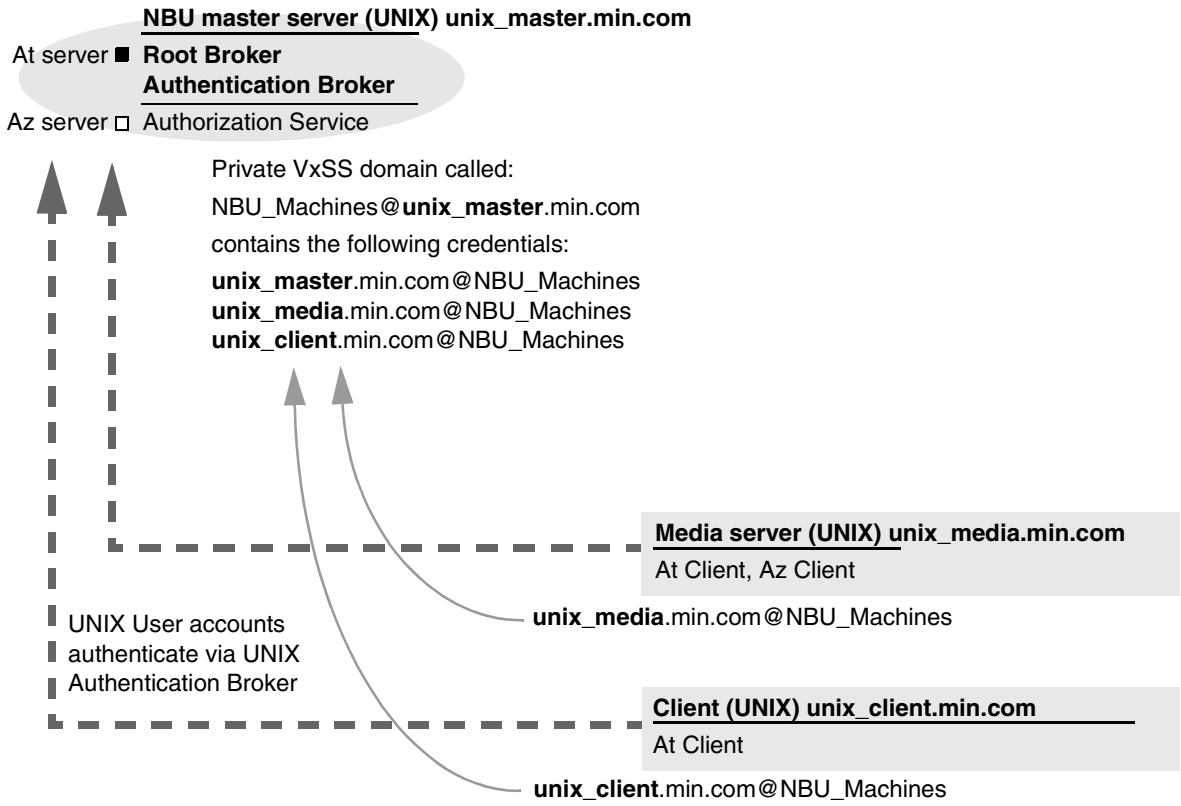
Verify Correct Authentication Domains

In the Access Control host properties or by using `regedit`, check that any defined authentication domains for the client are correct. Make certain the domains are spelled correctly, and that the authentication brokers listed for each of the domains is valid for that domain type.

UNIX Verification Points

These are the procedures that help you verify that the UNIX master server, media server and client are configured correctly for Access Control.

Configuration Containing UNIX Systems Only



Note:
Each machine has a private domain account created for it. Using these accounts allows NetBackup to more reliably identify machines as they communicate with each other.

Master Server Verification Points

The following sections describe procedures for UNIX master server verification.

Verify UNIX Master Server Settings

To determine in what domain a host is registered (where the primary Authentication broker resides), and the name of the machine the certificate represents, run `bpnbat` with `-whoami`. For example:

```
bpnbat -whoami -cf
/usr/openv/var/vxss/credentials/unix_master.min.com
Name: unix_master.min.com
Domain: NBU_Machines@win_master
Issued by: /CN=broker/OU=root@win_master/O=vx
Expiry Date: Nov 13 15:44:30 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

If the domain listed is not NBU_Machines@unix_master.min.com, consider running `bpnbat -addmachine` for the name in question *(unix_master)* on the machine that is serving the NBU_Machines domain *(unix_master)*.

Then, on the machine where we want to place the certificate, run:
`bpnbat -loginmachine`

Note When determining if a user's credentials have expired, keep in mind that the output displays the expiration time in GMT, not local time.

Note For the remaining procedures in this verification section, we assume that the commands are performed from an operating system window in which the user identity in question has run `bpnbat -login` using an identity that is a member of NBU_Security Admin. This is usually the first identity with which the security was set up.

Verify which Machines are Permitted to Perform Authorization Lookups

Logged in as root on the Authorization broker, run the following command:

`bpnbaz -ShowAuthorizers`

This command shows that *unix_master* and *unix_media* are permitted to perform Authorization lookups. Note that both servers are authenticated against the same vx (VERITAS Private Domain) Domain, NBU_Machines@unix_master.min.com.

```
bpnbaz -ShowAuthorizers
==========
```

```
Type: User
Domain Type: vx
Domain:NBU_Machines@unix_master.min.com
Name: unix_master.min.com

==========
Type: User
Domain Type: vx
Domain:NBU_Machines@unix_master.min.com
Name: unix_media.min.com

Operation completed successfully.
```

If a master or media server is missing from the list of Authorized machines, run `bpnbaz -allowauthorization` to add the missing machine.

Verify that the Database is Configured Correctly

To make sure that the database is configured correctly, run `bpnbaz -listgroups`:

```
bpnbaz -listgroups
NBU_User
NBU_Operator
NBU_Admin
NBU_Security Admin
Vault_Operator
Operation completed successfully.
```

If the groups do not appear, or if `bpnbaz -listmainobjects` does not return data, run `bpnbaz -SetupSecurity`.

Verify that the vxatd and vxazd Processes are Running

Run the `ps` command to ensure that `vxatd` and `vxazd` are running on the designated host. If necessary, start them. For example:

```
ps -fed |grep vx
root 10716     1  0   Nov 11 ?        0:02 /opt/VRTSat/bin/vxatd
root 10721     1  0   Nov 11 ?        4:17 /opt/VRTSaz/bin/vxazd
```

See the *VERITAS Security Services Administrator's Guide* for more details on how to start `vxatd` and `vxazd`.

Verify that the Host Properties are Configured Correctly

In the Access Control host properties, verify that the **VERITAS Security Services** property is set correctly. (The setting should be either **Automatic** or **Required**, depending on whether all machines are using VxSS or not. If all machines are not using VxSS, set it to **Automatic**.

In the Access Control host properties, verify that the authentication domains listed are spelled correctly and point to the proper servers (valid Authentication brokers). If all domains are UNIX-based, they should point to a UNIX machine running the At broker.

This can also be verified in `bp.conf` using `vi`.

```
cat bp.conf
SERVER = unix_master
SERVER = unix_media
CLIENT_NAME = unix_master
AUTHENTICATION_DOMAIN = min.com "default company NIS namespace" NIS
unix_master 0
AUTHENTICATION_DOMAIN = unix_master "unix_master password file"
PASSWD unix_master 0
AUTHORIZATION_SERVICE = unix_master.min.com 0
USE_VXSS = REQUIRED
#
```

Media Server Verification Points

The following sections describe procedures for UNIX media server verification.

Verify the Media Server

To determine which Authentication broker the media server is authenticated against, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf
/usr/openv/var/vxss/credentials/unix_media.min.com
Name: unix_media.min.com
Domain: NBU_Machines@unix_master.min.com
Issued by: /CN=broker/OU=root@unix_master.min.com/O=vx
Expiry Date: Nov  9 14:48:08 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the Server has Access to the Authorization Database

To make sure that the media server is able to access the Authorization database as it needs, run `bpnbaz -ListGroups -CredFile "`*`directory_containing_AZ_db`*`"`

For example:

```
bpnbaz -ListGroups -CredFile
/usr/openv/var/vxss/credentials/unix_media.min.com
NBU_User
NBU_Operator
NBU_Admin
NBU_Security Admin
Vault_Operator
Operation completed successfully.
```

If this command fails, run `bpnbaz -AllowAuthorization` on the master server that is the Authorization broker *(unix_master)*.

Unable to Load Library Message

Verifying the media server and verifying that the media server has access to the proper database indirectly informs us that the VxSS client libraries for both At and Az are properly installed. If either of these procedures fail with messages pertaining to "unable to load libraries," check to make certain the Authentication and Authorization client libraries are installed. See the *VERITAS Security Services Installation Guide* on the VxSS installation CD.

You may also verify that the Authentication domains are correct by viewing the Access Control host properties for this media server, or by using `cat(1)ing` the `bp.conf` file.

Client Verification Points

The following sections describe procedures for UNIX client verification.

Verify the Credential for the Client

To check that the credential for the client is indeed for the correct client and comes from the correct domain, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf
/usr/openv/var/vxss/credentials/unix_client.min.com
Name: unix_client.min.com
Domain: NBU_Machines@unix_master.min.com
Issued by: /CN=broker/OU=root@unix_master.min.com/O=vx
Expiry Date: Nov  9 14:49:00 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the VxSS Authentication Client Libraries are Installed

Run `bpnbat -login` on the client to verify that the VxSS authentication client libraries are installed.

```
bpnbat -login
Authentication Broker: unix_master.min.com
Authentication port[ Enter = default]:
Authentication type (NIS, NIS+, NT, vx, UNIXpwd): NIS
Domain: min.com
Name: Smith
Password:
Operation completed successfully.
```

This can also be done by looking at `/etc/vx/vss/*.loc` to see where the libraries are installed, and verify they are in the location indicated:

```
cat /etc/vx/vss/*.loc
ProductInstallDir=/opt/VRTSat
ProductInstallDir=/opt/VRTSaz
ls -l /opt/VRTSat/*/opt/VRTSaz/*
```

Verify Correct Authentication Domains

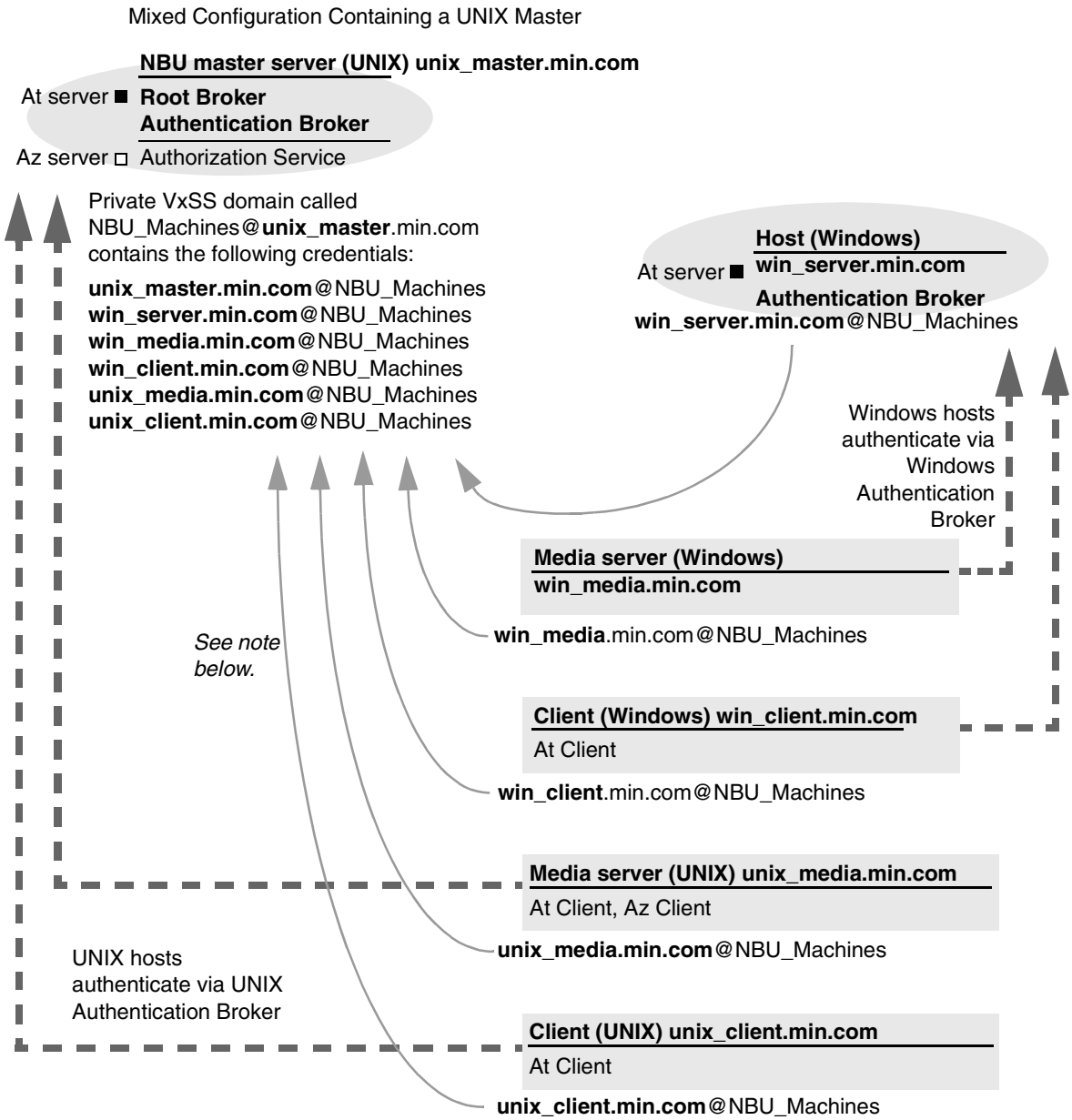
In the Access Control host properties or by using `vi`, check that any defined authentication domains for the client are correct. Make certain the domains are spelled correctly, and that the authentication brokers listed for each of the domains is valid for that domain type.

This can also be verified in `bp.conf` using `vi`.

```
cat bp.conf
SERVER = unix_master
SERVER = unix_media
CLIENT_NAME = unix_master
AUTHENTICATION_DOMAIN = min.com "default company NIS namespace" NIS
unix_master 0
AUTHENTICATION_DOMAIN = unix_master "unix_master password file"
PASSWD unix_master 0
AUTHORIZATION_SERVICE = unix_master.min.com 0
USE_VXSS = REQUIRED
```

Verification Points in a Mixed Environment with a UNIX Master Server

The following procedures can help you verify that the master server, media server and client are configured correctly for a heterogeneous NetBackup Access Control environment, where the master server is a UNIX machine.



Note:
Each machine has a private domain account created for it. Using these accounts allows NetBackup to more reliably identify machines as they communicate with each other.

Master Server Verification Points

Follow the same procedures as those listed in "Master Server Verification Points" on page 32.

Media Server Verification Points

Verify the UNIX Media Server

For UNIX media servers, follow the same procedures as those listed in "Media Server Verification Points" on page 34.

Verify the Windows Media Server

Check the machine certificate comes from the root Authentication broker, which is found on the UNIX master server *(unix_master)*.

If the certificate is missing, run the following commands to correct the problem:

- `bpnbat -addmachine` on the root Authentication broker (in this example, *unix_master*)
- `bpnbat -loginmachine` (in this example, *win_media*)

For example:

```
bpnbat -whoami -cf "C:\program
files\veritas\netbackup\var\vxss\credentials\win_media.min.com"
Name: win_media.min.com
Domain: NBU_Machines@unix_master.min.com
Issued by: /CN=broker/OU=root@unix_master.min.com/O=vx
Expiry Date: Nov 13 20:11:04 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that a Media Server is Permitted to Perform Authorization Lookups

Make sure the media server is allowed to perform authorization checks by running `bpnbaz -listgroups -CredFile`. For example:

```
bpnbaz -listgroups -CredFile "C:\program
files\veritas\netbackup\var\vxss\credentials\win_media.min.com"
NBU_User
NBU_Operator
NBU_Admin
NBU_Security Admin
Vault_Operator
Operation completed successfully.
```

If the media server is not allowed to perform authorization checks, run `bpnbaz -allowauthorization` on the master server for the media server name in question.

Unable to Load Library Message

Verifying the Windows media server and verifying that the media server is permitted to perform authorization checks indirectly informs us that the VxSS client libraries for both At and Az are properly installed. If either of these procedures fail with messages pertaining to "unable to load libraries," check to make certain the Authentication and Authorization client libraries are installed. See the *VERITAS Security Services Installation Guide* on the VxSS installation CD.

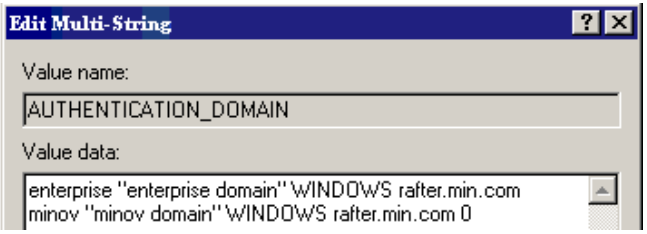
Verify Authentication Domains

You may also verify that the Authentication domains are correct by viewing the Access Control host properties for this media server, or by using `regedit` directly on the media server in the following location:

```
HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\config\
AUTHENTICATION_DOMAIN
```

Cross Platform Authentication Domains

Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers. In the example below, note that the WINDOWS domains point to win_media.min.com.



Client Verification Points

For UNIX client machines, follow the same procedures as those listed in "Client Verification Points" on page 35.

For Windows clients:

Verify the Credential for the Windows Client

To check that the credential for the client is indeed for the correct client and comes from the correct domain, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf "e:\program
files\veritas\netbackup\var\vxss\credentials\win_master.min.com"
Name: win_master.min.com
Domain: NBU_Machines@unix_master.min.com
Issued by: /CN=broker/OU=root@unix_master.min.com/O=vx
Expiry Date: Nov 13 19:50:50 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the VxSS Authentication Client Libraries are Installed

Run `bpnbat -login` on the client to verify that the VxSS authentication client libraries are installed. For example:

```
bpnbat -login
Authentication Broker: unix_master.min.com
Authentication port[ Enter = default]:
Authentication type (NIS, NIS+, NT, vx, UNIXpwd): NIS
Domain: min.com
Name: Smith
Password:
Operation completed successfully.
```

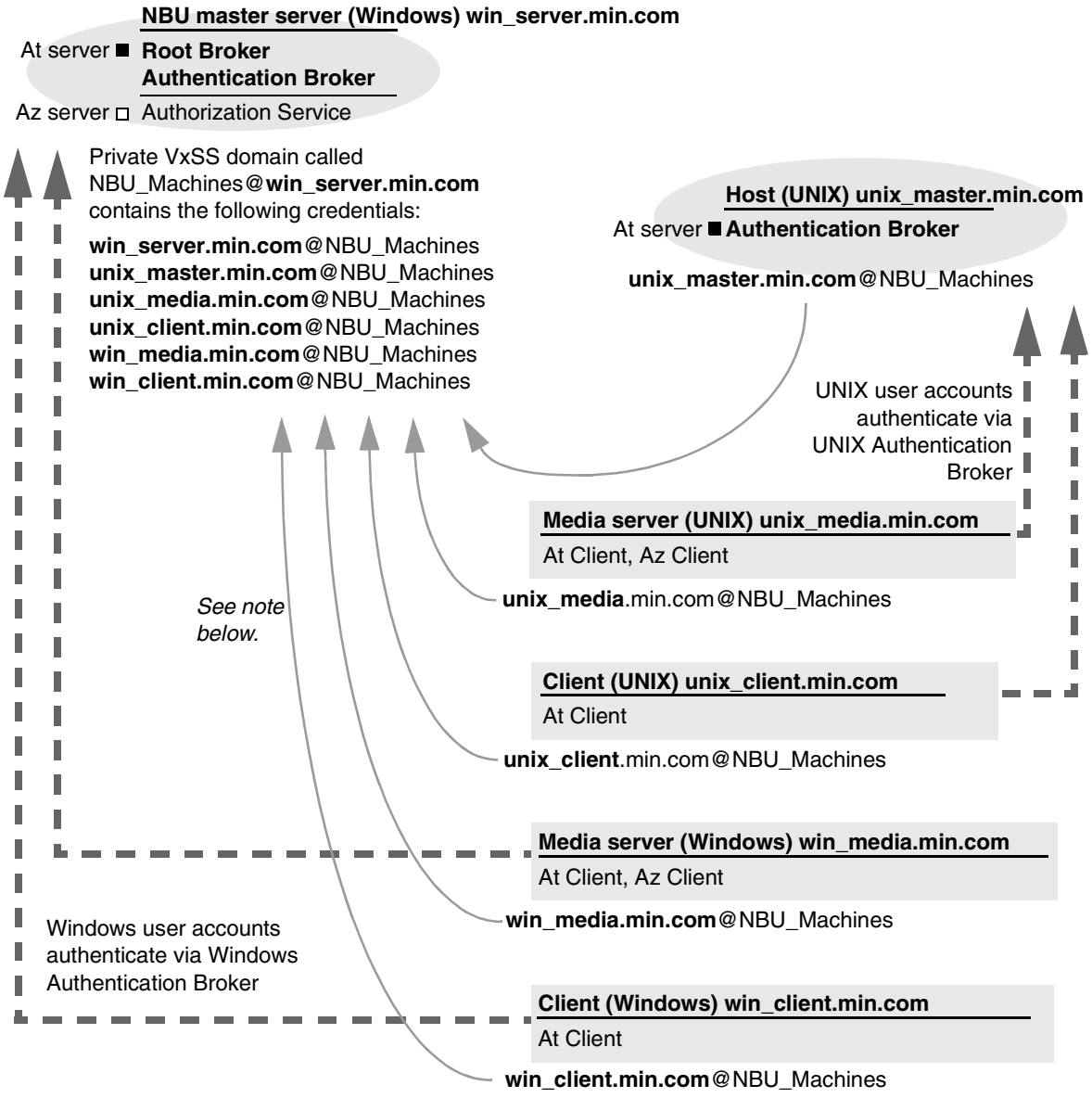
Verifying the Windows Authentication Broker

Make sure that the Windows Authentication broker either has mutual trust with the main UNIX Authentication broker, or is using the UNIX broker as its root broker. See the *VERITAS Security Services Installation Guide* on the VxSS installation CD for more information regarding these scenarios.

Verification Points in a Mixed Environment with a Windows Master Server

The following procedures can help you verify that the master server, media server and client are configured correctly for a heterogeneous NetBackup Access Control environment, where the master server is a Windows machine.

Mixed Configuration Containing a Windows Master



Note:
Each machine has a private domain account created for it. Using these accounts allows NetBackup to more reliably identify machines as they communicate with each other.

Master Server Verification Points

Follow the same procedures as those listed in "Master Server (Root Broker) Host Properties" on page 19.

Media Server Verification Points

Verify the Windows Media Server

For Windows media servers, follow the same procedures as those listed in "Media Server Verification Points" on page 28.

Verify the UNIX Media Server

Check that the machine certificate is issued from the root Authentication broker, found on the Windows master server *(win_master)*. To determine which Authentication broker the media server is authenticated against, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf
/usr/openv/var/vxss/credentials/unix_media.min.com
Name: unix_media.min.com
Domain: NBU_Machines@win_master.min.com
Issued by: /CN=broker/OU=root@win_master.min.com/O=vx
Expiry Date: Nov  9 14:48:08 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the Server has Access to the Authorization Database

To make sure that the media server is able to access the Authorization database as it needs to perform authorization checks, run `bpnbaz -ListGroups -CredFile "/usr/openv/var/vxss/credentials/<hostname>"`

For example:

```
bpnbaz -ListGroups -CredFile\
/usr/openv/var/vxss/credentials/unix_media.min.com
NBU_User
NBU_Operator
NBU_Admin
NBU_Security Admin
Vault_Operator
Operation completed successfully.
```

If the media server is not allowed to perform authorization checks, run `bpnbaz -allowauthorization` on the master server for the media server name in question.

Unable to Load Library Message

Verifying the media server and verifying that the media server has access to the proper database indirectly informs us that the VxSS client libraries for both At and Az are properly installed. If either of these procedures fail with messages pertaining to "unable to load libraries," check to make certain the Authentication and Authorization client libraries are installed. See the *VERITAS Security Services Installation Guide* on the VxSS installation CD.

Cross Platform Authentication Domains

You may also verify that the Authentication domains are correct by viewing the Access Control host properties for this media server, or by using `cat(1)ing` the `bp.conf` file.

Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers. In the example below, note that the PASSWD and NIS domains point to unix_media.min.com, which, in this example, is the UNIX Authentication broker:

```
cat bp.conf
SERVER = win_master.min.com
MEDIA_SERVER = unix_media.min.com
CLIENT_NAME = unix_media
AUTHENTICATION_DOMAIN = win_master "win_master domain" WINDOWS
win_master.min.com
 0
AUTHENTICATION_DOMAIN = enterprise "enterprise domain" WINDOWS
win_master.min.com 0
AUTHENTICATION_DOMAIN = unix_media.min.com "local unix_media
domain" PASSWD unix_media.min.com 0
AUTHENTICATION_DOMAIN = min.com "NIS domain" NIS
unix_media.min.com 0
AUTHORIZATION_SERVICE = win_master.min.com 0
USE_VXSS = REQUIRED
```

Client Verification Points

Verify the Credential for the Windows Client

For Windows clients, follow the same procedures as those listed in "Client Verification Points" on page 29.

Verify the Credential for the UNIX Client

To check that the credential for the client is indeed for the correct client and comes from the correct domain, run `bpnbat -whoami`. For example:

```
bpnbat -whoami -cf \
"/usr/openv/var/vxss/credentials/unix_client.min.com"
Name: unix_client.min.com
Domain: NBU_Machines@win_master.min.com
Issued by: /CN=broker/OU=root@win_master.min.com/O=vx
Expiry Date: Nov  6 21:16:01 2004 GMT
Authentication method: VERITAS Private Security
Operation completed successfully.
```

Verify that the VxSS Authentication Client Libraries are Installed

Run `bpnbat -login` on the client to verify that the VxSS authentication client libraries are installed.

```
bpnbat -login
Authentication Broker: unix_media.min.com
Authentication port[ Enter = default]:
Authentication type (NIS, NIS+, NT, vx, UNIXpwd): NIS
Domain: min.com
Name: Smith
Password:
You do not currently trust the server: unix_media.min.com, do you
wish to tr
ust it? (y/n):
y
Operation completed successfully.
```

Verify the UNIX Authentication Broker

Make sure that the UNIX Authentication broker either has mutual trust with the main Windows Authentication broker, or is using the Windows broker as its root broker. See the *VERITAS Security Services Installation Guide* on the VxSS installation CD for more information regarding this scenario.

Other Troubleshooting Topics

The following sections describe topics that may be helpful when configuring VxSS with NetBackup.

Expired Credentials Message

If your credential has expired or is incorrect, you may receive the following message while running a `bpnbaz` or `bpnbat` command:

```
Supplied credential is expired or incorrect. Please reauthenticate and
try again.
```

Run `bpnbat -Login` to update an expired credential.

Useful Debug Logs

The following logs are useful when debugging NetBackup Access Control:

On the master: `admin`, `bpcd`, `bprd`, `bpdbm`, `bpjobd`, `bpsched`

On the client: `admin`, `bpcd`, `bprd`, `bpdbjobs`

See the *NetBackup Troubleshooting Guide* for instructions on implementing proper logging.

If Uninstalling VxSS

On UNIX:

Using `installvss`, select the option for uninstalling Authentication and Authorization. The following directories should be empty after uninstalling:

```
/opt
/etc/vx/vss
/var/
```

On Windows:

Use the Windows **Add/Remove Programs** panel from the Control Menu to uninstall Authentication and Authorization. The `\Veritas\Security` directory should be empty after uninstalling.

Where Credentials Are Stored

NetBackup VxSS credentials are stored in the following UNIX directories:

User credentials: `$HOME/.vxss`

Machine credentials: `/usr/openv/var/vxss/credentials/`

VxSS Ports

VxSS daemons listen at the following ports:

Authentication:

```
netstat -an | grep 2821
```

Authorization:

```
netstat -an | grep 4032
```

Stopping VxSS Daemons

When stopping the VxSS daemons, stop Az first, then stop At.

When stopping the VxSS services, stop Authorization first, then stop Authentication.

UNIX: Use the following commands.

To stop Az: `/opt/VRTSaz/bin/vrtsaz -stop`

To stop At: Use the term signal as shown in the example below:

```
# ps -fed |grep vxatd
    root 16018     1  4 08:47:35 ?        0:01 ./vxatd
    root 16019 16011  0 08:47:39 pts/2    0:00 grep vxatd
# kill 16018
# ps -fed |grep vxard
    root 16021 16011  0 08:47:48 pts/2    0:00 grep vxard
```

Windows:

Use the Services utility that Windows provides, since these services do not appear in the NetBackup Activity Monitor.

If You Lock Yourself Out of NetBackup

It is possible to lock yourself out of the NetBackup Administration Console if Access Control is incorrectly configured.

If this occurs, use `vi` to read the bp.conf entries (UNIX) or `regedit` (Windows) to view the Windows registry in the following location:

```
HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\config
```

You'll look to see if he following entries are set correctly: AUTHORIZATION_SERVICE, AUTHENTICATION_DOMAIN, and USE_VXSS.

If the administrator does not wish to use NetBackup Access Control or does not have the VxSS libraries installed, make certain that the USE_VXSS entry is set to **Prohibited**, or is deleted entirely.

nbac_cron Utility

Use the `nbac_cron` utility to create identities under which to run *cron* or *at* jobs.

`nbac_cron` is found in the following location:

UNIX: `/opt/openv/netbackup/bin/goodies/nbac_cron`

Windows: `<install_path>\netbackup\bin\goodies\nbac_cron.exe`

nbac_cron options:

- `-SetupAt [-Port #]`
  `-SetupCron [-Port #]`

  Either option sets up an Authentication account. Optionally, specify a port number to use for authentication.

- `-AddAt`

  Create an *at* account for a user.

- `-AddCron`

  Create a *cron* account for a user.

Using the Access Management Utility

Users assigned to the NetBackup Security Administrator user group have access to **Access Management**. Users assigned to any other user group, including NetBackup Administrator, can see the Access Management node in the NetBackup Administration Console, but cannot expand it.

If a user other than a Security Administrator tries to select **Access Management**, an error message displays. Toolbar buttons and menu items specific to **Access Management** are not displayed.

Upon successful completion, the default NetBackup user groups should display in the NetBackup Administration Console under **Access Management** > **NBU User Groups**.

To list the groups on the command line, run `bpnbaz -ListGroups` on the machine where the VxSS Authorization server software is installed.

`bpnbaz` is located in directory `/usr/openv/netbackup/bin/admincmd`

(You must be logged in as the Security Administrator by using `bpnbat -login`)

```
bpnbaz -ListGroups
NBU_User
NBU_Operator
NBU_Admin
NBU_Security Admin
Vault_Operator
Operation completed successfully.
```

The NetBackup user groups are listed. This verifies that the Security Administrator can access the user groups.

Access Management Menus

The Menu bar consists of the following menu items:

Option	Description
File	Options **Change Server**, **New Window from Here**, **Adjust Application Time Zone**, **Export**, **Page Setup**, **Print Preview**, **Print**, **Close Window**, and **Exit** are described in Chapter 1 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.
Edit	Options **New**, **Change**, **Delete**, and **Find** are described in Chapter 1 of the *NetBackup System Administrator's Guide for UNIX, Volume I*. The **Change** option is available when a NBU user group is selected in the details pane.

Option	Description
View	Options **Show Toolbar**, **Show Tree**, **Back**, **Forward**, **Up One Level**, **Options**, **Refresh**, **Column Layout**, **Sort**, and **Filter** are described in Chapter 1 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.
Actions	The Actions menu contains the following options when **Access Management** is selected: ◆ **New User Group:** Click to create a new NetBackup user group. ◆ **Copy to New User Group:** Use to create a new user group based on an existing user group. Users and permissions can be changed as needed for the new user group.
Help	Options **Help Topics**, **Troubleshooter**, **License Keys**, **Current NBAC User**, and **About NetBackup Administration Console** are described in Chapter 1 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.

Determining Who Can Access NetBackup

Access Management allows only one user group, by default, the *NBU_Security Admin* user group, to define the following aspects of NetBackup Access Management:

- The permissions of individual users.
- The creation of user groups.

First, determine which NetBackup resources your users will need to access. (See "Permissions for Default NetBackup User Groups" on page 61 for resources and associated permissions.)

The Security Administrator may want to first consider what different users have in common, then create user groups with the permissions that these users require. User groups generally correspond to a role, such as administrators, operators, or end-users.

Consider basing user groups on one or more of the following criteria:

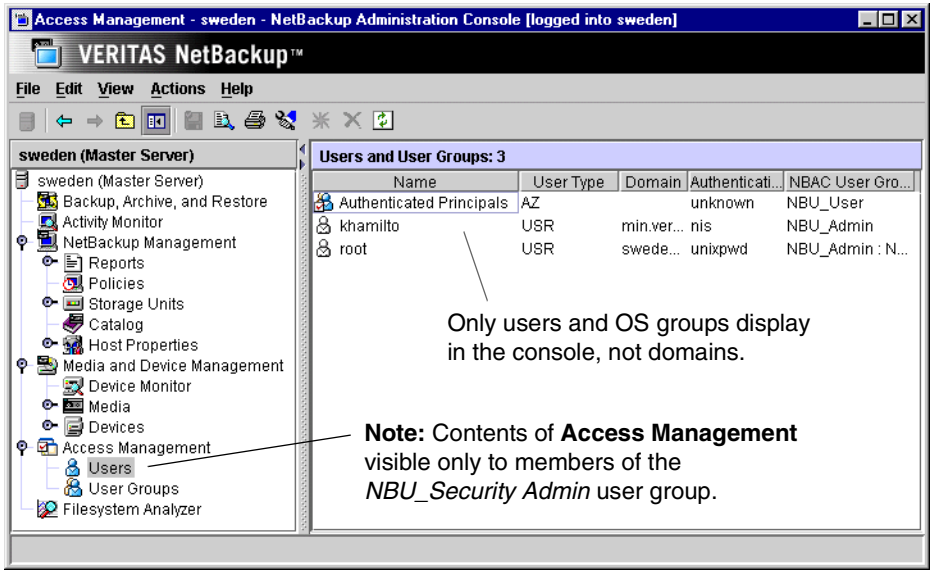
- Functional units in your organization (UNIX administration, for example)
- NetBackup resources (drives, policies, for example)
- Location (East Coast or West coast, for example)
- Individual responsibilities (tape operator, for example)

Note Permissions are granted to individuals in user groups, not to individuals on a per-host basis. If a machine is authenticated within the configuration, any individual in the user group can operate NetBackup to the extent that they are authorized to do so. There are no restrictions based on a machine name.

Individual Users

NetBackup Access Management uses your existing OS-defined users, groups, and domains. As such, Access Management maintains no list of users and passwords. When defining members of groups, the Security Administrator is specifying existing OS level users as members of user groups.

Every authenticated user belongs to at least one authorization user group. By default, every user belongs to the user group *NBU_Users*, which contains all authenticated users.



There are two types of users that are implicit members of groups:

- On the server hosting the Authorization daemons, `root` is an implicit member of the *NBU_Security Admin* user group
- All authenticated users are implicit members of the *NBU_Users* user group

All other groups must have members defined explicitly. The NetBackup Security Administrator can delete members added manually to other groups; however, the Security Administrator may not delete the predefined implicit members of the *NBU_Users* and *NBU_Security Admin* groups. OS groups and OS users may be added to an authorization group.

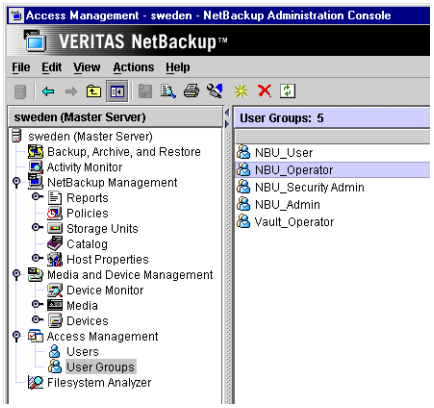
Note Although *root* (UNIX) or *administrator* (Windows) on the master server are added to the NetBackup Administrators user group and get NetBackup Administrator permissions, *root* and *administrator* are not predefined users.)

User Groups

Rather than assigning permissions directly to individual users, NetBackup Access Management is configured by assigning permissions to user groups, then assigning users to the user groups.

Upon successful installation, NetBackup provides five default user groups that complement how sites often manage the duties of NetBackup operation. The user groups are listed under **Access Management** > **NBU User Groups**. Keep in mind that the contents of **Access Management** are visible to members of the *NBU_Security Admin* group only.

The Security Administrator may choose to use the default NetBackup user groups, or may choose to create custom user groups.



Note: Contents of **Access Management** visible only to members of the *NBU_Security Admin* user group.

Default User Groups

The permissions granted to users in each of the five default user groups correlate to the group name. Essentially, an authorization object correlates to a node in the NetBackup Administration Console tree.

The following sections describe each NetBackup default user group:

Security Administrator (*NBU_Security Admin*)

There are usually very few members in the *NBU_Security Admin* user group. The only permission that the Security Administrator possesses by default is that of configuring Access Control within **Access Management**. Configuring Access Control includes the following permissions:

- Ability to see the contents of **Access Management** in the NetBackup Administration Console
- Ability to create, modify and delete users and user groups
- Ability to assign users to user groups
- Ability to assign permissions to user groups

Administrator (*NBU_Admin*)

By default, members of the *NBU_Admin* user group have full permission to access, configure, and operate any NetBackup authorization object. In other words, members have all the capabilities that are currently available to administrators without Access Management in place. However, as members of this group, it is not necessary to log on as root or administrator at the OS level.

Note Members of the *NBU_Admin* user group cannot see the contents of **Access Management**, and therefore, cannot ascribe permissions to other user groups.

Operator (*NBU_Operator*)

The main task of the *NBU_Operator* user group is to monitor jobs. For example, members of the *NBU_Operator* user group might monitor jobs and notify a NetBackup administrator if there is a problem so the problem can be addressed by the administrator. Using the default permissions, a member of the *NBU_Operator* user group would probably not have enough access to be address larger problems.

Members of the *NBU_Operator* user group have permissions that allow them to perform some tasks such as moving tapes, operating drives, and inventorying robots.

Default User (*NBU_User*)

The *NBU_User* user group is the default NetBackup user group with the fewest permissions. Members of the *NBU_User* user group can only backup, restore, and archive files. *NBU_User* user group members have access to the functionality of the NetBackup client interface (BAR).

Vault Operator (*Vault_Operator*)

The *Vault_Operator* user group is the default user group that contains permissions to perform the operator actions necessary for the Vault process.

Additional User Groups

The Security Administrator (member of *NBU_Security Admin* or equivalent) can create user groups as needed. Although the default user groups can be selected, changed and saved, NetBackup recommends that the groups be copied, renamed, then saved in order to retain the default settings for future reference.

User Group Configuration

The Security Administrator can create a new user groups by clicking **Actions** > **New Group** or by selecting an existing user group and selecting **Actions** > **Copy to New Group**.

▼ To create a new user group

1. As a member of the *NBU_Security Admin* user group (or equivalent), expand **Access Management** > **User Groups**.
2. Select **Actions** > **New User Group**. The Add New User Group dialog displays, opened to the **General** tab.
3. Type the name of the new group in the **Name** field, then click the **Users** tab. For more information on users, see "Users Tab" on page 57.
4. Select the defined users that you wish to assign to this new user group, then click **Assign**. Or, to include all the defined users in the group, click **Assign All**. To remove users from the assigned users list, select the user name, then click **Remove**.
5. Click the **Permissions** tab. For more information on permissions, see "Permissions Tab" on page 60.
6. Select a resource from the Resources list, then select the permissions for the object.
7. Click **OK** to save the user group and the group permissions.

▼ To create a new user group by copying an existing user group

1. As a member of the *NBU_Security Admin* user group (or equivalent), expand **Access Management** > **User Groups**.
2. Select an existing user group in the Details pane. (The pane on the left side of the NetBackup Administration Console.)
3. Select **Actions** > **Copy to New User Group**. A dialog based on the selected user group displays, opened to the **General** tab.
4. Type the name of the new group in the **Name** field, then click the **Users** tab.
5. Select the defined users that you wish to assign to this new user group, then click **Assign**. Or, to include all the defined users in the group, click **Assign All**. To remove users from the assigned users list, select the user name, then click **Remove**.

6. Click the **Permissions** tab.

7. Select a resource from the Resources list, then select the permissions for the object.

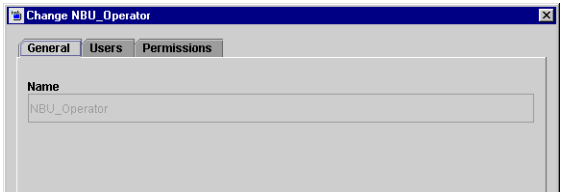
8. Click **OK** to save the user group and the group permissions. The new name for the user group appears in the Details pane.

Renaming User Groups

Once a NetBackup user group has been created, the user group cannot be renamed. The alternative to directly renaming a user group is to copy the user group, give the copy a new name, ensure the same membership as the original, then delete the original NetBackup user group.

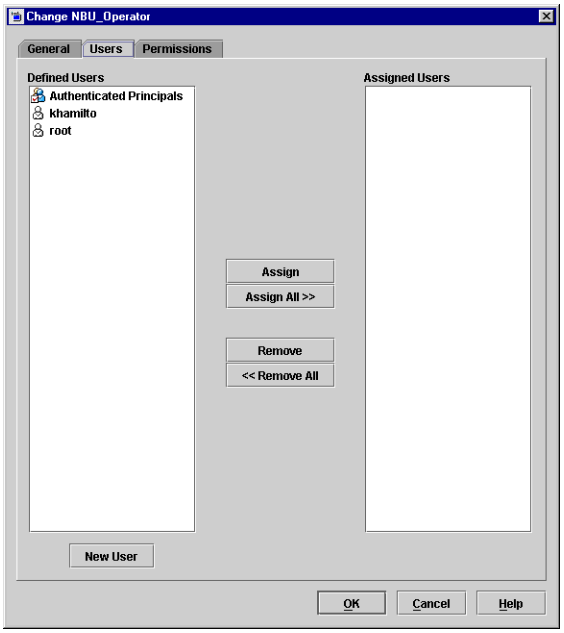
General Tab

The General tab contains the name of the user group. If creating a new user group, the **Name** field can be edited.



Users Tab

The Users tab contains controls to assign and remove users from user groups.



Defined Users

The Defined Users list is a list of all users defined manually within other groups.

- **Assign** button: Select a user in the Defined User list and click **Assign** to assign that user to a user group.
- **Assign All** button: Click **Assign All** to add all defined users to the user group.

Assigned Users

The **Assigned Users** list contains defined users who have been added to the user group.

- **Remove** button: Select a user in the Assigned Users list and click **Remove** to remove that user from the user group.
- **Remove All** button: Click **Remove All** to remove all assigned users from the Assigned User list.

New User

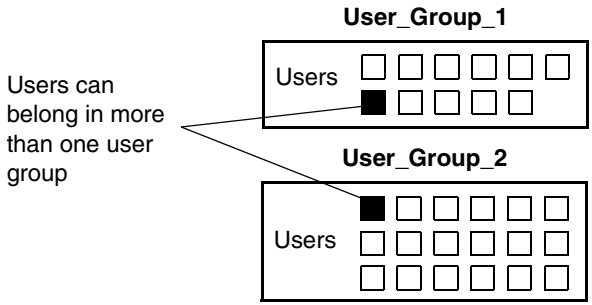
Click **New User** to add a user to the **Defined Users** list. After adding a user, the name appears in the **Defined Users** list and the Security Administrator can assign the user to the user group. (See "To add a new user to a user group" on page 59.)

Defining Users Groups and Users

NetBackup authenticates existing users of the operating system rather than requiring that NetBackup users be created with a NetBackup password and profile.

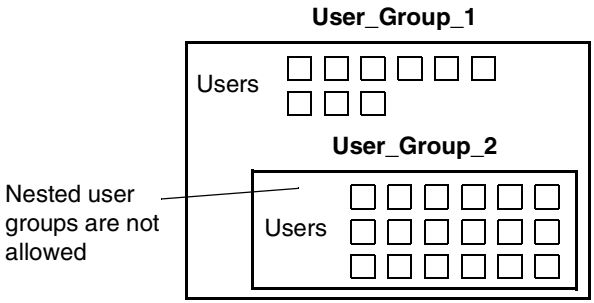
Defining a User Group

Users can belong to more than one user group and have the combined access of both groups.

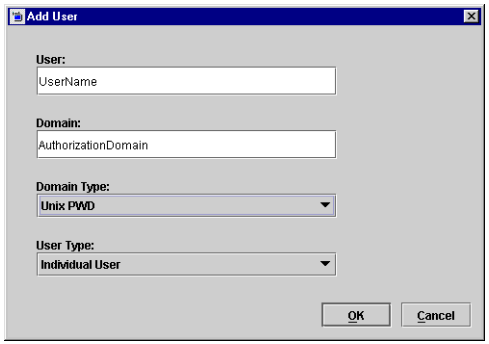


While users can be members of multiple user groups simultaneously, NetBackup does not allow user groups to be nested.

For example, while members of a user group can belong to more than one user group, a user group cannot belong to another user group.



▼ To add a new user to a user group



1. As a member of the *NBU_Security Admin* user group (or equivalent), expand **Access Management** > **NBU User Groups**.
2. Double-click on the user group to which you wish to add a user.
3. Select the **Users** tab and click **New User**.
4. Enter the user name and the authentication domain. Select the domain type of the user: NIS, NIS+, PASSWD, NT or Vx. See the *VERITAS Security Services Administrator's Guide* for more information on domain types.

   For the **User Type**, select whether the user is an individual user or an OS domain.
5. Click **OK**. The name is added to the Assigned Users list.

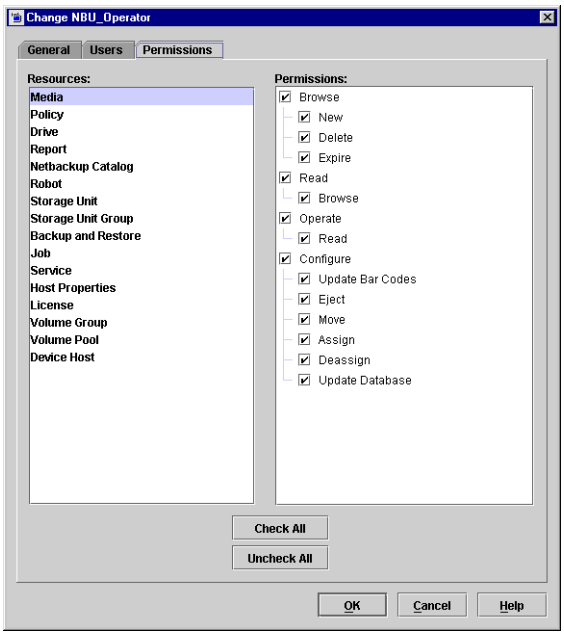
Permissions Tab

The **Permissions** tab contains a list of NetBackup authorization objects and configurable permissions associated with each object.

Authorization Objects and Permissions List

Select an authorization object, then place a check in front of a permission that you want to grant the members of the user group currently selected.

When a user group is copied to create a new user group, the permission settings are copied as well.



Permissions for Default NetBackup User Groups

The permissions granted to users in each of the five default user groups correlate to the name of the user group.

Backup, Archive, and Restore (BAR) Client Interface

The table below shows the permissions associated with the BAR authorization object for the five default NetBackup user groups. BAR includes only Access and Operate permission sets, and does not include a Configure permission set.

In the NetBackup Administration Console, BAR is accessed by selecting **File** > **Backup, Archive, and Restore**.

Backup, Archive, and Restore Permission Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read	---	X	X	X	X
	Browse	---	X	X	X	X
Operate	Backup	---	X	X	X	X
	Restore	---	X	X	---	---
	Alternate client	---	X	X	---	---
	List	---	X	X	X	X
	DB Agent	---	X	---	---	---
	Admin Access	---	X	---	---	---

License Permissions

The table below shows the permissions associated with the License authorization object for the five default NetBackup user groups.

In the NetBackup Administration Console, the license dialog is accessed by selecting **Help** > **License Keys**.

License Permission Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read license	---	X	---	---	---
	Browse license	---	X	---	---	---
Configure	New	---	X	---	---	---
	Delete	---	X	---	---	---
Operate	Assign license	---	X	---	---	---

Jobs Tab in the Activity Monitor Permissions

The table below shows the permissions associated with the Jobs tab authorization object for the five default NetBackup user groups.

The Jobs tab is found in the NetBackup Administration Console under **NetBackup Management** > **Activity Monitor** > **Jobs** tab.

Jobs Tab Permission Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read job	---	X	X	---	---
	Browse job	---	X	X	---	---
Configure	Delete job	---	X	X	---	---
	New job	---	X	X	---	---
Operate	Suspend job	---	X	X	---	---
	Resume job	---	X	X	---	---
	Restart job	---	X	X	---	---
	Cancel job	---	X	X	---	---

Permissions in the Device Monitor

The table below shows the permissions associated with the Device Monitor authorization object for the five default NetBackup user groups.

The Device Monitor is found in the NetBackup Administration Console under **Media and Device Management**.

Device Monitor Permission Default

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read device host	---	X	X	---	---
	Browse device host	---	X	X	---	---
Configure	New	---	X	---	---	---
	Delete	---	X	---	---	---
Operate	Up drive	---	X	X	---	---
	Down drive	---	X	X	---	---
	Reset drive	---	X	X	---	---

Daemon Tab Permissions in the Activity Monitor

The table below shows the permissions associated with the Daemon tab authorization object for the five default NetBackup user groups. The Daemon tab includes only Access and Operate permission sets, and does not include a Configure permission set.

The Daemon tab is found in the NetBackup Administration Console under **NetBackup Management** > **Activity Monitor** > **Daemon** tab.

Daemon Tab Permission Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read	---	X	X	---	---
	Browse	---	X	X	---	---
Operate	Stop daemon	---	X*	X	---	---

* If a user is *not* a member of the NBU_Admin user group, but *is* logged on as an OS administrator (`root`), the user will be able to restart a daemon from the command line only:

```
/etc/init.d/netbackup start
```

If a user is a member of the NBU_Admin user group, but *is not* logged on as an OS administrator (`root`), the user will *not* be able to restart a daemon from the NetBackup Administration Console or from the command line.

Reports Permissions

The table below shows the permissions associated with the Reports authorization object for the five default NetBackup user groups. Reports includes only the Access permission set, and does not include a Configure or Operate permission set.

Reports is found in the NetBackup Administration Console under **NetBackup Management** > **Reports**.

Reports Permission Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read report	---	X	---	---	X
	Browse report	---	X	---	---	X

Policy Permissions

The table below shows the permissions associated with the Policy authorization object for the five default NetBackup user groups.

Policy is found in the NetBackup Administration Console under **NetBackup Management** > **Policies**.

Policy Permission Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read policy	---	X	X	---	---
	Browse policy	---	X	X	---	---
Configure	New policy	---	X	---	---	---
	Delete policy	---	X	---	---	---
Operate	Activate policy	---	X	---	---	---
	Deactivate policy	---	X	---	---	---
	Backup (manually)	---	X	X	---	---

Storage Units Permissions

The table below shows the permissions associated with the Storage Unit authorization object for the five default NetBackup user groups.

Storage Units is found in the NetBackup Administration Console under **NetBackup Management** > **Storage Units**.

Storage Unit Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read storage unit	---	X	---	---	---
	Browse storage unit	---	X	---	---	---
Configure	New storage unit	---	X	---	---	---
	Delete storage unit	---	X	---	---	---
Operate	Assign storage unit	---	X	---	---	---

Storage Unit Groups Permissions

The table below shows the permissions associated with the Storage Unit Groups authorization object for the five default NetBackup user groups.

Storage Unit Groups is found in the NetBackup Administration Console under **NetBackup Management** > **Storage Unit Groups**.

Storage Unit Groups Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read storage unit group	---	X	---	---	---
	Browse storage unit group	---	X	---	---	---
Configure	New storage unit group	---	X	---	---	---
	Delete storage unit group	---	X	---	---	---
Operate	Assign storage unit group	---	X	---	---	---

Catalogs Permissions

The table below shows the permissions associated with the Catalog authorization object for the five default NetBackup user groups.

Catalogs is found in the NetBackup Administration Console under **NetBackup Management** > **Catalogs**.

Catalogs Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Accesss	Read catalog	---	X	---	---	---
	Browse catalog	---	X	---	---	---
Configure	New	---	X	---	---	---
	Delete	---	X	---	---	---
	Expire	---	X	---	---	---
Operate	Verify catalog	---	X	---	---	---
	Duplicate catalog	---	X	---	---	---
	Import catalog	---	X	---	---	---
	Set Primary Copy	---	X	---	---	---
	Backup	---	X	---	---	---
	Restore	---	X	---	---	---
	Read configuration	---	X	---	---	---
	Set configuration	---	X	---	---	---

Host Properties Permissions

The table below shows the permissions associated with the Host Properties authorization object for the five default NetBackup user groups.

Host Properties is found in the NetBackup Administration Console under **NetBackup Management** > **Host Properties**.

Host Properties Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read host properties	---	X	X	---	---
	Browse host properties	---	X	X	---	---
Configure	New host properties	---	X	---	---	---
	Delete host properties	---	X	---	---	---

Media Permissions

The table below shows the permissions associated with the Media authorization object for the five default NetBackup user groups.

Media is found in the NetBackup Administration Console under **Media and Device Management** > **Media**.

Media Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read media	---	X	X	---	X
	Browse media	---	X	X	---	X
Configure	New media	---	X	---	---	---
	Delete media	---	X	---	---	---
	Expire media	---	X	---	---	---
Operate	Update barcode	---	X	---	---	X
	Inject media	---	X	X	---	X
	Eject media	---	X	X	---	X
	Move media	---	X	X	---	X
	Assign media	---	X	X	---	X
	Deassign media	---	X	X	---	X
	Update database	---	X	X	---	X

Volume Group Permissions

The table below shows the permissions associated with the Volume Group authorization object for the five default NetBackup user groups.

Volume Group is found in the NetBackup Administration Console under **Media and Device Management** > **Media** > **Volume Groups**.

Volume Group Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read volume group	---	X	---	---	---
	Browse volume group	---	X	---	---	---
Configure	New volume group	---	X	---	---	---
	Delete volume group	---	X	---	---	---

Volume Pools Permissions

The table below shows the permissions associated with the Volume Pools authorization object for the five default NetBackup user groups.

Volume Pools is found in the NetBackup Administration Console under **Media and Device Management** > **Media** > **Volume Pools**.

Volume Pools Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read volume pool	---	X	---	---	---
	Browse volume pool	---	X	---	---	---
Configure	New volume pool	---	X	---	---	---
	Delete volume pool	---	X	---	---	---
Operate	Assign volume pool	---	X	---	---	---

Robots Permissions

The table below shows the permissions associated with the Robots authorization object for the five default NetBackup user groups.

Robots is found in the NetBackup Administration Console under **Media and Device Management** > **Media** > **Robots**.

Volume Robots Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read robot	---	X	X	---	X
	Browse robot	---	X	X	---	X
Configure	New robot	---	X	---	---	---
	Delete robot	---	X	---	---	---
Operate	Inventory robot	---	X	X	---	X

Device Host Permissions

The table below shows the permissions associated with the Device Host authorization object for the five default NetBackup user groups.

Device Host is found in the NetBackup Administration Console under **Media and Device Management** > **Devices** > **Hosts**.

Device Host Permission Set Defaults

Set	Activity	Sec Admin	NBU_Admin	NBU_Operator	NBU_User	Vault_Operator
Access	Read device host	---	X	X	---	---
	Browse device host	---	X	X	---	---
Configure	New device host	---	X	---	---	---
	Delete device host	---	X	---	---	---
	Synchronize device host	---	X	X	---	---
Operate	Stop device host	---	X	X	---	---

Enhanced Authentication and Authorization 2

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 provides administrative privileges to UNIX `root` administrators or Windows system administrators on NetBackup servers. In order to use the enhanced authorization, you must configure and enable it.

This chapter contains the following sections:

- "Common Configuration Elements" on page 72
- "Enhanced Authentication" on page 82
- "Enhanced Authorization" on page 91

Note Access Management and Enhanced Authorization and Authentication are independent methods of access control. Access Management is the newest and will be the preferred method in future NetBackup releases. If both Access Management and Enhanced Authorization and Authentication are configured, Access Management takes precedence.

There are additional types of authorization outside of what is described in this chapter.

One of these is the appearance of MEDIA_SERVER entries in the `bp.conf`. The machine listed as a MEDIA_SERVER has media server privileges *only* and has no administrative privileges. For more information, see "MEDIA_SERVER" on page 156.

Another form of authorization concerns restricting administrative privileges when using the NetBackup Java Console (`jnbSA`) through entries in `auth.conf`.

Refer to "NetBackup-Java Administration Console Architectural Overview" on page 489 in *NetBackup System Administrator's Guide for UNIX, Volume I* for information relevant to understanding this topic.

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 of these files. 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`
Enhanced Authorization	authorize.txt	UNIX	`/usr/openv/var/`
		Windows	*`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`

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.

```
# 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.

- 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 domain name patterns and network 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 73.)

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 the `names_allow.txt` file or the `names_deny.txt` file 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 comma-separated host names or IP addresses.

```
# 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.

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 73.)

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 "Syntax rules for `methods.txt`" on page 73.)

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 95.)

File Location of authorize.txt

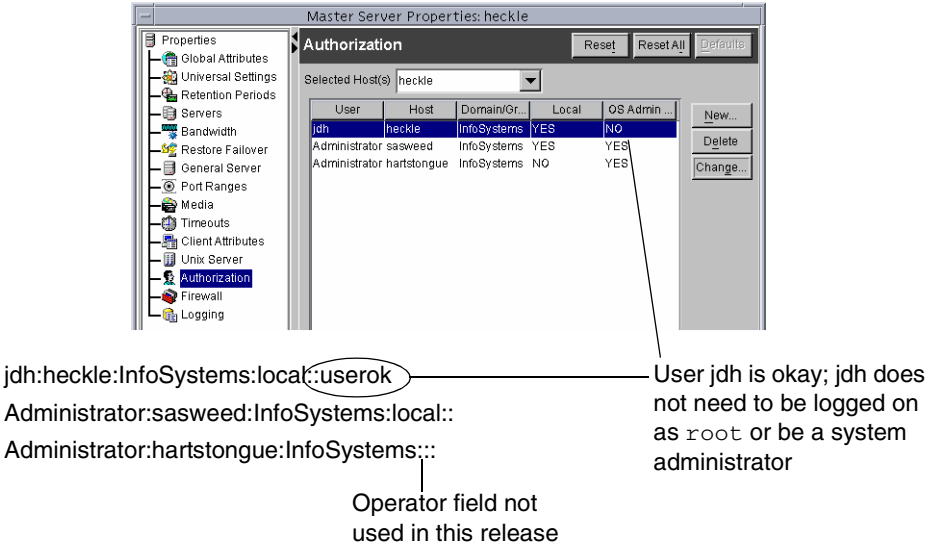
Platform	Path
UNIX	`/usr/openv/var/authorize.txt`
Windows	*install_path*`\NetBackup\var\authorize.txt`

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 page entries with the corresponding `authorize.txt` file.

Comparing Authorization Property Page 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 Administration 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.

```
# 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 72.)

Commands

The following commands are used to configure and manage authentication. For more information on these commands, see the *NetBackup Commands for UNIX* guide.

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 95.)

bpauthsync

Run `bpauthsync` on the master server to set up enhanced authentication for one or more clients and media servers. `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/`

Location of bpauthsync and bpauthorize commands

Windows	*install_path*\NetBackup\bin\admincmd\

vopie_util

Run vopie_util on NetBackup servers and clients to update 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.

Location of vopied_util command

Platform	Path
UNIX	/usr/openv/bin/
Windows	*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	*install_path*\NetBackup\bin\vopied

Files

vopie Files

The vopie processes use during authentication.

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`

- The *`localhost`* is the host name of the local system. There will be a local host directory for every possible local host name.
- The *`remotehost`* contains the hashed or public key 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.

The `unhashed` files contains the secret key that NetBackup uses when it responds to challenges from remote systems.

Location of Unhashed Files

Platform	Path
UNIX	`/usr/openv/var/auth/vopie/unhashed/`*`localhost/remotehost`*`.txt`
Windows	*`lnstall_path`*`\NetBackup\var\auth\vopie\unhashed\`*`localhost`*`\`*`remotehost`*`.txt`

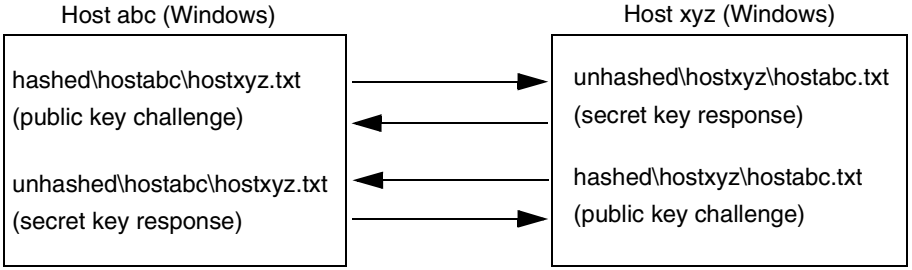
Where:

- *`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 `root` 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 one system with the `unhashed` files on another system. This enables the remote host to offer the correct response when it is challenged. The following figure illustrates this exchange between Windows 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 challenges 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 nonroot 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 installation process installs the necessary files and commands. The administrator then uses commands to set up the files so they contain the proper authentication information.

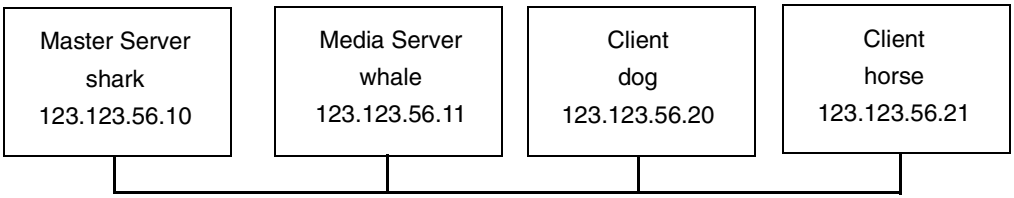
2. Configure NetBackup policies and add clients to the policies.

3. Run:
   `/usr/openv/netbackup/bin/admincmd/bpauthsync` on the master server. (See the following section to determine which options to use.)

   `bpauthsync` sets up authentication files on the NetBackup servers and clients. See the guide, *NetBackup Commands for UNIX*, for information on all NetBackup commands.

vopie Enhanced Authentication Examples

The examples in this section are based on the following configuration:



vopie Example 1: Typical Configuration

Assume that you want to configure `vopie` authentication for all systems in the figure below. NetBackup server and client software has already been installed.

1. Configure NetBackup policies and add clients to the policies.

2. Run the following command on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -servers
   -clients
   ```

   This synchronizes the key files on all the systems.

3. On the master server, copy the `methods_allow.txt` to a temporary file. For example, `/tmp/ma.txt`.

4. To the temporary file, add an entry for each host that requires authentication:

   ```
   vopie : shark
   vopie : whale
   vopie : dog
   vopie : horse
   ```

5. Synchronize the `methods_allow.txt` files on the servers and the clients by running the following on the master server (all on one line):

```
/usr/openv/netbackup/bin/admincmd/bpauthsync -methods
-methods_allow /tmp/ma.txt -servers -clients
```

The information in `/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 horse 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):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods
   -methods_allow /dev/null -clients horse
   ```

   This disables authentication on the client.

2. On the master server, remove the entry for horse from the `/usr/openv/var/auth/methods_allow.txt` file.

3. Synchronize the methods files on all servers by running the following on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods -servers
   ```

   Authentication is no longer performed when communicating with client horse.

vopie Example 3: Adding a Client

Assume that all systems are configured for authentication, except for client horse.

To add authentication for client horse:

1. On the master server, copy the `methods_allow.txt` to a temporary file. For example, `/tmp/ma.txt`.

2. Add an entry for the new client to the temporary file:

   ```
   vopie : horse
   ```

3. Synchronize the methods files on the servers and the new client by running the following on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -methods
   -methods_allow /tmp/ma.txt -servers -clients horse
   ```

   The information in `/tmp/ma.txt` is written in the `methods_allow.txt` files on the servers and the client.

vopie Example 4: Restoring Authentication After Client Disk Crash

Assume that horse 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:

   `/usr/openv/var/auth/methods_allow.txt.save`

2. Remove the entry for the failed client from `methods_allow.txt` on the master server.

3. Push the modified `methods_allow.txt` file to the other servers by running the following (all on one line):

   `/usr/openv/netbackup/bin/admincmd/bpauthsync -methods -servers`

   This disables authentication for the failed client so the servers can communicate with it during recovery.

4. Reinstall the operating system (Windows or UNIX) and NetBackup on the failed client by following the instructions in the *Troubleshooting Guide for UNIX and Windows*. However, do not restore any NetBackup or user files at this time.

5. On the master server, run the following command to synchronize and push the original methods to the servers and the failed client. The command is on one line:

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -methods
   -servers -clients horse -methods_allow
   /usr/openv/var/auth/methods_allow.txt.save
   ```

   The information in `methods_allow.txt.save` is written in the `methods_allow.txt` files on servers and the client. The original authentication methods are now restored.

Note Do not restore the files in the `/usr/openv/var/auth` directory on the client or authentication will have to be resynchronized.

6. Complete the client recovery by restoring the original NetBackup and user files as explained in the *NetBackup Troubleshooting Guide for UNIX and Windows*.

vopie Example 5: Restoring Authentication on NetBackup Master 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 UNIX and 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):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -servers
   -clients
   ```

If the NetBackup catalog backup was written to a storage unit on whale, shark cannot recover the catalogs because the two servers cannot authenticate one another. In this instance, the following steps are required:

1. Install NetBackup on the master server (do not restore any files at this time).

2. Disable authentication between the master server and the media server where the catalog backup was written, by modifying their `methods_allow.txt` files:

   a. On the master server, remove the entry for the media server from the `methods_allow.txt` file (if an entry is present).

   b. On the media server, remove the entry for the master server from the `methods_allow.txt` file.

3. On the master server, run `bprecover` to restore the catalog files.

4. Restore all files to the master server, including those in the `/usr/openv/var/auth`*`install_path`*directory.

5. On the media server, add back the entry for the master server from the `methods_allow.txt` file.

6. Synchronize all servers and clients by running the following on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -servers
   -clients
   ```

   The original configuration is now restored.

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.

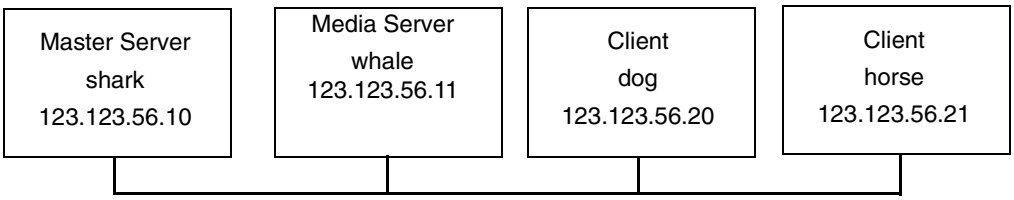
The `noauth` method is easier to configure than the `vopie` method. Consider using the `noauth` method rather than the `vopie` method if full authentication is not necessary, yet you want to use the Enhanced Authorization feature described in "Enhanced Authorization" on page 91.

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.

The examples in this section are based on the following 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, `/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 : horse
```

3. Synchronize the `methods_allow.txt` files on the servers and the clients by running the following on the master server (all on one line):

```
/usr/openv/netbackup/bin/admincmd/bpauthsync -methods
-methods_allow /tmp/ma.txt -servers -clients
```

The information in `/tmp/ma.txt` is written to `methods_allow.txt` on the servers and clients.

To disable authentication for client horse:

1. Push an empty `methods_allow.txt` file to the client by running the following on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods
   -methods_allow /dev/null -clients horse
   ```

   This disables authentication on the client.

2. On the master server, remove the entry for horse from the `/usr/openv/var/auth/methods_allow.txt` file.

3. Synchronize the methods files on all servers by running the following on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods -servers
   ```

   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 horse.

To add authentication for client horse:

1. On the master server, copy the `methods_allow.txt` to a temporary file. For example, `/tmp/ma.txt`.

2. Add an entry for the new client to the temporary file:

   ```
   noauth : horse
   ```

3. Synchronize the `methods_allow.txt` files on the servers and the new client by running the following on the master server (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods
   -methods_allow.txt /tmp/ma.txt -servers -clients horse
   ```

   The information in `/tmp/ma.txt` is written to `methods_allow.txt` files on the servers and the client.

Assume that client horse 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 `/usr/openv/var/auth/methods_allow.txt.save`

2. Remove the entry for the failed client from `methods_allow.txt` on the master server.

3. Push the modified `methods_allow.txt` file to the other servers by running the following (all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods -servers
   ```

   This disables authentication for the failed client so the servers can communicate with it during recovery.

4. Reinstall the operating system (Windows or UNIX) and NetBackup on the failed client by following the instructions in the *NetBackup Troubleshooting Guide for UNIX and Windows*. However, do not restore any NetBackup or user files at this time.

5. On the master server, run the following command to push the original methods to the servers and the failed client (the command is all on one line):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -methods -servers
   -clients horse -methods_allow
   /usr/openv/var/auth/methods_allow.txt.save
   ```

   The information in `methods_allow.txt.save` is written in `methods_allow.txt` on the servers and the client. The original authentication methods are restored.

6. Complete the client recovery by restoring the original NetBackup and user files as explained in the *NetBackup Troubleshooting Guide for UNIX and Windows*.

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 UNIX and 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):

   ```
   /usr/openv/netbackup/bin/admincmd/bpauthsync -servers -clients
   ```

If the NetBackup catalog backup was written to a storage unit on whale, shark cannot recover the catalogs because the two servers cannot authenticate one another. In this instance, the following steps are required:

1. Install NetBackup on the master server (do not restore any files at this time).

2. Disable authentication between the master server and the media server where the catalog backup was written, by modifying their `methods_allow.txt` files:

   a. On the master server, remove the entry for the media server from the `methods_allow.txt` file (if an entry is present).

   b. On the media server, remove the entry for the master server from the `methods_allow.txt` file.

3. On the master server, run `bprecover` to restore the catalog files.

4. Restore all files to the master server, including those in the `/usr/openv/var/auth` directory.

5. On the media server, add back the entry for the master server from the `methods_allow.txt` file.

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 UNIX and 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` and `vopied` (`/usr/openv/logs/vopied`)
   - On the client, create debug log directories for `bpcd`, `bpbackup`, `bprestore`, `bplist` and `vopied` (`/usr/openv/logs/vopied`)

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.

Note All references in this section to the NetBackup Administration Console host when the context is the NetBackup-Java Administration Console refer to the NetBackup-Java console's application server host. (See "NetBackup-Java Administration Console Architectural Overview" on page 489 in *NetBackup System Administrator's Guide for UNIX, Volume I*.)

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

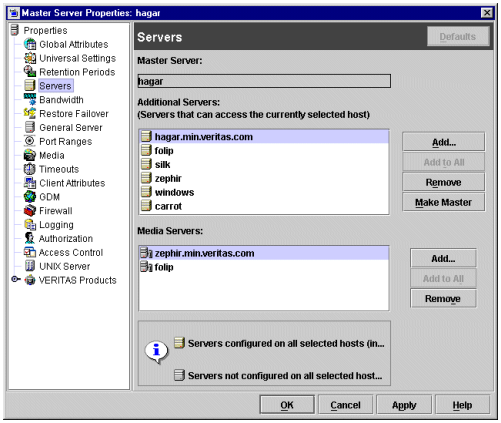
When an administrator on a remote NetBackup Administration Console makes a request to a NetBackup server, and enhanced authentication is enabled between the two systems, the *user_name*, *host_name*, *domain_group_name*, and `local` flag are passed from the requesting NetBackup Administration Console 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.

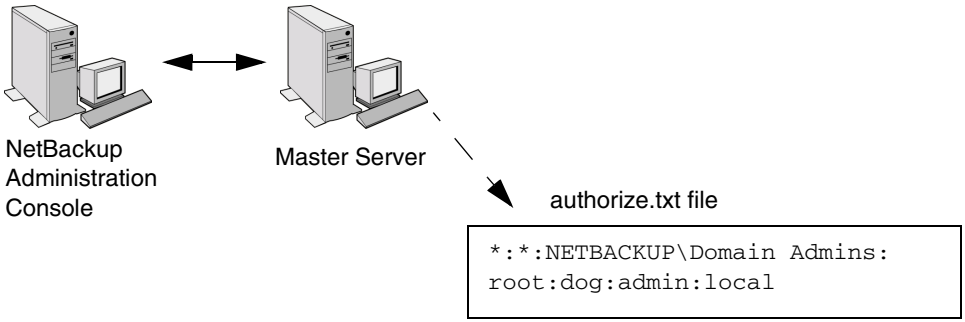
If a match exists, the request is authorized (allowed). If the request is not authorized, the request can proceed only if the NetBackup Administration Console making the request contains:

- On UNIX servers:
  `SERVER = server_name` entry in the `bp.conf` file of the accepting server. This is the host where the console runs.
- On Windows servers:
  The server must be among those listed under **Additional Servers** on the **Servers** properties page.

  (See the *NetBackup System Administrator's Guide for UNIX, Volume I*.)



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*).



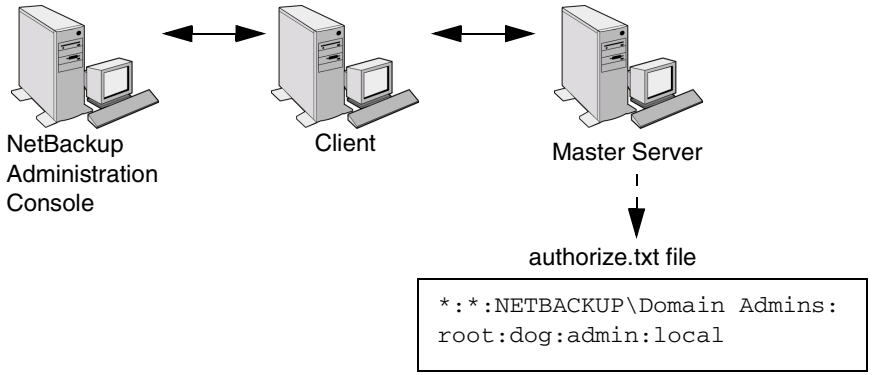
Gaining Access to a Client

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 Administration Console to the NetBackup client accepting the request.

If the requesting host 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 Administration 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 420.)

2. Enable NetBackup authentication. (See "Enabling NetBackup Enhanced Authentication" on page 94.)

3. Add an authorized user (creating an `authorize.txt` file). (See "Adding an Authorized User" on page 95.)

4. Optionally, specify the preferred group. (See "Using the Administration Console to Specify Preferred Groups (Optional)" on page 95.)

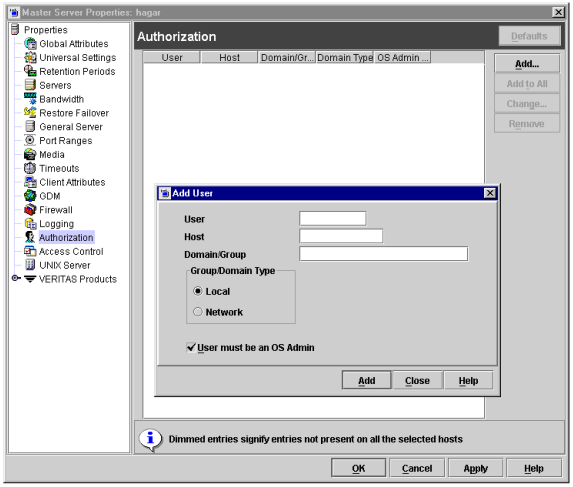
Enabling NetBackup Enhanced Authentication

To use enhanced authorization, first 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.

Adding an Authorized User

To enable enhanced authorization, create a list of authorized users.

▼ To create a list of authorized users



1. Expand **NetBackup Management** > **Host Properties** > **Master Server** (or **Media Servers**) > *Selected master or media server* > **Authorization**.

2. Click **Add**. The **Add User** dialog appears.

3. Type the user name that will have access to this server. To allow any user, type: *

4. Type the domain or group name to which the user belongs. To allow any domain group, type: *

5. Select whether the domain is local or on a network.

6. Type the host name that will be accessing the selected master or media server. To allow any host, type: *

7. Select to allow users onto the machine to administrate NetBackup who are not system administrators or logged on as UNIX `root`.

8. 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.

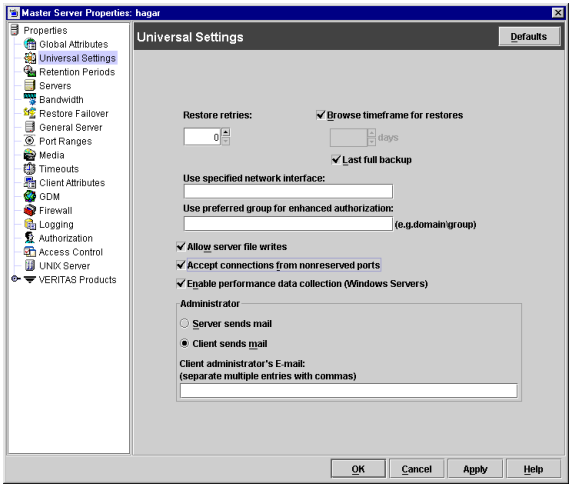
Using the Administration Console to Specify Preferred Groups (Optional)

You can specify a preferred group of administrative users in the NetBackup Administration 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 subject, see "Media Manager Configuration File (vm.conf)" in the *NetBackup Media Manager System Administrator's Guide*.

▼ To specify a preferred group

1. Expand **NetBackup Management** > **Host Properties** > **Master Server** (or **Media Servers**) > *Selected master or media server* > **Universal Settings**.



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.

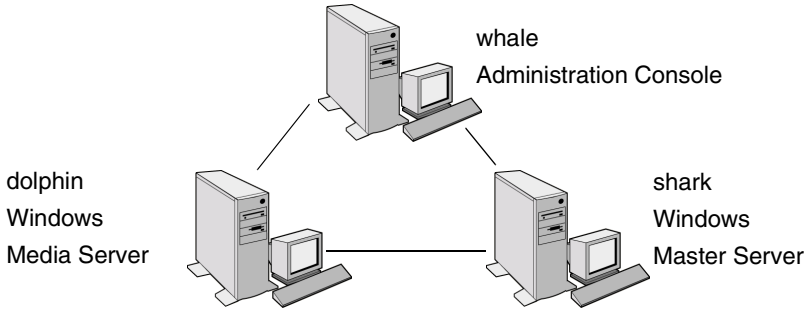
A check is made to determine if the user is a member of domain\group. This check is limited to NT global groups. In other words, if PREFERRED_GROUP is set to a domain local group, a match will not occur and the user's primary domain\group will be used.

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.

2. 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 3

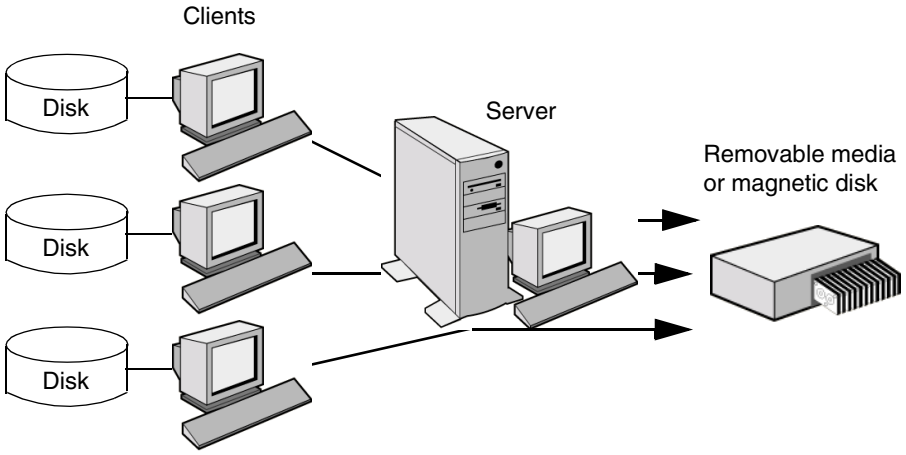
This chapter explains settings that, in many instances, are optional. The sections in this chapter include the following:

- "Multiplexing" on page 100
- "Using Multiple NetBackup Servers" on page 105
- "Configuring a Master and Media Server Grouping" on page 106
- "Dynamic Host Name and IP Addressing" on page 113
- "Bandwidth Limiting" on page 118
- "Busy-File Processing (UNIX Clients Only)" on page 122
- "Configuring E-mail Notifications" on page 129
- "Specifying the Locale of the NetBackup Installation" on page 130
- "Adjusting Time Zones in the NetBackup-Java Console" on page 131
- "NetBackup Configuration Options" on page 134
- "Restricting Administrative Privileges of Media Servers" on page 181

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 smaller than the largest allowed value. Also, enable fast-tape positioning (locate block), if it applies to the tape drives you are using.

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 51 in the *System Administrator's Guide, Volume I*.) The number can range from 1 through 32, 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, for all storage units, of the concurrent backup jobs that can run on each storage unit.
- The maximum number of concurrent backup jobs that can run on a single storage unit is equal to the Maximum Multiplexing per drive, multiplied 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. This setting is discussed in the section "Media Multiplexing" on page 171 in the *System Administrator's Guide, Volume I.* 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 32, 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.

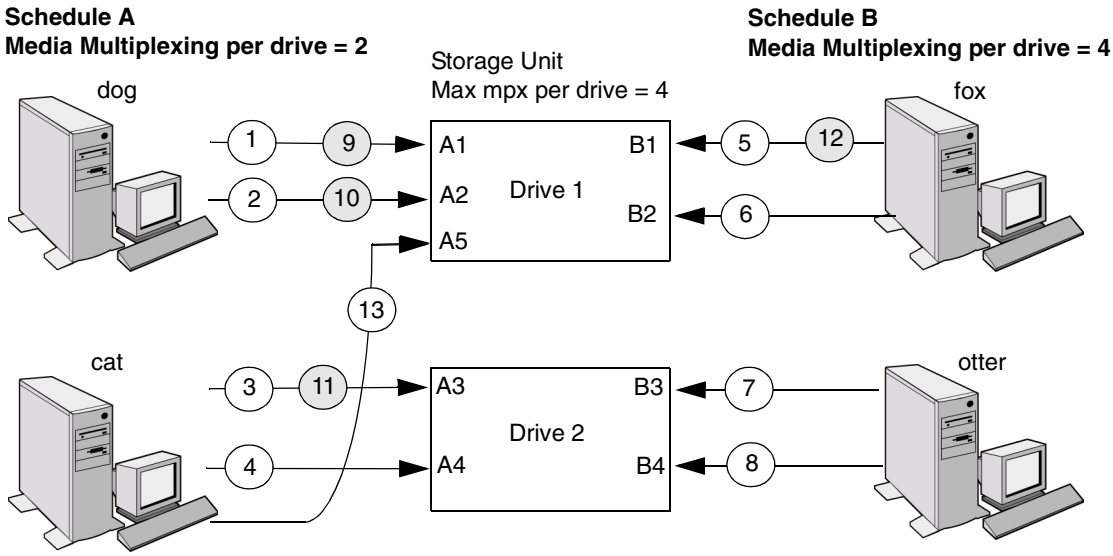
When NetBackup multiplexes jobs, it continues to add jobs to a drive until the number of jobs on the drive matches either of the following:

- 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 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 81 in the *System Administrator's Guide, Volume I*.)

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. This can be set with the `bpconfig` command. (See "Setting the Number of Streams That Can Run Concurrently" on page 95 in the *System Administrator's Guide, Volume I*.)

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

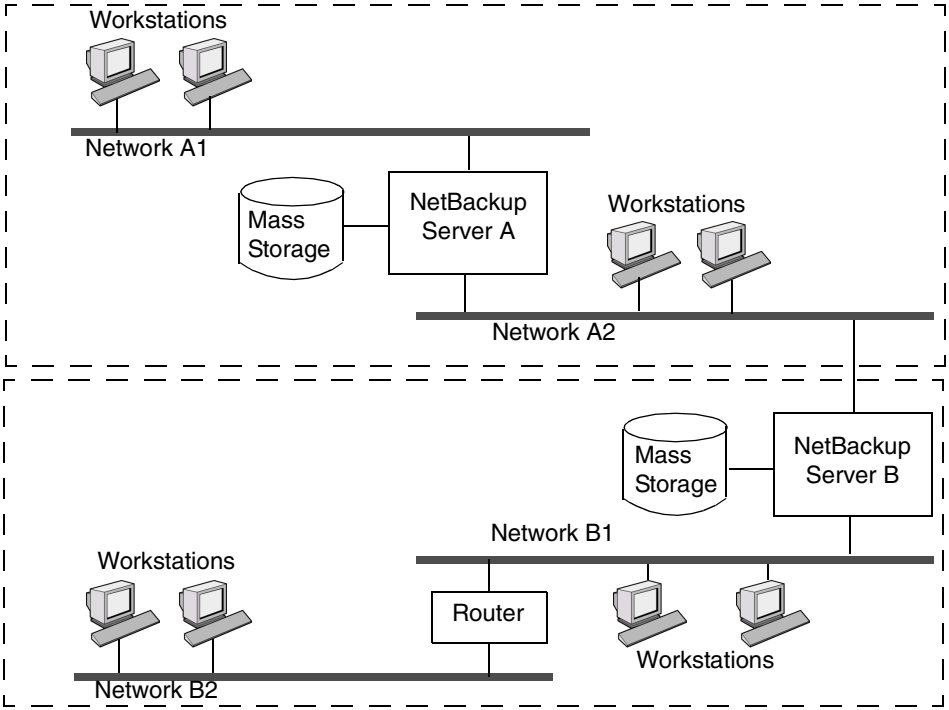
Demultiplexing speeds up future restores and is also useful for creating a copy for off-site storage. Use duplication to demultiplex a backup. Duplication lets you copy one multiplexed backup at a time form the source media to the target media. When duplication is complete, the target contains a single demultiplexed copy of each duplicated backup. (The target can also have other backups.) If desired, you can make the duplicate copy the primary copy. Do not select Preserve Multiplexing when duplicating the backups.

Note If you use the `bpduplicate` command instead of the NetBackup Administration Console, do not include the `-mpx` option on that command.

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. You can also create a configuration where one server is the master and the other is a media server.



Configuring a Master and Media Server Grouping

NetBackup lets you set up a group of NetBackup servers where one server is the master and the others are used only as media servers and have peripherals to provide additional storage. The master server controls all backup scheduling and the other media servers provide additional storage.

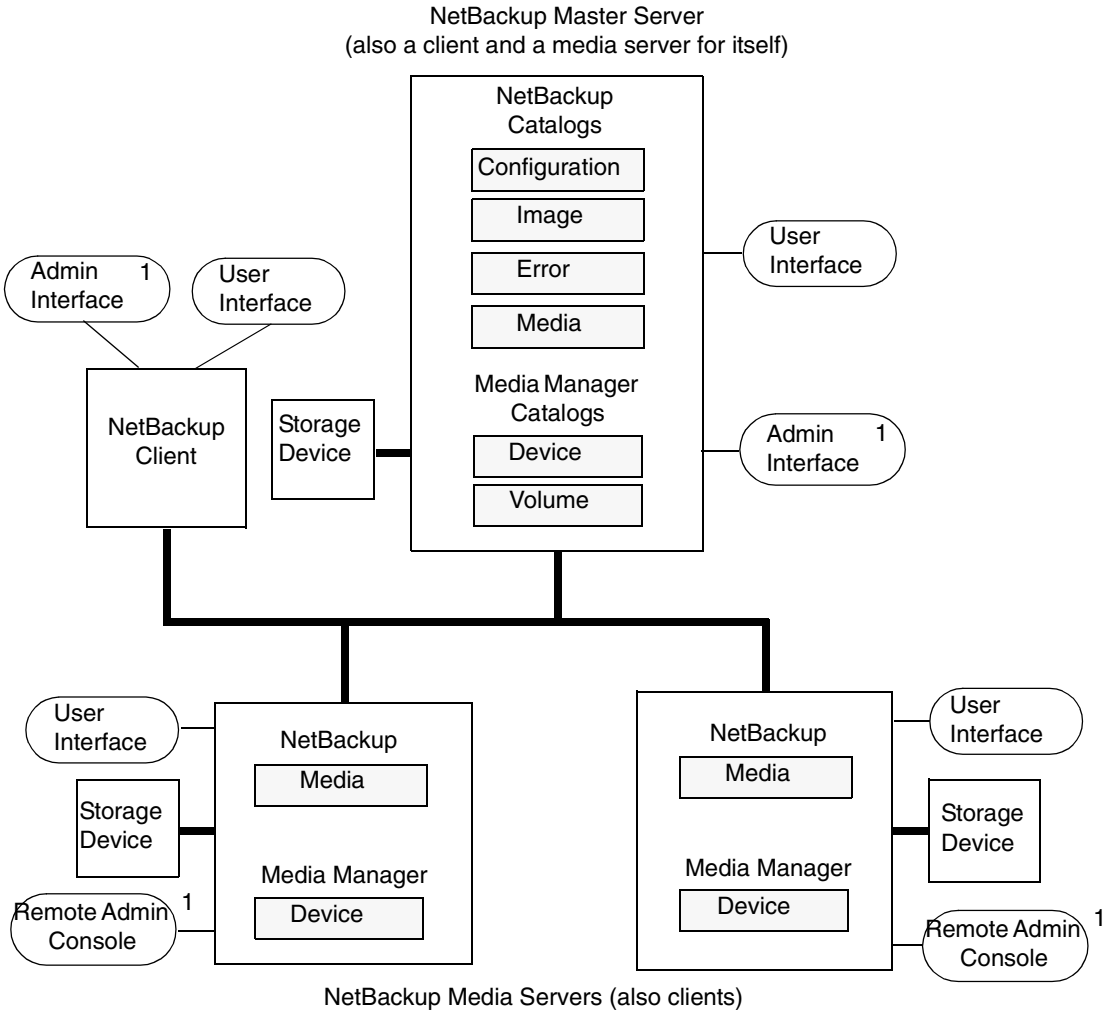
Grouping refers collectively to the master and its media servers. In a grouping of NetBackup servers, a client can have its backup directed to any device on any server in the grouping.

A common strategy is to install extra peripherals on clients that produce large amounts of data and make them media servers. The data from the client is then directed to the client's own peripherals. This reduces network traffic by allowing the data to be backed up without transferring it over the network. It also distributes the backup load between the master and the media servers.

Two important points to remember about master and media servers:

- There can be only one master server in a grouping.
- A NetBackup server is a media server for itself but cannot be a media server for another master.

The following figure shows where software is installed and where the NetBackup catalogs are located. The following topics provide more details on master and media servers along with a procedure to configure them.



NOTES

1. You can also use the Backup, Archive, and Restore NetBackup user interface from a Windows client that has the Remote Administration Console installed.

Software on Each Server

Applies to NetBackup Enterprise Server only.

You install NetBackup server software on each NetBackup server that has a peripheral that you want to include in a storage unit. The NetBackup install program has choices for master and media server installation.

NetBackup Catalogs

Applies to NetBackup Enterprise Server only.

The master server has a complete set of NetBackup and Media Manager catalogs (the media and device catalogs contain information for only the master server). Additional media servers have only two catalogs:

- Media: Contains information on media used for backups on the drives attached to the media server.
- Device: Contains information on drives and robots configured on the media server.

Special Note on Configuring Volumes

To simplify administration, it is recommended that you use only one server as a volume database host and add all your volumes on that host. Multiple configurations make administration more complicated and it is not possible to merge the volume information later.

Note Regardless of which server is the volume database host, the one that has the drive always requests the media. If the media isn't available, the mount request shows up on the server with the drive.

NetBackup and Media Manager Daemons

Applies to NetBackup Enterprise Server only.

The NetBackup database manager (`bpdbm`) is used only on master servers.

On Windows servers, the equivalents to the NetBackup and Media Manager daemons on UNIX servers are as follows:

- NetBackup Device Manager service = Media Manager device daemon (`ltid`)
- NetBackup Client service = NetBackup client daemon (`bpcd`)
- NetBackup Request Manager service = NetBackup request daemon (`bprd`)
- NetBackup Volume Manager service = Media Manager volume daemon (`vmd`)

- NetBackup Database Manager service = NetBackup database manager (`bpdbm`)

▼ To add media servers

Applies to NetBackup Enterprise Server only.

Note For information on configuring a NetBackup Windows server, see the *NetBackup System Administrator's Guide for Windows*.

1. Install the following software packages on the media server as explained in the vendor's documentation:
   - Any software required to drive the storage devices. This refers to software that the storage-device vendor provides.
   - NetBackup server software as explained in the *NetBackup Installation Guide for UNIX.*

     If you decide to make a UNIX media server a client, install the client software from the master server, not from the distribution media. When the installation script asks you if the host is the master server, reply no and enter the name of the master server when prompted for it.
2. On a Windows media server, configure the drives and robots as explained in the *Media Manager System Administrator's Guide for Windows*.
3. On a UNIX media server, configure the drives and robots using the following steps.
   a. Log in to the media server.
   b. Create the necessary device files, if this was not done at the time the devices were installed. If necessary, refer to the documentation for the device and your host system. The *Media Manager Device Configuration Guide* has advice on creating device files.
   c. Configure the robots and drives within Media Manager as instructed in the *Media Manager System Administrator's Guide for UNIX*.

      Remember, the server that you specify as the Volume Database Host is the one that will keep records of volumes used in this device. The Volume Database Host can be any of the following:
      - Master server
      - Media server that you are currently adding
      - Another media server

Note Use only one server as a volume database host and add all your volumes on that host. Multiple volume database hosts complicate administration and it is not possible to merge the volume information later.

4. Add the volumes for each robot or nonrobotic drive configured in step 2 or step 3.

Always add the volumes on the server that you specified as the volume database host for the devices in step 2 or step 3. See the *Media Manager System Administrator's Guide for UNIX* for instructions on adding volumes.

Note Defining a separate volume pool for volumes used on the media server can simplify administration.

5. On the master server, make the following changes to the NetBackup configuration:

a. Add the media server's storage units. Remember, when adding the storage units, always specify the media server as the media server for the storage unit.

b. Add the catalog paths for the media server to the NetBackup catalog backup configuration. For instructions, see Chapter 4, "Managing Catalogs and Images" on page 199 in the *System Administrator's Guide, Volume I*.

Paths on a Windows media server:

media_server_name:*install_path*\NetBackup\db

media_server_name:*install_path*\Volmgr\database

Where *install_path* is the directory where the NetBackup software is installed on the media server.

Paths on a UNIX media server:

media_server_name:/usr/openv/netbackup/db/media

media_server_name:/usr/openv/volmgr/database

c. Configure the NetBackup policies and schedules that use the storage units you configured on the media server.

6. Run the `/usr/openv/netbackup/bin/add_slave_on_clients` script from the master server to add the name of the new media server to the `/usr/openv/netbackup/bp.conf` file on each UNIX client.

If the update fails on any client, either:

- Fix the problem and rerun `add_slave_on_clients`. Or,

- Edit the `/usr/openv/netbackup/bp.conf` files on the clients that fail by adding the following below the entry for the master server (which is always the first `SERVER` entry):

  `SERVER = media_server_name`

  where *`media_server_name`* is the host name of the media server.

Note You will encounter problems with NetBackup, unless the host names in the `bp.conf` file match those shown in the `/etc/hosts` file (or appropriate NIS, or DNS file).
The host names must also match throughout your network. If you are using NIS, this applies to the NIS hosts file. See "Rules for Using Host Names in NetBackup" on page 328, for more information on choosing host names for NetBackup hosts and clients.
In addition, the `SERVER` entries MUST be the same on all servers in a master and media server grouping. It is recommended (but not mandatory) that all other `bp.conf` entries, except `CLIENT_NAME`, also match on all servers.

7. On each PC client, add `SERVER` entries for the new media server.

- For most PC clients, you can add these entries through the user interface on the client. For instructions on a specific client, see the NetBackup user's guide for that client.
- The first `SERVER` entry in each case must be that of the master server. An entry for the media server must appear lower in the list:

  ```
  SERVER = master_name
  SERVER = media_server_name
  ```

8. On the master server, stop and restart the NetBackup request daemon (`bprd`) and database daemon (`bpdbm`).

a. To stop `bprd`, run the following:

```
/usr/openv/netbackup/bin/admincmd/bprdreq -terminate
```

b. To stop `bpdbm`, run the following:

```
/usr/openv/netbackup/bin/bpdbm -terminate
```

c. To restart both daemons, run the following:

```
/usr/openv/netbackup/bin/initbprd
```

9. Test your configuration by performing a user backup or a manual backup that uses a schedule specifying a storage unit on the media server.

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, NIS, 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 5 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 select **File** > **NetBackup Client Properties**. The NetBackup Client Properties dialog appears. Select the **General** tab. Change the **Client Name** to 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 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
123.123.123.73 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 20 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
.
.
.
nbclient20
```

Configuring the NetBackup Master 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:

`/usr/openv/netbackup/db/client`

You can create, update, list, and delete client entries with the `bpclient` command. The `bpclient` command is in the following directory:

`/usr/openv/netbackup/bin/admincmd`

- To create a dynamic client entry:

  `bpclient -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 -delete -client` *`client_name`*

- To list a client entry:

```
bpclient -L -client client_name
```

- To list all client entries:

```
bpclient -L -All
```

In our example, you can enter these commands to create the 20 clients:

```
cd /usr/openv/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
.
.
.
bpclient -add -client nbclient20 -dynamic_address 1
```

To see what is currently in the client database, run `bpclient` as follows:

```
/usr/openv/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
.
.
.
Client Name: nbclient20
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 on the Windows client.

Start the Backup, Archive, and Restore user interface on the client and select **File** > **NetBackup Client Properties**. The NetBackup Client Properties dialog appears. Select the **General** tab. Change the **Client Name** to specify the NetBackup client name for the Windows client.

In the NetBackup Administration Console, set **Announce DHCP Interval** to specify how many minutes the client waits before announcing that it is using a different IP address. (See "Announce DHCP Interval" on page 374 in the *System Administrator's Guide, Volume I*.)

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 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 the following clients:
  - NetBackup for Oracle clients
  - NetBackup for DataTools SQL-BackTrack clients
  - 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 **NetBackup Management** > **Host Properties** > **Master Servers** > **Bandwidth**. (See “Bandwidth Properties” on page 314 in the *System Administrator’s Guide, Volume I*.)

Or, add one or more `LIMIT_BANDWIDTH` entries to the `/usr/openv/netbackup/bp.conf` file 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. For information on adding these entries, see “LIMIT_BANDWIDTH” on page 153.

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 `bp.conf` file 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

Busy-File Processing (UNIX Clients Only)

Note Busy-file processing applies only to UNIX clients.
For information concerning Microsoft Windows clients, see "VSP (Volume Snapshot Provider) Properties" on page 396 in the *System Administrator's Guide, Volume I*. For clients other than Windows and UNIX, see "OTM Properties" on page 375 in the *System Administrator's Guide, Volume I*.

A busy file is a file that was detected as changed during a user or scheduled backup. Typically, this occurs if a process is writing to a file while NetBackup is attempting to back it up. The backup usually completes with a status of 1, indicating that the backup was partially successful. The busy-file processing feature lets the user control the actions of NetBackup when busy files are detected.

To enable busy-file processing, you add the `BUSY_FILE_PROCESSING` option to the client `/usr/openv/netbackup/bp.conf` file. You then add other busy-file options to control the processing of busy files. These other options can exist in both the client `/usr/openv/netbackup/bp.conf` file and a user's `bp.conf` (the user's `bp.conf` file takes precedence when the options are in both places).

NetBackup creates several files and directories when processing busy files. Initially, a working directory named `busy_files` is created under `/usr/openv/netbackup`. NetBackup then creates an `actions` directory under `busy_files` and places `action` files in that directory. An `action` file has the information that NetBackup uses to control the processing of busy files. By default, the contents of the action file are derived from the `BUSY_FILE_ACTION` options in `bp.conf`. A user can also create an action file in order to control a specific backup policy and schedule. NetBackup creates a logs directory under `busy_files` for storing busy file status and diagnostic information.

Getting Started

Perform the following steps to enable the busy files feature:

- Modify the `bp.conf` file options as described in the following section, "Modifying bp.conf" on page 123.
- Copy the script

  `/usr/openv/netbackup/bin/goodies/bpend_notify_busy`

  to

  `/usr/openv/netbackup/bin/bpend_notify.`

  Be sure to set the file access permissions to allow *group* and *other* to execute `bpend_notify`.
- Configure a policy with a user backup schedule to be used by busy-file backups.

  This policy will service the backup requests generated by the `repeat` option in the `actions` file. The policy name is significant, since by default, NetBackup searches alphabetically (upper-case characters first) for the first available policy with a user backup schedule and an open backup window. For example, a policy name of `AAA_busy_files` is selected ahead of `B_policy`.

Modifying bp.conf

The user can direct busy-file processing by setting the following in the `bp.conf` file.

BUSY_FILE_PROCESSING

Used in a `/usr/openv/netbackup/bp.conf` file on a client, this option enables the NetBackup busy-file-processing feature. By default, this option is not in `bp.conf`, thus disabling busy-file processing.

BUSY_FILE_DIRECTORY

Used in a `/usr/openv/netbackup/bp.conf` or `$HOME/bp.conf` file on a client, this option specifies the path to the busy files working directory. By default, `bp.conf` does not contain this option and NetBackup creates the `busy_files` directory in `/usr/openv/netbackup`.

BUSY_FILE_ACTION

Used in a `/usr/openv/netbackup/bp.conf` or `$HOME/bp.conf` file on a client, this option directs the action that NetBackup performs on busy files. There can be multiple entries of the following form:

`BUSY_FILE_ACTION =` *`filename_template action_template`*

Where

- *`filename_template`* is the absolute pathname and file name of the busy file. The shell language metacharacters `*, ?, [], [ - ]` can be used for pattern matching of filenames or parts of filenames.
- *`action_template`* is one of the following:

  `MAIL | mail`

  Directs NetBackup to mail a busy file notification message to the user specified by the `BUSY_FILE_NOTIFY_USER` option.

  `REPEAT | repeat [repeat_count]`

  Directs NetBackup to retry the backup on the specified busy file. A repeat count can be specified to control the number of backup attempts. The default repeat count is 1.

  `IGNORE | 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.

  `BUSY_FILE_NOTIFY_USER`

Used in a /usr/openv/netbackup/bp.conf or $HOME/bp.conf file on a client, this option specifies the recipient of the busy file notification message when BUSY_FILE_ACTION is set to MAIL or mail. By default, BUSY_FILE_NOTIFY_USER is not in bp.conf and the mail recipient is root.

Examples

Example 1

```
BUSY_FILE_PROCESSING
BUSY_FILE_NOTIFY_USER = kwc
BUSY_FILE_ACTION = /usr/* mail
BUSY_FILE_ACTION = /usr/local ignore
```

NetBackup will send an E-mail notification message to the user kwc for all busy files that it finds under /usr, except for those in /usr/local.

Example 2

```
BUSY_FILE_PROCESSING
BUSY_FILE_ACTION = /usr/openv mail
BUSY_FILE_ACTION = /usr/* repeat 2
BUSY_FILE_ACTION = /usr/local ignore
```

This set of options causes NetBackup to take the following actions when it encounters busy files:

- Send a busy-file-notification message to root for busy files in /usr/openv.
- Repeat the backup up to a maximum of two times for all busy files that it finds under /usr, except for those in /usr/openv and /usr/local.
- Exclude the busy files in /usr/local from all actions.

Creating Action Files

When a backup operation begins, NetBackup creates a default action file named actions in the busy_files/actions directory. The contents of the actions file are derived from the BUSY_FILE_ACTION options in the bp.conf file.

NetBackup refers to the default action file for all future busy-file processing, unless you override the default by creating an action file to control a specific backup policy and schedule. The naming convention for the policy and schedule action files is one of the following:

actions.*policy_name.schedule_name*
actions.*policy_name*

Where *policy_name* and *schedule_name* correspond to a predefined backup policy and schedule.

When searching for an action file, NetBackup does the following:

1. Checks for a file that names a specific policy and schedule, such as:

   actions.*policy_name.schedule_name*

2. If a file for a specific policy and schedule is not found, NetBackup searches for a less-specific name, such as the following:

   actions.*policy_name*

3. If a less-specific name does not exist, NetBackup refers to the default action file.

The contents of user-created action files are similar to the default. Optional comment lines can be included and the specification is the same as for the BUSY_FILE_ACTION option:

```
# comment_line
filename_template action_template
```

Example 1

The bp.conf file might contain the following:

```
BUSY_FILE_ACTION = /usr/openv mail
BUSY_FILE_ACTION = /usr/* repeat 2
BUSY_FILE_ACTION = /usr/local ignore
```

If it does, the default actions file, named actions, will contain the following:

```
/usr/openv mail
/usr/* repeat 2
/usr/local ignore
```

Example 2

An action file name for a backup policy production_servers with a schedule name full follows:

```
actions.production_servers.full
```

The actions file can contain the following:

```
/bin/* repeat
```

If it does, NetBackup repeats the backup for busy files in the /bin directory.

Logs Directory

During busy-file processing NetBackup creates a number of files under the `busy_files/logs` directory. These files contain status and diagnostic information that is recorded by NetBackup. NetBackup derives the names of these files from the policy name, schedule name, and process id (PID) of the backup.

- Busy-file log

  NetBackup records the names of any busy files in the busy file log. The name of the busy-file log has the following form:

  `policy_name.schedule_name.PID`

- Diagnostic-log file

  NetBackup generates a log file that contains diagnostic information. The name of the log file has the following form:

  log.*`policy_name.schedule_name.PID`*

- Retry-log file

  NetBackup also generates a retry file that contains diagnostic information that is recorded when the `repeat` option is specified. The name of the retry file has the following form:

  `policy_name.schedule_name.PID.retry.retry_count`

  Where *`retry_count`* starts at zero and is incremented by one every time a backup is repeated. Processing stops when *`retry_count`* is one less than the number specified on the `repeat` option.

Example

To service busy-file backup requests, the administrator defined a policy named AAA_busy_files that has a user backup schedule named user. A scheduled backup is initiated with the policy named production_servers, schedule named full, and PID of 1442.

If busy files are detected, NetBackup generates the following files in the `/usr/openv/netbackup/busy_files/logs` directory:

```
production_servers.full.1442
log.production_servers.full.1442
```

If the actions file has repeat count set to 2, NetBackup generates the following files:

```
production_servers.full.1442.retry.0
AAA_busy_files.user.10639
log.AAA_busy_files.user.10639
```

If a second repeat backup is attempted, NetBackup generates the following files:

```
production_servers.full.1442.retry.1
AAA_busy_files.user.15639
log.AAA_busy_files.user.15639
```

Modifying bpend_notify_busy

The administrator can modify busy-file processing by changing the `bpend_notify_busy` script. The *only* recommended changes are as follows:

- Changing the `RETRY_POLICY` and `RETRY_SCHED` variables from `NONE` to the busy-file-backup policy name and schedule name.
- Remove the files in the logs directory after busy-file processing (these logs are not removed automatically):

  a. At the end of the `busy_files()` function, add the following command:

  ```
  /bin/rm -f $LOG_FILE
  ```

  b. After the call to the `busy_files()` function in main, add the following commands:

  ```
  /bin/rm -f $BUSYFILELOG
  /bin/rm -f $RETRY_FILE
  ```

Configuring E-mail Notifications

You can configure NetBackup to send e-mail notifications to users and administrators with the results of backup, archive, and restore operations.

The types of notifications you can configure are as follows:

- Notify server administrators when a scheduled backup, administrator-directed manual backup, or a backup of the NetBackup databases occurs.

  Configure NetBackup to E-mail these notifications by specifying the server administrator's address with the NetBackup master server Global Attribute property, **Administrator's E-mail Address**. (See the *NetBackup System Administrator's Guide, Volume I*.)

  If you customize the `dbbackup_notify` script to include an e-mail message and recipient, this script also sends a message after each NetBackup database backup.

- Notify users on UNIX clients as to the success or failure of their user operations.

  To configure these notifications, specify the user's e-mail address with the `USEMAIL` option in the user's personal `bp.conf` file. This file is located in the user's home directory (create one if necessary).

- Notify system administrators of UNIX clients about the success or failure of scheduled or manual backups.

  To configure these notifications, specify the client administrator's address with the `USEMAIL` option in the `/usr/openv/netbackup/bp.conf` file on the client.

You can also set up e-mail notifications with the scripts provided with NetBackup UNIX server software. (See "Goodies Scripts" on page 450.)

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 the Locale of a 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.

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.
	
	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 to 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.

To Specify the Locale of a NetBackup Installation (continued)

Platform	Directions

	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 defines 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`).

Adjusting Time Zones in the NetBackup-Java Console

Sites in a geographically dispersed NetBackup configuration may need to adjust the time zone in the NetBackup-Java Console for administration of remote NetBackup hosts. (In this context, a remote NetBackup host may either be the host specified in the console login dialog or one referenced via the **File** > **Change Server** capability in the console.)

The default time zone for the console is that of the host on which the console is started, not the host specified (if different) in the console login dialog.

- For backup, restore or archive operations from within the NetBackup-Java Console (`jnbSA`) or the Backup, Archive, and Restore application when running on a client (`jbpSA`), the time zone should be set relative to that of the NetBackup server from which the client restores files.
- When administering servers in different time zones, the time zone must be set in separate instances of the NetBackup-Java Console.

  For example, open a NetBackup-Java Console to set the time zone for your local server in the Central time zone. To set the time zone for a server in the Pacific time zone as well, open another NetBackup-Java Console.

  Do not simply open a new window (**File** > **New Window from Here**) in the first NetBackup-Java Console, change servers (**File** > **Change Server**), and set the time zone for the Pacific time zone server. Doing so changes the time zone for the Central time zone server as well.

▼ To set the time zone and Daylight Savings Time

1. In the NetBackup Administration Console, or in the Backup, Archive, and Restore client interface, select **File** > **Adjust Application Time Zone**. The Adjust Time Zone dialog appears.

2. To use the **Standard** tab to configure the time zone:

   a. Clear the **Use custom time zone** check box.

   b. Select the time zone.

   c. To use daylight savings time, select **Use daylight savings time**.

   d. To have administrative capabilities and apply the settings to the current session and all future sessions, select **Save as default time zone**.

3. To use the Custom tab to configure the time zone:

   a. Select the **Use custom time zone** check box.

   b. Select the time zone on which to base the Backup, Archive, and Restore interface time. For a list of time zones, see Time Zone Table.

   c. Adjust the time to reflect how many hours/minutes the server's time zone is offset (either behind or ahead) of Greenwich Mean Time.

   d. To use daylight savings time, select **Use daylight savings** time.

   e. Indicate when Daylight Savings Time (DST) should begin. You can use one of the following methods:

      - To begin DST on a specific date, select **Absolute date** and indicate the desired month and day.
      - To begin DST on the first occurrence of a day in a month, select **First day of week in month** and indicate the desired day of the week and the month.
      - To begin DST on the first occurrence of a day in a month and after a specific date, select **First day of week in month after date** and indicate the desired day of the week and the month and day.
      - To begin DST on the last occurrence of a day in a month, select **Last day of week in month** and indicate the desired day of the week and the month.

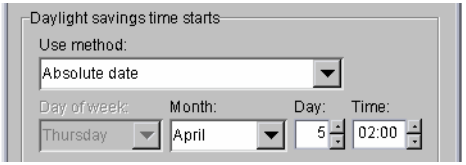
- To begin DST on the last occurrence of a day in a month and before a specific date, select **Last day of week in month after date** and indicate the desired day of the week and the month and day.

f. Select the appropriate **Day of week**, **Month**, **Day**, and **Time**.

Select **Absolute date** to have DST begin on a specific date.

Indicate the desired month and day.

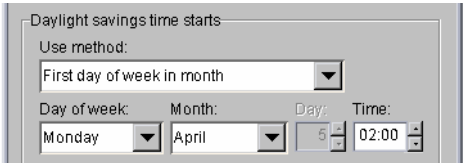
To have DST begin on April 5:



Select **First day of week in month** to have DST begin on the first occurrence of a day in a month.

Indicate the desired day of the week and the month.

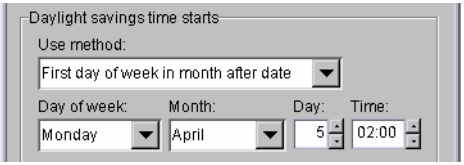
To begin DST on the first Monday in April:



Select **First day of week in month after date** to have DST begin on the first occurrence of a day in a month and after a specific date.

Indicate the desired day of the week and the month and day.

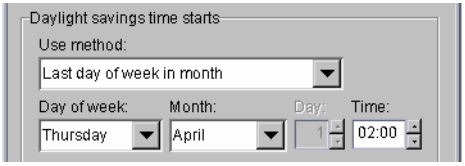
To begin DST on the first Monday after April 5:



Select **Last day of week in month** to have DST begin on the last occurrence of a day in a month.

Indicate the desired day of the week and the month.

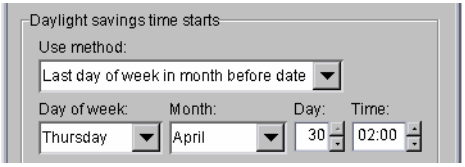
To begin DST on the last Thursday in April:



Select **Last day of week in month after date** to have DST begin on the last occurrence of a day in a month and before a specific date.

Indicate the desired day of the week and the month and day.

To begin DST before April 30:



g. Indicate when DST should end, using one of the methods defined in step e.

h. To have administrative capabilities and apply the settings to the current session and all future sessions, select **Save as default time zone**.

4. Click **OK**.

NetBackup Configuration Options

The NetBackup configuration options allow the administrator to customize NetBackup to meet specific site preferences and requirements.

Most configuration options can be set within **NetBackup Management** > **Host Properties** within **Master Servers**, **Media Servers**, or **Clients**. Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.

In most instances, the internal software defaults provide satisfactory results. However, if settings must be changed from their defaults, do so according to the following instructions.

Method for Specifying the Configuration Options

The method to use for specifying the configuration options depends on the type of server or client you are configuring.

- On NetBackup UNIX servers and clients, specify the configuration options in the `bp.conf` file as explained in this chapter.
- On NetBackup Windows servers, these options are referred to as NetBackup properties and are explained in the *NetBackup System Administrator's Guide for UNIX, Volume I*.
- On PC clients, specify configuration options as explained in the NetBackup user's guide for the client.

Note After making a change to the `/usr/openv/netbackup/bp.conf` file on the master server, stop and restart all NetBackup daemons and utilities. This ensures that the new `bp.conf` values will be used by all the NetBackup processes that require them (a process reads `bp.conf` only when it begins). This action is not required for changes to `bp.conf` files on a client or to a `$HOME/bp.conf` file on the master server.

Syntax Rules for bp.conf Options

Use the following syntax rules when creating entries in `bp.conf`:

- Use the # symbol to comment out lines
- Any number of spaces or tabs are allowed on either side of = signs
- Blank lines are allowed
- Any number of blanks or tabs are allowed at the start of a line

bp.conf Options for Master Servers

The `bp.conf` options for NetBackup UNIX servers are located in the following file:

```
/usr/openv/netbackup/bp.conf
```

If a single UNIX system is running as both a client and a server, the `/usr/openv/netbackup/bp.conf` file will contain both server and client options.

Each nonroot user on a UNIX client can also have a personal `bp.conf` file in their home directory:

```
$HOME/bp.conf
```

See the `bp.conf` discussion for UNIX clients later in this chapter for an explanation of client options and which of these can be in a personal `bp.conf` file.

Note The `SERVER` option *must* be present in the `/usr/openv/netbackup/bp.conf` file on all NetBackup UNIX clients and servers. It is also the *only required* entry in these `bp.conf` files. As installed, NetBackup uses internal software defaults for all options in the `bp.conf` file, except `SERVER`. During installation, NetBackup sets the `SERVER` option to the name of the master server where the software is installed.

Applies to NetBackup Enterprise Server only.
The `SERVER` entries *MUST* be the same on all servers in a master and media server cluster. It is recommended (but not mandatory) that all other entries, except `CLIENT_NAME`, also match on all servers.

ALLOW_MEDIA_OVERWRITE

The ALLOW_MEDIA_OVERWRITE option overrides NetBackup's overwrite protection for various media formats on removable media.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or check the **Allow Media Overwrite** setting in the Media dialog under server host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

For example, to permit overwriting the cpio format, add the following on the master server (and media servers if applicable):

```
ALLOW_MEDIA_OVERWRITE = CPIO
```

ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA

The ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA option allows NetBackup to mix retention levels on media. Default: This option is not present and each volume can contain backups of only a single retention level.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or check the **Allow Multiple Retentions per Media** setting in the Media dialog under server host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

ALLOW_NON_RESERVED_PORTS

The ALLOW_NON_RESERVED_PORTS option specifies that the NetBackup client daemon (`bpcd`) can accept remote connections from nonprivileged ports (port numbers 1024 or greater). If this entry is not present, then `bpcd` requires remote connections to come from privileged ports (port numbers 1024 or smaller). This option can be useful when NetBackup clients and servers are on opposite sides of a firewall.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX server or client. For use on a client, see "ALLOW_NON_RESERVED_PORTS" on page 137.

AUTHENTICATION_DOMAIN

The `AUTHENTICATION_DOMAIN` entry defines a set of VxSS authentication principals. A master server that uses VxSS must have at least one `AUTHENTICATION_DOMAIN` entry, and more than one can be specified.

If a media server or client does not define an authentication domain, it will use the authentication domains of its master server.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers or by setting the **Authentication Domain** in the Access Control properties under Master Server host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

```
AUTHENTICATION_DOMAIN = domain "comment" mechanism broker [ port ]
```

Where:

- *`domain`* is an Internet domain name or a Windows domain name.
- *`"comment"`* is a quoted comment describing the authentication domain.
- *`mechanism`* is the authentication mechanism. The mechanism is indicated by one of the following keywords:
  - `NIS` (Network Information Service version 1)
  - `NIS+` (Network Information Service version 2)

- PASSWD (Local UNIX password file on the specified broker)
- VXPD (VxSS private database)
- WINDOWS (Windows Active Directory or primary domain controller)

- *broker* is the host name or IP address of the authentication broker.
- *port* is the port number of the authentication broker. The default is the standard port number for authentication brokers.

Example

```
AUTHENTICATION_DOMAIN = mycompany.com "Typical UNIX logins" NIS
broker1.mycompany.com
AUTHENTICATION_DOMAIN = OurEnterprise "Typical Windows logins" WINDOWS
broker2.mycompany.com 5544
AUTHENTICATION_DOMAIN = mycompany.com "VxSS-Only Identities" VXPD
broker1.mycompany.com
AUTHENTICATION_DOMAIN = broker3.mycompany.com "Local UNIX Logins on
host broker3" PASSWD broker3.mycompany.com
```

In the example, mycompany.com is the Internet domain name and OurEnterprise is the Windows domain name.

The broker on host name broker1 handles both NIS and private authentication for VxSS.

The broker on host name broker2 handles Windows authentication for VxSS.

broker2 uses the non-standard port number 5544.

The broker on host name broker3 uses its local /etc/passwd file for VxSS authentication.

AUTHORIZATION_SERVICE

The AUTHORIZATION_SERVICE entry defines the VxSS authorization service to be used by the local NetBackup server. A master server that uses VxSS must define an authorization service. If a media server does not define an authorization service, it will use its master server's authorization service.

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup master servers or by setting the **Authorization Service** in the Access Control properties under Master Server host properties. Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.

AUTHORIZATION_SERVICE = *host* [*port*]

Where:

host is the host name or IP address of the authorization service.

port is the port number of the authorization service. The default is the standard port number for the authorization service.

BPBRM_VERBOSE

Used for debugging purposes, the BPBRM_VERBOSE option controls the amount of information NetBackup includes in its bpbrm debug log. Default: The same value as the bp.conf VERBOSE entry (**Global Logging Level**). The BPBRM_VERBOSE entry overrides the bp.conf VERBOSE entry.

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup servers or set the **BPBRM Logging Level** in the Logging host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

To use the same value as the bp.conf VERBOSE entry for bpbrm, enter:

```
BPBRM_VERBOSE = 0
```

This is the same as setting **BPBRM Logging Level** in the Logging host properties to *Same as Global*.

To log the minimum amount of information for bpbrm, enter:

```
BPBRM_VERBOSE = -1
```

This is the same as setting **BPBRM Logging Level** in the Logging host properties to 0.

To log additional information for bpbrm, enter a value of 1 through 5:

```
BPBRM_VERBOSE = 1
```

This is the same as setting **BPBRM Logging Level** in the Logging host properties to 1.

To log the maximum amount of information for bpbrm, enter:

```
BPBRM_VERBOSE = 5
```

This is the same as setting **BPBRM Logging Level** in the Logging host properties to 5.

For information about enabling the bpbrm debug log, see the section titled, "Debug Logs" in the *NetBackup Troubleshooting Guide for UNIX and Windows*.

BPDBJOBS_COLDEFS

Add BPDBJOBS_COLDEFS entries to the `bp.conf` file to customize the output of `bpdbjobs`. Add a BPDBJOBS_COLDEFS entry for every column you wish to include in the output using the following format:

`BPDBJOBS_COLDEFS = COLDEFS_ENTRY [minimum_size [true | false]]`

Where:

`COLDEFS_ENTRY` is the name of the column to include in the output. See the following table for valid BPDBJOBS_COLDEFS entries.

`minimum_size` is the minimum column width. If not specified, the default is a width of 5.

`true` indicates that the column should expand as needed. If not specified, `true` is the default.

`false` indicates that the column should not expand beyond the *`minimum_size`*.

The order of the entries determines the order that the column headings will appear.

Example

```
BPDBJOBS_COLDEFS = JOBID 5 true
BPDBJOBS_COLDEFS = TYPE 4 true
BPDBJOBS_COLDEFS = STATE 5 true
BPDBJOBS_COLDEFS = STATUS 6 true
BPDBJOBS_COLDEFS = POLICY 6 true
BPDBJOBS_COLDEFS = SCHEDULE 8 true
BPDBJOBS_COLDEFS = CLIENT 6 true
BPDBJOBS_COLDEFS = DSTMEDIA_SERVER 12 true
BPDBJOBS_COLDEFS = ACTPID 10 true
```

Note Keep in mind the following ramifications of adding a BPDBJOBS_COLDEFS entry to the `bp.conf` conditions:
– Adding even one `BPDBJOBS_COLDEFS` entry overrides all default columns.
– All users on the local system will see only those columns specified in the `bp.conf` file.

BPDBJOBS_COLDEFS Entries and Corresponding Column Head Names

COLDEFS Entry	Column Name	COLDEFS Entry	Column Name
ACTIVEELAPSED	**Active Elapsed** (elapsed active time)	PATHNAME	**KB Per Sec**
ACTPID	**Active PID** (PID of job)	PARENTJOBID	**Parent JobID**
ATTEMPT	**Attempt**	POLICY	**Policy**
BACKUPTYPE	**Backup Type**	POLICYTYPE	**Policy Type**
CLIENT	**Client**	PRIORITY	**Priority**
COMPLETION	**Completion** (percent complete)	PROFILE	**Profile** (Vault only)
COMPRESSION	**Compression** (yes or no)	RETENTION	**Retention** (retention period)
DSTMEDIA_SERVER	**Dest Media Svr** (writing media server)	RESUMABLE	**Resumable**
DSTMEDIAID	**Dest Media ID** (writing media ID)	ROBOT	**Robot** (Vault only)
DSTSTORAGE_UNIT	**Dest StUnit** (writing storage unit)	RQSTPID	**Request PID** (PID requesting job, if applicable)
ELAPSED	**Elapsed** (elapsed time)	SCHEDULE	**Schedule**
ENDED	**Ended**	SCHEDULETYPE	**Schedule Type**
ESTFILE	**Est File** (estimated number of files)	SESSIONID	**Session ID** (Vault only)
ESTKB	**Est KB** (estimated number of kilobytes)	SRCMEDIA_SERVER	**Src Media Svr**
FILES	**Files**	SRCMEDIAID	**Src Media ID**
GROUP	**Group**	SRCSTORAGE_UNIT	**Src StUnit**
JOBID	**JobID**	STARTED	**Started**

BPDBJOBS_COLDEFS Entries and Corresponding Column Head Names (continued)

COLDEFS Entry	Column Name	COLDEFS Entry	Column Name
KBPERSEC	**Pathname**	STATE	**State**
KILOBYTES	**Kilobytes**	STATUS	**Status**
LASTBACKUP	**Last Backup** (date and time)	STREAMNUMBER	**Stream Number**
MAINPID	**Main PID** (PID spawning job, if applicable)	SUSPENDABLE	**Suspendable**
NUMTAPESEJECT	**Media to Eject** (number of tapes to eject; Vault only)	TYPE	**Type** (job type)
OPERATION	**Operation** (current operation)	VAULT	**Vault** (Vault only)
OWNER	**Owner**		

BPDBM_VERBOSE

Used for debugging purposes, the `BPDBM_VERBOSE` option controls the amount of information NetBackup includes in its `bpdbm` debug log. Default: The same value as the `bp.conf VERBOSE` entry (**Global Logging Level**). The `BPDBM_VERBOSE` entry overrides the `bp.conf VERBOSE` entry (**Global Logging Level**).

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or set the **BPDBM Logging Level** in the Logging host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

To use the same value as the `bp.conf VERBOSE` entry for `bpdbm`, enter:

```
BPDBM_VERBOSE = 0
```

This is the same as setting **BPDBM Logging Level** in the Logging host properties to *Same as Global*.

To log the minimum amount of information for `bpbrm`, enter:

```
BPDBM_VERBOSE = -1
```

This is the same as setting **BPDBM Logging Level** in the Logging host properties to 0.

To log additional information for `bpdbm`, enter a value of `1` through `5`:

```
BPDBM_VERBOSE = 1
```

This is the same as setting **BPDBM Logging Level** in the Logging host properties to 1.

To log the maximum amount of information for bpdbm, enter:

```
BPDBM_VERBOSE = 5
```

This is the same as setting **BPDBM Logging Level** in the Logging host properties to 5.

The following examples show two bp.conf entries that enable logging, while minimizing the rate of growth of the bpdbm debug file:

```
VERBOSE = 5
BPDBM_VERBOSE = -1
```

For information about enabling the bpdbm debug log, see the *NetBackup Troubleshooting Guide for UNIX and Windows*.

BPRD_VERBOSE

Used for debugging purposes, the BPRD_VERBOSE option controls the amount of information NetBackup includes in its bprd debug logs. Default: The same value as the bp.conf VERBOSE entry (**Global Logging Level**). The BPRD_VERBOSE entry overrides the bp.conf VERBOSE entry (**Global Logging Level**).

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup servers or set the **BPRD Logging Level** in the Logging host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

To use the same value as the bp.conf VERBOSE entry for bprd, enter:

```
BPRD_VERBOSE = 0
```

This is the same as setting **BPRD Logging Level** in the Logging host properties to *Same as Global*.

To log the minimum amount of information for bprd, enter:

```
BPRD_VERBOSE = -1
```

This is the same as setting **BPRD Logging Level** in the Logging host properties to 0.

To log additional information for bprd, enter a value of 1 through 5:

```
BPRD_VERBOSE = 1
```

This is the same as setting **BPRD Logging Level** in the Logging host properties to 1.

To log the maximum amount of information for bprd, enter:

```
BPRD_VERBOSE = 5
```

This is the same as setting **BPRD Logging Level** in the Logging host properties to 5.

For information about enabling the bprd debug log, see the section titled, "Debug Logs" in the *NetBackup Troubleshooting Guide for UNIX and Windows*.

BPSCHED_VERBOSE

Used for debugging purposes, the `BPSCHED_VERBOSE` option controls the amount of information NetBackup includes in its `bpsched` debug logs. Default: The same value as the `bp.conf VERBOSE` entry (**Global Logging Level**). The `BPSCHED_VERBOSE` entry overrides the `bp.conf VERBOSE` entry (**Global Logging Level**).

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or set the **BPSCHED Logging Level** in the Logging host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

To use the same value as the `bp.conf VERBOSE` entry for `bpsched`, enter:

```
BPSCHED_VERBOSE = 0
```

This is the same as setting **BPSCHED Logging Level** in the Logging host properties to *Same as Global*.

To log the minimum amount of information for `bpsched`, enter:

```
BPSCHED_VERBOSE = -1
```

This is the same as setting **BPSCHED Logging Level** in the Logging host properties to 0.

To log additional information for `bpsched`, enter a value of `1` through `5`:

```
BPSCHED_VERBOSE = 1
```

This is the same as setting **BPSCHED Logging Level** in the Logging host properties to 1.

To log the maximum amount of information for `bpsched`, enter:

```
BPSCHED_VERBOSE = 5
```

This is the same as setting **BPSCHED Logging Level** in the Logging host properties to 5.

The following example shows two `bp.conf` entries that enable logging, while minimizing the rate of growth of the `bpsched` debug file:

```
VERBOSE = 5
BPSCHED_VERBOSE = -1
```

For information about enabling the `bpsched` debug log, see the section titled, "Debug Logs" in the *NetBackup Troubleshooting Guide for UNIX and Windows*.

BPTM_VERBOSE

Used for debugging purposes, the `BPTM_VERBOSE` option controls the amount of information NetBackup includes in its `bptm` debug logs. Default: The same value as the `bp.conf VERBOSE` entry (**Global Logging Level**). The `BPTM_VERBOSE` entry overrides the `bp.conf VERBOSE` entry (**Global Logging Level**).

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or set the **BPTM Logging Level** in the Logging host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

To use the same value as the `bp.conf VERBOSE` entry for `bptm`, enter:

```
BPTM_VERBOSE = 0
```

This is the same as setting **BPTM Logging Level** in the Logging host properties to *Same as Global*.

To log the minimum amount of information for `bptm`, enter:

```
BPTM_VERBOSE = -1
```

This is the same as setting **BPTM Logging Level** in the Logging host properties to 0.

To log additional information for `bptm`, enter a value of `1` through `5`:

```
BPTM_VERBOSE = 1
```

This is the same as setting **BPTM Logging Level** in the Logging host properties to 1.

To log the maximum amount of information for `bptm`, enter:

```
BPTM_VERBOSE = 5
```

This is the same as setting **BPTM Logging Level** in the Logging host properties to 5.

For information about enabling the `bptm` debug log, see the section titled, "Debug Logs" in the *NetBackup Troubleshooting Guide for UNIX and Windows*.

BPEND_TIMEOUT

Note If you change this option, verify that the `CLIENT_READ_TIMEOUT` option is set to the same or higher value.

Specifies the numberof seconds to wait for the `bpend_notify` script on a client to complete. Default: Timeout is 300 seconds.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

BPSTART_TIMEOUT

Note If you change this option, verify that the `CLIENT_READ_TIMEOUT` option is also set to the same or higher value.

Specifies the number of seconds to wait for the `bpstart_notify` script on a client to complete. Default: 300 seconds.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

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). (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers. The following is an example entry:

```
BPTM_QUERY_TIMEOUT=80
```

CHECK_RESTORE_CLIENT

Specifies that the client being restored to is checked before starting the restore. This prevents an unresponsive client from slowing down the restores of other clients that have data on the same tapes. This option only applies to master servers.

CLIENT_CONNECT_TIMEOUT

Specifies the number of seconds that the server waits before timing out when connecting to a client. Default: 300 seconds.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

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 a client configured to accept nonreserved ports. For information on client configuration, see "ALLOW_NON_RESERVED_PORTS" on page 137.

You can add this option to the `/usr/openv/netbackup/bp.conf` files on NetBackup servers or clients.

The following example permits ports from 4800 through 5000:

```
CLIENT_PORT_WINDOW = 4800 5000
```

If you specify 0 for the first number (default), the operating system determines the nonreserved port to use.

Refer to "NBJAVA_CLIENT_PORT_WINDOW" on page 499 in the *System Administrator's Guide, Volume I* for connections from the NetBackup-Java console.

CLIENT_READ_TIMEOUT

Note Use this option only on a server or a database agent (such as NetBackup for Oracle). This option has a reasonable default and has to be changed only if problems are encountered.

Specifies the number of seconds to use for the client-read timeout.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

You can also add this option on database agents (such as NetBackup for Oracle).

The `CLIENT_READ_TIMEOUT` on a database agent is a special case because these types of clients can initially require more time to get ready than other clients. This is the case because database backup utilities frequently start several backup jobs at the same time, which slows the CPU.

The sequence on a database agent is as follows:

- NetBackup on the database agent reads the client's `CLIENT_READ_TIMEOUT` to find the value to use initially. If the option is not set, the standard default of five minutes is used.
- When the database agent API receives the server's value, it uses it as the `CLIENT_READ_TIMEOUT`.

Default: `CLIENT_READ_TIMEOUT` is not specified on either a server or database agent and the timeout is 300 seconds.

Note We suggest that you set `CLIENT_READ_TIMEOUT` on the database agent to a value greater than 5 minutes. A setting of 15 minutes has been found to be adequate for many installations.

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 a client configured to accept only reserved ports. For information on client configuration, see "ALLOW_NON_RESERVED_PORTS" on page 137.

You can add this option to the `/usr/openv/netbackup/bp.conf` files on NetBackup servers or clients.

The following example permits ports from 900 through 1023:

```
CLIENT_RESERVED_PORT_WINDOW = 900 1023
```

Default: Range of 512 through 1023. Note that if you specify 0 for the first number, a nonreserved port is used instead and is chosen by the operating system.

CONNECT_OPTIONS

Specifies three options designed to enhance firewall efficiency with NetBackup:

- Whether the server will be connected to using a reserved or nonreserved port number.
- Whether the server will be connected to by another server using the traditional call-back method or using the VERITAS Network daemon (`vnetd`).
- Whether the server will be connected to by using one the following methods:
  - `vnetd` or the daemon's port number,
  - by using `vnetd` only, or
  - by using the daemon's port number only.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or make your selections on the Firewall host properties dialog. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

To use this entry, add it to `/usr/openv/netbackup/bp.conf` on NetBackup servers in the following format:

```
CONNECT_OPTIONS = server_name [ 0 | 1 ][ 0 | 1 ][ 0 | 1 | 2 ]
```

Where:

- *Server_name* is the name of the server to be connected to. *Server_name* must be at NetBackup level 4.5 for `vnetd` to work.
- The first setting indicates the type of port to use to connect to *server_name*:

  `0` = Use a reserved port number (default).

  `1` = Use a nonreserved port number. If you select this option, enable **Allow Nonreserved Ports** for the selected *server_name*. See the Universal Settings dialog under **Host Properties** > **Media Servers**. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)
- The second setting indicates the call-back method to use to connect to *server_name*:

  `0` = Use the traditional call-back method (default).

`1` = Use the `vnetd` no call-back method.

- The third setting is relevant to NetBackup clients and servers. This setting indicates the connection method to use to connect to *server_name*:

  `0` = Connect to a daemon on the server using `vnetd` if possible, otherwise connect using the traditional port number of the daemon.

  `1` = Connect to a daemon on the server using `vnetd` only.

  `2` = Connect to a daemon on the server using the traditional port number of the daemon only (default).

The `bp.conf` file may contain CONNECT_OPTIONS settings for multiple servers. For example:

```
CONNECT_OPTIONS = shark 0 0 0
```

`bpcd` connections to server *shark* must use a reserved port number and the traditional call-back method.

Connections to `bpdbm`, `vmd`, `bprd`, and robotic daemons on server *shark* can use either `vnetd` or the daemon's port number.

```
CONNECT_OPTIONS = dolphin 1 0 1
```

`bpcd` connections to server *dolphin* must use a nonreserved port number and the traditional call-back method.

Connections to `bpdbm`, `vmd`, `bprd`, and robotic daemons on server *dolphin* must use `vnetd`.

```
CONNECT_OPTIONS = perch 0 1 2
```

`bpcd` connections to server *perch* must use a reserved port number and `vnetd`.

Connections to `bpdbm`, `vmd`, `bprd`, and robotic daemons on server *perch* must use the daemon's port number.

```
CONNECT_OPTIONS = trout 1 1 2
```

`bpcd` connections to server *trout* must use a nonreserved port number and vnetd.

Connections to `bpdbm`, `vmd`, `bprd`, and robotic daemons on server *trout* must use the daemon's port number.

Refer to "NBJAVA_CONNECT_OPTION" on page 499 in the *System Administrator's Guide, Volume I* for connections from the NetBackup-Java Console.

DISABLE_JOB_LOGGING

Disables the logging of job information required by the NetBackup job monitor. Default: Job logging occurs.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

DISABLE_STANDALONE_DRIVE_EXTENSIONS

Disables the nonrobotic drive operations. This means that during a backup, NetBackup does not automatically attempt to use whatever labeled or unlabeled media it finds in a nonrobotic drive. Default: Standalone drive extensions are enabled.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

DISABLE_SCSI_RESERVE

Disables the use of SCSI reserve to all tape devices from this host.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or uncheck the **Enable SCSI Reserve/Release** setting in the Media dialog host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

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). Default: Backups can span media.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

DISALLOW_CLIENT_LIST_RESTORE

Note Override the `DISALLOW_CLIENT_LIST_RESTORE` option for individual clients by changing their `list_restore` setting. (See "Setting Client List and Restore Permissions" on page 441 in the *System Administrator's Guide, Volume I*.)

Denies list and restore requests for all clients. When this option is present, clients cannot list or restore files that they have backed up through this master server. Default: This option is not present and clients can list and restore their files.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers.

DISALLOW_CLIENT_RESTORE

Note You can override the `DISALLOW_CLIENT_RESTORE` option for individual clients by changing their `list_restore` setting. (See "Setting Client List and Restore Permissions" on page 441 in the *System Administrator's Guide, Volume I*.)

Denies restore requests for all clients. When this option is present, clients cannot restore files that they have backed up through this master server. Default: This option is not present and clients can restore their files.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers.

FAILOVER_RESTORE_MEDIA_SERVERS

Applies to NetBackup Enterprise Server:

Specifies automatic failover to another NetBackup server if a server is temporarily inaccessible for a restore. This failover does not require administrator intervention. Default: NetBackup does not perform automatic failover. The format for the entry follows:

`FAILOVER_RESTORE_MEDIA_SERVERS` = *`failed_host host1 host2 ... hostN`*

Where:

`failed_host` is the server that is not operational.

`host1 ... hostN` are the servers that provide failover capabilities.

When automatic failover is necessary for a server, NetBackup searches from left to right through the associated `FAILOVER_RESTORE_MEDIA_SERVERS` list until it finds one that is eligible to perform the restore.

Note There can be multiple `FAILOVER_RESTORE_MEDIA_SERVERS` entries and each entry can have multiple servers. However, a NetBackup server can be a *`failed_host`* in only one entry.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on the NetBackup master server.

After adding the `FAILOVER_RESTORE_MEDIA_SERVERS` entry, stop and restart the NetBackup Request daemon on the master server where you are changing the configuration. (See "Server Independent Restores" on page 450 in the *System Administrator's Guide, Volume I*.)

FORCE_RESTORE_MEDIA_SERVER

Applies to NetBackup Enterprise Server:

Forces restores to go to a specific server, regardless of where the files were backed up. The format for the entry follows:

```
FORCE_RESTORE_MEDIA_SERVER = fromhost tohost
```

Where *fromhost* is the server that performed the original backup and *tohost* is the server to use for the restore.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on the NetBackup master server.

After adding the `FORCE_RESTORE_MEDIA_SERVER` entry, stop and restart the NetBackup Request daemon on the master server. Before attempting a restore, physically move the media to *tohost* and update the Media Manager volume database to reflect the move.

This setting applies to all storage units on the original server. Restores for any storage unit on `fromhost` will go to `tohost`. To revert to the original configuration for future restores, delete the entry. (See "Server Independent Restores" on page 450 in the *System Administrator's Guide, Volume I*.)

GENERATE_ENGLISH_LOGS

Enables the generation of an English error log, and English trace logs for the `bparchive`, `bpbackup`, `bpduplicate`, `bpimport`, and `bprestore` commands. This option is useful to support personnel assisting in distributed environments where differing locales result in logs with various languages.

When enabled, an English text error log (indicated by the suffix _en) is created in the following directory:

```
/usr/openv/netbackup/db/error
```

Setting the `GENERATE_ENGLISH_LOGS` option also forces the `-en` argument on the execution of all `bparchive`, `bpbackup`, `bpduplicate`, `bpimport`, and `bprestore` commands when the progress log is specified (`-L`). The English text progress log is indicated by the suffix _en.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers and clients.

INCOMPLETE_JOB_CLEAN_INTERVAL

Indicates the number of days a failed restore job can remain in the incomplete state before being moved to the done state:

```
INCOMPLETE_JOB_CLEAN_INTERVAL = x
```

Where *x* is a value between `0` and `365`. A value of `0` indicates that failed, incomplete jobs will never be automatically moved to the done state. (Default: `7` days.)

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or check the **Move Restore Job From Incomplete State to Done State** setting in the Global Attributes dialog under server host properties. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

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 the following:

```
INITIAL_BROWSE_SEARCH_LIMIT = 7
```

This option can be specified on the master server and applies to all NetBackup clients. It can also be specified on a UNIX client. When specified on a UNIX client, it 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).

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.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers and clients.

KNOWN_MASTER

Specifies the master servers that can be administered by the GDM server. Add this option to the configuration using the GDM graphical interface. (See the *Global Data Manager System Administrator's Guide*.)

Configure this option in the GDM server host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

LIMIT_BANDWIDTH

Note Read "Bandwidth Limiting" on page 118 before setting this option.

Specifies a limit for the network bandwidth used by one or more NetBackup clients on a network. The actual limiting occurs on the client side of the backup connection. This feature limits only backups. Restores are unaffected. Default: The bandwidth is not limited.

Each `LIMIT_BANDWIDTH` entry specifies the bandwidth value and the IP address of the clients and networks to which it applies. The syntax is as follows:

```
LIMIT_BANDWIDTH = xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz
```

```
LIMIT_BANDWIDTH = xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz
```

Where:

- *xxx.xxx.xxx.xxx* is the beginning of the IP address range. (For example, 10.0.0.2.)
- *yyy.yyy.yyy.yyy* is the end of the IP address range. (For example, 10.0.0.49.)
- *zzz* is the bandwidth limitation in kilobytes per second. (For example, 200.) A value of 0 disables throttling for the individual client or the range of IP addresses covered by this entry.

You can add `LIMIT_BANDWIDTH` entries to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers.

MASTER_OF_MASTERS

Specifies the GDM server that can administer this server. Add this option to the configuration using the GDM graphical interface. (See the *Global Data Manager System Administrator's Guide*.)

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a NetBackup server that will be administered by a master of masters.

For example, assume that a master server named alpha is to be administered by a master of masters named omega. In this instance, you add the following entry to the `bp.conf` file on alpha:

```
MASTER_OF_MASTERS = omega
```

In addition, you add a `SERVER` entry for omega so alpha's `bp.conf` file has at least the following entries:

```
SERVER = alpha
ERVER = omega (the entry for omega must follow the alpha entry)
```

The `SERVER` entry allows omega to communicate with alpha. The `MASTER_OF_MASTERS` entry grants omega permission to administer alpha.

To complete the configuration, you add a `KNOWN_MASTER` entry for alpha to the `bp.conf` file on omega.

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.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or by entering a **Media ID Prefix** setting in the Media dialog under server host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

The prefix must be one to three alpha-numeric characters. NetBackup appends remaining numeric characters. The following is an example entry:

```
MEDIA_ID_PREFIX = FEB
```

NetBackup appends remaining numeric characters so the assigned media IDs become FEB000, FEB001, and so on.

The default media ID prefix is `A`: NetBackup assigns A00000, then A00001, and so on.

```
MEDIA_ID_PREFIX = A
```

MEDIA_UNMOUNT_DELAY

When `MEDIA_UNMOUNT_DELAY` is specified, the media unload is delayed for the specified number of seconds after the requested operation has completed. (Applies only to user operations.)

For example, assume the delay is 120 seconds:

```
MEDIA_UNMOUNT_DELAY = 120
```

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or enter a value for **Media Unmount Delay** in the Media host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

MEDIA_REQUEST_DELAY

Applies only to nonrobotic drives and specifies the number of seconds that NetBackup waits for a drive to become ready. Default: 0 seconds.

For example, assume the delay is 150 seconds:

```
MEDIA_REQUEST_DELAY = 150
```

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or enter a value for **Media Request Delay** in the Media host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

MEDIA_SERVER

The `bp.conf MEDIA_SERVER` entry is similar to the `bp.conf SERVER` entry.

A host specified as a `MEDIA_SERVER` is able to back up and restore clients. However, if the host is not specified as a `SERVER`, the host has limited administrative capabilities.

For example, assume the media server's name is oak:

```
MEDIA_SERVER = oak
```

(See "Restricting Administrative Privileges of Media Servers" on page 181.)

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or enter a media server name in the Media Servers list in the Servers host properties. (See Chapter 7 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

MPX_RESTORE_DELAY

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: 30 seconds.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers.

For example, assume the delay is 60 seconds:

```
MPX_RESTORE_DELAY = 60
```

MUST_USE_LOCAL_DRIVE

If the client is also a master server and this entry is present, backups for this client must occur on a local drive. If the client is not a master server, this entry has no effect.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers or check the **Must Use Local Drive** setting in the General Server host properties dialog. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

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 entry is not present, the job fails with a 219 status. By default, this option is not present and jobs fail with a status code 219 if the storage unit is not available.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers. The following is an example entry:

```
QUEUE_ON_ERROR
```

This entry 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. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

RANDOM_PORTS

Specifies whether NetBackup chooses port numbers randomly or sequentially when it requires one for communication with NetBackup on other computers.

- If `RANDOM_PORTS = YES` (default), NetBackup chooses port numbers randomly from those that are free in the allowed range. For example, if the range is from 1024 through 5000, it chooses randomly from the numbers in this range.
- If `RANDOM_PORTS = NO`, NetBackup chooses numbers sequentially, starting with highest number that is available in the allowed range. For example, if the range is from 1024 through 5000, NetBackup chooses 5000 (assuming it is free). If 5000 is being used, port 4999 is chosen.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers and clients.

By default, this option is not present and NetBackup uses the random method for selecting port numbers.

RE_READ_INTERVAL

Determines how often NetBackup checks storage units for available drives. Default: 300 seconds (5 minutes). (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

For example, assume the re-read interval is 350 seconds:

```
RE_READ_INTERVAL = 350
```

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or by entering a value for the **Re-read Interval** setting in the General Server host properties dialog. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

REQUIRED_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 and, by default, the operating system determines the one to use. To force NetBackup connections to be through a specific network interface, use this entry to specify the network host name of that interface.

In the following example, `host1` is the network host name of the interface:

```
REQUIRED_INTERFACE = host1
```

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a NetBackup client or server. Default: The entry does not exist and the operating system determines the interface to use.

Example 1 - Client with multiple network interfaces

Assume you have a NetBackup client with two network interfaces. One is for the regular network and one is for the backup network:

- The host name for the regular interface is fred
- 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 users on fred start a backup, restore, or list operation, the request ideally always goes out on the fred_nb interface and over the backup network. This assumes that fred and the network are set up for this. However, 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 alternate client restores for barney. This allows the server to accept the request, but leaves NetBackup traffic on the regular network. A better solution is to add the following entry to the `bp.conf` file on fred:

```
REQUIRED_INTERFACE = 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 you have a NetBackup server with two network interfaces. One is for the regular network and one is for the backup network:

- The host name for the regular interface is barney

- The host name for the backup interface is barney_nb

The `bp.conf` file on all NetBackup servers and clients has a `SERVER = barney_nb` entry.

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 for this. However, 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 a `SERVER = barney` entry to the `bp.conf` file on the client. The client now accepts requests from barney, but NetBackup traffic is still on the regular network.

A better solution is to add the following entry to the `bp.conf` file on barney:

```
REQUIRED_INTERFACE = barney_nb
```

Now, when barney connects to a client, the connection is always through the barney_nb interface and everything works as intended.

SERVER

For a NetBackup master server, the first `SERVER` entry in the `bp.conf` file must point to that master server itself. During installation, `SERVER` is automatically set to the name of the system where you are installing NetBackup server software.

Applies to NetBackup Enterprise Server:

If you configure NetBackup media servers for a master server, the `bp.conf` file on the master server must have a `SERVER` entry or `MEDIA_SERVER` entry for each. As previously mentioned, the first `SERVER` entry in the list designates the master server itself. The `SERVER` or `MEDIA_SERVER` entries should be added after the first, self-referencing entry.

A NetBackup master server can be backed up as a NetBackup client by servers belonging to another cluster, in which case the `bp.conf` file on the master server should have `SERVER` entries for those servers as well.

The following is an example `bp.conf` file on a master server:

```
SERVER = Master_server (this master server itself)
SERVER = NBU_server (master server of another cluster)
SERVER = Media_server_#1
MEDIA_SERVER = Media_server_#2
.
.
.
```

The first SERVER entry in the bp.conf files on all the media servers must point to the master server for those media servers. A media server can have only one master server. However, a media server can be backed up as a NetBackup client by servers belonging to another cluster, in which case the bp.conf on the media server should have SERVER entries for those servers as well.

The following is an example bp.conf file on a media server:

```
SERVER = Master_server (for this media server)
SERVER = NBU_server (master server of another cluster)
SERVER = Media_server_#1
MEDIA_SERVER = Media_server_#2
.
.
.
```

The SERVER entries must be the same on all servers in a master and media server cluster.

If you modify or add a SERVER entry in the bp.conf file on the master server, stop and restart both the NetBackup request daemon (bprd) and NetBackup database manager (bpdbm) so NetBackup will recognize the change.

The SERVER option *must* be present in the /usr/openv/netbackup/bp.conf file on all NetBackup UNIX servers and clients. It is the only required entry in these bp.conf files. This option is not used in $HOME/bp.conf files on a client.

SERVER_PORT_WINDOW

Specifies the range of nonreserved ports on which this computer accepts connections from NetBackup on other computers. Default range: 1024 through 5000. For information on client configuration, see "ALLOW_NON_RESERVED_PORTS" on page 137.

The following example permits ports from 4900 through 5000:

```
SERVER_PORT_WINDOW = 4900 5000
```

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup servers or enter values for **Server Port Window** in the Port Ranges host properties dialog. This option can also be useful on clients that are running the NetBackup-Java application server.

SERVER_RESERVED_PORT_WINDOW

Specifies the range of local reserved ports on which this computer accepts connections from NetBackup on other computers. Default range: 512 through 1023.

This setting applies when connecting to a client configured to accept only reserved ports. This entry is generally not useful on clients. For information on client configuration, see "ALLOW_NON_RESERVED_PORTS" on page 137.

The following example permits ports from 900 through 1023:

```
SERVER_RESERVED_PORT_WINDOW = 900 1023
```

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or enter values for **Server Reserved Port Window** in the Port Ranges host properties dialog.

SKIP_RESTORE_TO_SYMLINK_DIR

`SKIP_RESTORE_TO_SYMLINK_DIR` forces NetBackup to check all directories on a UNIX client into which files are being restored. If the file to be restored is under a symbolically linked directory, NetBackup does not restore the file.

For example, if the UNIX client requests a restore for `/home/user/.cshrc` and `/home/user` is a symbolic link, NetBackup will not restore `.cshrc`.

The addition of `SKIP_RESTORE_TO_SYMLINK_DIR` helps minimize potential security and data-loss problems if the restore is being performed with root permissions. Without `SKIP_RESTORE_TO_SYMLINK_DIR` indicated in the `bp.conf` file, NetBackup follows any symbolically linked directories and restores files to that location.

Note There will be a performance degradation to restore jobs using this option.

`SKIP_RESTORE_TO_SYMLINK_DIR` and `UNLINK_ON_OVERWRITE` do not affect each other if both are specified, with one exception:

If **Overwrite Existing Files** is selected with `SKIP_RESTORE_TO_SYMLINK_DIR` and `UNLINK_ON_OVERWRITE`, symbolic links that the restore job comes across will be unlinked before checking, and the files and directory will be restored.

For example, if `/home/user/` was backed up as a directory and, when restored, it is a symbolic link to a directory:

- With just `SKIP_RESTORE_TO_SYMLINK_DIR` set (and **Overwrite Existing Files** indicated), no files will be restored into the directory the symbolic link points to, and the symbolic link will remain.
- With both `UNLINK_ON_OVERWRITE` and `SKIP_RESTORE_TO_SYMLINK_DIR` (and **Overwrite Existing Files** indicated), the symbolic link directory will be unlinked, the original directory will be restored, and all files within the directory will also be restored.
- With neither set (and **Overwrite Existing Files** indicated), NetBackup will follow the symbolic link and restore all files into the directory the symbolic link points to.

SERVER_CONNECT_TIMEOUT

Applies to NetBackup Enterprise Server:

`SERVER_CONNECT_TIMEOUT` specifies the number of seconds that the master server waits before timing out when connecting to a media server. Default: Timeout period is 30 seconds.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers.

The following example permits a timeout of 60 seconds:

```
SERVER_CONNECT_TIMEOUT = 60
```

SPC_SERVER

SANPoint Control recommends that the SPC server be installed on a machine other than the master server, preferably on a machine by itself.

TIMEOUT_IN_QUEUE

Determines 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). (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

The following example permits a timeout of 30000 seconds:

```
TIMEOUT_IN_QUEUE = 30000
```

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers or by entering a value for **Timeout in Queue** in the Timeouts host properties dialog. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

UNLINK_ON_OVERWRITE

When a UNIX client indicates **Overwrite Existing Files** as a restore option, `UNLINK_ON_OVERWRITE` forces NetBackup to first check for the existence of a file to be restored, unlink the file if it exists, then restore the file. The file can be any normal file, symbolic link, hard link, or empty directory.

The addition of `UNLINK_ON_OVERWRITE` helps minimize potential security and data-loss problems from following existing symbolic links. It also guarantees that files will be restored exactly as they were backed up.

Note There will be a performance degradation to restore jobs using this option.

Without UNLINK_ON_OVERWRITE indicated in the bp.conf file (or set to NO), but overwrite is specified, NetBackup will unlink existing files or empty directories when restoring symbolic links, hard links, or special files (CHR, BLK, and FIFO). However, NetBackup will *not* unlink when restoring normal files or directories. This can be a problem with symbolic links because NetBackup will follow the symbolic link to create or replace file(s) pointed to by the symbolic link or in a directory pointed to by a symbolic link.

SKIP_RESTORE_TO_SYMLINK_DIR and UNLINK_ON_OVERWRITE do not affect each other if both are specified, with one exception:

If **Overwrite Existing Files** is selected with SKIP_RESTORE_TO_SYMLINK_DIR and UNLINK_ON_OVERWRITE, symbolic links that the restore job comes across will be unlinked before checking, and the files and directory will be restored.

For example, if /home/user/ was backed up as a directory and, when restored, it is a symbolic link to a directory:

- With just SKIP_RESTORE_TO_SYMLINK_DIR set (and **Overwrite Existing Files** indicated), no files will be restored into the directory the symbolic link points to, and the symbolic link will remain.
- With both UNLINK_ON_OVERWRITE and SKIP_RESTORE_TO_SYMLINK_DIR (and **Overwrite Existing Files** indicated), the symbolically linked directory will be unlinked, the original directory will be restored, and all files within the directory will also be restored.
- With neither set (and **Overwrite Existing Files** indicated), NetBackup will follow the symbolic link and restore all files into the directory the symbolic link points to.

USE_VXSS

The USE_VXSS entry specifies whether the local system uses VxSS.

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup master servers or by setting the **Use VERITAS Security Subsystem** in the Access Control properties under Master Server host properties. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

```
USE_VXSS = REQUIRED | PROHIBITED | AUTOMATIC
```

Where:

REQUIRED indicates that the local system always uses VxSS. Connections from systems not using VxSS are rejected.

PROHIBITED indicates that the local system never uses VxSS. Connections from systems using VxSS are rejected (default).

AUTOMATIC indicates that the local system negotiates with the remote system whether to use VxSS.

If USE_VXSS = AUTOMATIC is specified, VXSS_NETWORK entries can be used to require or prohibit VxSS connections with specified remote systems. See VXSS_NETWORK for an example using USE_VXSS = AUTOMATIC.

VERBOSE

Used for debugging purposes, the VERBOSE option controls the amount of information NetBackup includes in its logs. Default: Disabled.

```
VERBOSE [ 0 | 1 | 2 | 3 | 4 | 5 ]
```

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup servers or by setting the Master Server host property, **Global Logging Level**, on the Logging dialog. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

VXSS_NETWORK

The VXSS_NETWORK entry identifies whether a specific network or remote system must or must not use VxSS with the local system.

If a media server or client does not define a VxSS network, it will use the VxSS networks of its master server.

Use this option by adding it to the /usr/openv/netbackup/bp.conf file on NetBackup master servers or by setting the Master Server host property, **VxSS Networks List**, on the Access Control dialog. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

VXSS_NETWORK is relevant only if USE_VXSS is set to AUTOMATIC (USE_VXSS = AUTOMATIC). More than one VXSS_NETWORK entry can be specified.

```
VXSS_NETWORK = hostname | IP_address | .domain | network.
[AUTOMATIC | REQUIRED | PROHIBITED]
```

Possible values:

- hostname
  The host name of the remote system.
- IP_address
  The IP address of the remote system.
- .domain
  A dot followed by the Internet domain name of the remote systems.

- `network.`
  The network of the remote systems followed by a dot.

The optional second value can be one of the following keywords:

- AUTOMATIC
- REQUIRED
- PROHIBITED

Note If a system is specified by more than one VXSS_NETWORK entry, the first occurance takes precedence.

Example

```
USE_VXSS = AUTOMATIC
VXSS_NETWORK = fred.mycompany.com
VXSS_NETWORK = 10.0.0.37 REQUIRED
VXSS_NETWORK = 10.0.0. PROHIBITED
VXSS_NETWORK = .theircompany.com
VXSS_NETWORK = wilma.theircompany.com PROHIBITED
VXSS_NETWORK = barney.mycompany.com PROHIBITED
```

In the example, VxSS is required for connections between the local system and the system with host `fred.mycompany.com`.

VxSS is required for connections between the local system and the system with IP address `10.0.0.37`.

VxSS is prohibited for connections between the local system and systems in the `10.0.0` network except for `10.0.0.37`.

VxSS is required for connections between the local system and systems within the `theircompany.com` Internet domain.

VxSS is required for connections between the local system and the system with host name `wilma.theircompany.com` despite the `PROHIBITED` entry for `wilma.theircompany.com`. The REQUIRED entry for `.theircompany.com` takes precedence.

VxSS is prohibited for connections between the local system and the system with host name `barney.mycompany.com`

WAIT_IN_QUEUE

Causes active jobs to enter the requeued state if the required storage unit becomes unavailable (for example, if a drive goes down). The jobs will 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. Default: This option is not present and the job is not requeued. (See Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers.

The following is an example entry:

```
WAIT_IN_QUEUE
```

bp.conf Options for UNIX Clients

On NetBackup UNIX clients, the main `bp.conf` file is located in the following pathname:

```
/usr/openv/netbackup/bp.conf
```

As installed, NetBackup uses internal software defaults for all options in the `bp.conf` file, except `SERVER`. During installation, NetBackup sets the `SERVER` option to the name of the master server where the software is installed.

Note The `SERVER` option must be in the `/usr/openv/netbackup/bp.conf` file on all NetBackup UNIX clients. It is also the only required entry in this file.

If a single UNIX system is running as both a client and a server, both the server and client options are in the `/usr/openv/netbackup/bp.conf` file.

Each nonroot user on a UNIX client can have a personal `bp.conf` file in their home directory as follows:

```
$HOME/bp.conf
```

The options in personal `bp.conf` files apply only to user operations. During a user operation, NetBackup checks the `$HOME/bp.conf` file before `/usr/openv/netbackup/bp.conf`. Root users do not have personal `bp.conf` files. NetBackup uses the `/usr/openv/netbackup/bp.conf` file for root users.

The following topics describe the options that you can specify in the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a NetBackup UNIX client.

Note PC clients provide similar options that you can change either through the client-user interface or in a configuration file, depending on the client. For instructions, see the *NetBackup User's Guide* for the client.

ALLOW_NON_RESERVED_PORTS

Specifies that the NetBackup client daemon (`bpcd`) can accept remote connections from non-privileged ports (port numbers 1024 or greater). If this entry is not present, then `bpcd` requires remote connections to come from privileged ports (port numbers less than 1024). This option can be useful when NetBackup clients and servers are on opposite sides of a firewall.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

In addition to adding `ALLOW_NON_RESERVED_PORTS` to the client, execute the following commands as root on the master server.

```
cd /usr/openv/netbackup/bin/admincmd
./bpclient -client client_name -add -connect_nr_port 1
```

Where *`client_name`* is the name of the client where you added the `ALLOW_NON_RESERVED_PORTS` option. These commands instruct the master server to use nonprivileged ports.

AUTHENTICATION_DOMAIN

The `AUTHENTICATION_DOMAIN` entry defines a set of VxSS authentication principals. A client that uses VxSS must have at least one `AUTHENTICATION_DOMAIN` entry, and more than one can be specified. (See "AUTHENTICATION_DOMAIN" on page 137 for more information.)

If a media server or client does not define an authentication domain, it will use the authentication domains of its master server.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on a UNIX client or by setting the **Authentication Domains** in the Access Control properties under client host properties. (See "Authentication Domain Tab within Access Control Properties Dialog" on page 307 in *NetBackup System Administrator's Guide for UNIX, Volume I*.)

BPARCHIVE_POLICY

Specifies the name of the policy to use for user archives. Default: `BPARCHIVE_POLICY` is not in any `bp.conf` file and NetBackup uses the first policy that it finds that has the client and a user archive schedule.

For example:

```
BPARCHIVE_POLICY = arch_1
```

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence if it exists.

BPARCHIVE_SCHED

Specifies the name of the schedule for user archives. Default: `BPARCHIVE_SCHED` is not in any `bp.conf` file and NetBackup uses the first archive schedule in the first policy that it finds that has this client.

For example

```
BPARCHIVE_SCHED = user_arch1
```

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence if it exists.

BPBACKUP_POLICY

Specifies the name of the policy name to use for user backups. Default: `BPBACKUP_POLICY`, is not in any `bp.conf` file and NetBackup uses the first policy it finds that has both the client and a user backup schedule.

For example,

```
BPBACKUP_POLICY = userback_1
```

You can add this option to the `/usr/openv/netbackup/bp.conf` and (or) `$HOME/bp.conf` files on a UNIX client.

The value in user's `$HOME/bp.conf` file takes precedence if it exists.

BPBACKUP_SCHED

Specifies the name of the schedule to use for user backups. Default: `BPBACKUP_SCHED` is not in any `bp.conf` file and NetBackup uses the first policy it finds that has both the client and a user backup schedule.

For example:

BPBACKUP_SCHED = user_back1

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence if it exists.

BUSY_FILE_ACTION

Directs the action that NetBackup performs on busy files when busy-file processing is enabled.

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence if it exists.

There can be multiple entries of the following form:

BUSY_FILE_ACTION = *`filename_template action_template`*

Where

- *`filename_template`* is the absolute pathname and file name of the busy file. The shell language metacharacters `*, ?, [], [ - ]` can be used for pattern matching of filenames or parts of filenames.
- *`action_template`* is one of the following:

  `MAIL | mail`

  Directs NetBackup to E-mail a busy file notification message to the user specified by the `BUSY_FILE_NOTIFY_USER` option.

  `REPEAT | repeat [repeat_count]`

  Directs NetBackup to retry the backup on the specified busy file. A repeat count can be specified to control the number of backup attempts. The default repeat count is 1.

  `IGNORE | ignore`

  Directs NetBackup to exclude the busy file from busy file processing.

BUSY_FILE_DIRECTORY

The `BUSY_FILE_DIRECTORY` option specifies the path to the busy-files working directory when busy-file processing is enabled. Default: `BUSY_FILE_DIRECTORY` is not in any `bp.conf` file and NetBackup creates the `busy_files` directory in `/usr/openv/netbackup`.

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence, if it exists.

BUSY_FILE_NOTIFY_USER

The `BUSY_FILE_NOTIFY_USER` option specifies the recipient of the busy file notification message when `BUSY_FILE_ACTION` is set to `MAIL` or `mail`. Default: `BUSY_FILE_NOTIFY_USER` is not in any `bp.conf` file and the E-mail recipient is root.

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence, if it exists.

BUSY_FILE_PROCESSING

The `BUSY_FILE_PROCESSING` option lets the user control the actions that NetBackup performs when it determines that a file is changing while it is being backed up. Default: `BUSY_FILE_PROCESSING` option is not in `bp.conf` and busy-file processing does not occur. (See "Busy-File Processing (UNIX Clients Only)" on page 122 for instructions on setting this option.)

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

CLIENT_NAME

Specifies the name of the client as it is known to NetBackup. There can be one `CLIENT_NAME` entry and it must match the name used in the policy that is backing up the client. The only exception is for an alternate client restore, where the name must match that of the client whose files are being restored. (See "Allowing Redirected Restores" on page 431.) The client installation procedures automatically set `CLIENT_NAME` to the value specified on the `ftp_to_client` or `install_client` command in the installation scripts.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

It can also be added to a `$HOME/bp.conf` file on a UNIX client but this is normally done only for alternate-client restores.

If the value is not in any `bp.conf` file, NetBackup uses the value returned by the `gethostname()` library function.

CLIENT_PORT_WINDOW

Specifies the range of nonreserved ports on this computer that are used for connecting to NetBackup on other computers. (See "CLIENT_PORT_WINDOW" on page 146.)

CLIENT_READ_TIMEOUT

Specifies the number of seconds for the client-read timeout on a server or a database agent. (See "CLIENT_READ_TIMEOUT" on page 147.)

CLIENT_RESERVED_PORT_WINDOW

Specifies the range of reserved ports on this computer that are used for connecting to NetBackup on other computers. (See "CLIENT_RESERVED_PORT_WINDOW" on page 147.)

COMPRESS_SUFFIX

Note This option has a reasonable default and has to be changed only if problems are encountered.

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. Default, `COMPRESS_SUFFIX` is not in the `bp.conf` file. (See "Compression" on page 90 for more information on compressing files.)

You cannot use wildcards when specifying these extensions. For example, you can specify the following:

.A1

You cannot specify either of the following:

.A* or .A[1-9]

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

CRYPT_CIPHER

Note `CRYPT_CIPHER` applies only to clients that have the NetBackup Encryption option installed. For information on NetBackup Encryption, see the *NetBackup Encryption System Administrator's Guide*.

The CRYPT_CIPHER entry on the client takes one the following values:

- `AES-128-CFB` (used when no method is specified; default)
- `AES-256-CFB`
- `BF-CFB`
- `DES-EDE-CFB`

This client property can also be configured on the Encryption host properties dialog for each client. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

CRYPT_KIND

Note `CRYPT_KIND` applies only to 5.1 clients that have the NetBackup Encryption option installed. For information on NetBackup Encryption, see the *NetBackup Encryption System Administrator's Guide*.

The CRYPT_KIND entry on the client determines whether the standard encryption or legacy encryption will be used in the backup. Normally, CRYPT_KIND is set automatically. The values that can be entered are the following:

`NONE` = No encryption is used on the client (default)

`LEGACY` = Use on NetBackup clients running versions previous to 5.1. Legacy pertains to 40-bit and 56-bit Data Encryption Standard (DES).

`STANDARD` = Use on NetBackup 5.1 clients in order to use the 128-bit and 256-bit options of NetBackup Encryption.

This client property can also be configured on the Encryption host properties dialog for each client. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

CRYPT_OPTION

Note `CRYPT_OPTION` applies only to clients that have the NetBackup Encryption option installed. For information on NetBackup Encryption, see the *NetBackup Encryption System Administrator's Guide*.

`CRYPT_OPTION` specifies the encryption options on NetBackup clients. NetBackup creates this entry automatically in the `/usr/openv/netbackup/bp.conf` file on a UNIX client when you run the `bpinst_crypt` command on the NetBackup master server.

Do not alter the entry or create this file manually unless it has been accidentally deleted. The allowable values follow:

`DENIED|denied`

Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error. This option is the default for a client that has not been configured for encryption.

`ALLOWED|allowed`

Specifies that the client allows either encrypted or unencrypted backups.

`REQUIRED|required`

Specifies that the client requires encrypted backups. If this value is specified and the server requests an unencrypted backup, it is considered an error.

This client property can also be configured on the Encryption host properties dialog for each client. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

CRYPT_STRENGTH

Note `CRYPT_STRENGTH` applies only to clients that have the NetBackup Encryption option installed. See the *NetBackup Encryption System Administrator's Guide*.

Specifies the encryption strength on NetBackup clients. NetBackup creates this entry automatically in the `/usr/openv/netbackup/bp.conf` file on a UNIX client when you run the `bpinst_crypt` command on the NetBackup master server.

Do not alter the entry or create it manually unless it has been accidentally deleted. The possible values follow:

`DES_40|des_40`

Specifies 40-bit DES encryption. This is the default value for a client that has not been configured for encryption.

`DES_56|des_56`

Specifies 56-bit DES encryption.

This client property can also be configured on the Encryption host properties dialog for each client. (Configuration options are described in Chapter 7 of the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

CRYPT_LIBPATH

Note `CRYPT_LIBPATH` applies only to clients that have the NetBackup Encryption option installed. See the *NetBackup Encryption System Administrator's Guide*.

Specifies the directory that contains the encryption libraries for NetBackup clients. NetBackup creates this entry automatically in the `/usr/openv/netbackup/bp.conf` file on a UNIX client when you run the `bpinst_crypt` command on the NetBackup master server.

Do not alter the entry or create it manually unless it has been accidentally deleted.

- The following is the default value on UNIX systems:

  `/usr/openv/lib/`

- The following is the default value on Windows systems:

  install_path\bin\

  Where *install_path* is the directory where NetBackup is installed and by default is C:\Program Files\VERITAS.

CRYPT_KEYFILE

Note CRYPT_KEYFILE applies only to clients that have the NetBackup Encryption option installed. See the *NetBackup Encryption System Administrator's Guide*.

Specifies the file that contains the encryption keys on NetBackup clients. NetBackup creates this entry automatically in the /usr/openv/netbackup/bp.conf file on a UNIX client when you run the bpinst_crypt command on the NetBackup master server.

Do not alter the entry or create it manually unless it has been accidentally deleted. The default values follow:

- On UNIX systems: /usr/openv/netbackup/keyfile
- On Windows systems: *install_path*\bin\keyfile.dat

  Where *install_path* is the directory where NetBackup is installed and by default is C:\Program Files\VERITAS.

DISALLOW_SERVER_FILE_WRITES

Prevents the NetBackup server from creating files on the NetBackup client. For example, this prevents server-directed restores or server-directed updates of the bp.conf file on the client.

You can add this option to the /usr/openv/netbackup/bp.conf file on a UNIX client. By default, server writes are allowed.

DO_NOT_RESET_FILE_ACCESS_TIME

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.

Specifies that if a file is backed up, its access time (atime) will show the time of the backup. Default: NetBackup preserves the access time by resetting it to the value it had before the backup.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

GENERATE_ENGLISH_LOGS

Enables the generation of an English error log, and English trace logs for the `bparchive`, `bpbackup`, `bpduplicate`, `bpimport`, and `bprestore` commands. This option is useful to support personnel assisting in distributed environments where differing locales result in logs with various languages.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup servers and clients.

IGNORE_XATTR

By default, extended attribute files on Solaris 9 clients and named data streams on VxFS 4.0 clients are backed up. To disable the backing up of extended attributes and named data streams, add IGNORE_XATTR to the `/usr/openv/netbackup/bp.conf` file on the Solaris 9 or VxFS 4.0 client. (IGNORE_XATTR was formerly IGNORE_XATTR_SOLARIS.)

The presence of this entry in the `bp.conf` file means that NetBackup will not check for the existence of extended attributes or named data streams. (See “Backup and Restore of Extended Attribute Files and Named Data Streams” on page 119.)

INFORMIX_HOME

Specifies the path to the Informix home directory and is required when the client is using NetBackup for Informix.

You must add this option to the `/usr/openv/netbackup/bp.conf` file on UNIX clients that are running NetBackup for Informix.

INITIAL_BROWSE_SEARCH_LIMIT

Reduces the default number of days back that NetBackup searches for files to restore.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on NetBackup master servers and clients. (See “INITIAL_BROWSE_SEARCH_LIMIT” on page 153.)

KEEP_DATABASE_COMM_FILE

Causes NetBackup to keep database agent logs for seven days. Default: NetBackup keeps database agent logs for only one day.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX database agent (for example, a client that is running NetBackup for Informix).

KEEP_LOGS_DAYS

Specifies the number of days to keep job and progress logs generated by the NetBackup Java program, Backup, Archive, and Restore. NetBackup writes these files in the `usr/openv/netbackup/logs/user_ops/`*`username`*`/jobs` and `/usr/openv/netbackup/logs/user_ops/`*`username`*`/logs` directories. There is a directory for each user that uses the Backup, Archive, and Restore program. Default: Three days.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

LIST_FILES_TIMEOUT

Specifies the number of minutes to wait for a response from the NetBackup server when listing files by using the client-user interface or `bplist`. If this time is exceeded, the user receives a `socket read failed` error even if the server is still processing the user's request. Default: `LIST_FILES_TIMEOUT` is not in any `bp.conf` file and NetBackup uses a value of 30 minutes.

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

The value in the user's `$HOME/bp.conf` file takes precedence if it exists.

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 (see `chmod(1)`). If `LOCKED_FILE_ACTION` is specified and has a value of `SKIP` (the only legal value), NetBackup skips files that currently have mandatory locking set by another process and logs a message to this effect.

You can add this option to the `/usr/openv/netbackup/bp.conf` files on a UNIX client. Default: NetBackup waits for files to become unlocked.

MEDIA_SERVER

Specifies that the listed machine is a media server *only*. Machines listed as media servers can back up and restore clients, but have limited administrative privileges.

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. The percentage of machine resources used is also greater. 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.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client. Default: NetBackup assumes a value of one megabyte.

NFS_ACCESS_TIMEOUT

Specifies the number of seconds that the backup process waits when processing an NFS mount table before considering an NFS file system unavailable.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client. Default: Timeout period is five seconds.

RANDOM_PORTS

Specifies whether NetBackup chooses port numbers randomly or sequentially when it requires one for communication with NetBackup on other computers. (See "RANDOM_PORTS" on page 165.)

RESTORE_RETRIES

Note This option has a reasonable default and will have to be changed only if problems are encountered.

Specifies the number of times to retry a restore after a failure. Default: There are no retries.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

REQUIRED_INTERFACE

Specifies the network interface that NetBackup uses when connecting to another NetBackup client or server. (See "REQUIRED_INTERFACE" on page 166.)

SERVER_PORT_WINDOW

Specifies the range of nonreserved ports on which this computer accepts connections from NetBackup on other computers.

SERVER

Applies to NetBackup Enterprise Server only.

Defines the list of NetBackup master servers and media servers that can access the NetBackup client. During client installation, the `SERVER` is set to the name of the primary master server for this client. Other `SERVER` entries can be added for any other master servers for this client, and for media servers for this client. (Media servers for this NetBackup client can also be added using the `MEDIA_SERVER` option.)

If you configure media servers, you must have a `SERVER` or `MEDIA_SERVER` entry for each media server in the NetBackup client's `bp.conf` file.

The following is an example `bp.conf` file on a client:

```
SERVER = Master_server (default master server)
SERVER = NBU_server (other master server)
SERVER = Media_server_#1
MEDIA_SERVER = Media_server_#2
.
.
.
```

The first `SERVER` entry denotes the master server to which the client would connect by default for any requests (for example, backing up, listing or restoring files). The `SERVER` option must be present in the `/usr/openv/netbackup/bp.conf` file on all UNIX clients. It is also the only required entry in the `bp.conf` file for clients. This option is not used in a `$HOME/bp.conf` file. On NetBackup UNIX servers, the `SERVER` entry applies to both client and the server.

SYBASE_HOME

Specifies the path to the Sybase home directory and is required when using NetBackup for Sybase to back up Sybase databases. Default: `SYBASE_HOME` is not in the `bp.conf` file.

You must add this option to the `/usr/openv/netbackup/bp.conf` file on a NetBackup for Sybase client.

USE_CTIME_FOR_INCREMENTALS

Note If you specify `USE_CTIME_FOR_INCREMENTALS`, you must also specify `DO_NOT_RESET_FILE_ACCESS_TIME`.

DO NOT use these options 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.

Causes NetBackup client software to use both modification time (mtime) and inode change time (ctime) during incremental backups to determine if a file has changed.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client. Default: NetBackup uses only mtime.

USE_VXSS

The `USE_VXSS` entry specifies whether the local system uses VxSS.

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on the client or by setting the **Use VERITAS Security Subsystem** in the Access Control properties under client host properties. (See "VERITAS Security Services (VxSS)" on page 304 in *NetBackup System Administrator's Guide for UNIX, Volume I*.)

USEMAIL

Specifies the E-mail address where NetBackup sends status on the outcome of operations for a UNIX client. Default: `USEMAIL` is not present in any `bp.conf` file and no E-mail is sent.

Note You can use multiple addresses or an E-mail alias as long as there are no blanks or white space between them.

You can add this option to the `/usr/openv/netbackup/bp.conf` and `$HOME/bp.conf` files on a UNIX client.

- If the `/usr/openv/netbackup/bp.conf` file specifies an address, NetBackup sends automatic backup and manual backup status to that address.
- If the `$HOME/bp.conf` file specifies an address, NetBackup also sends status on the success or failure of user operations to that address.

VERBOSE

The VERBOSE entry causes NetBackup to include more information in its logs. Default: Disabled.

You can add this option to the `/usr/openv/netbackup/bp.conf` file on a UNIX client.

VXSS_NETWORK

The `VXSS_NETWORK` entry identifies whether a specific network or remote system must or must not use VxSS with the local system.

If a media server or client does not define a VxSS network, it will use the VxSS networks of its master server. (See "VXSS_NETWORK" on page 164 for more information.)

Use this option by adding it to the `/usr/openv/netbackup/bp.conf` file on a UNIX client or by setting the **VxSS Networks List** in the Access Control properties under client host properties. (See "VxSS Networks List" on page 305 in *NetBackup System Administrator's Guide for UNIX, Volume I*.)

UNIX Client Examples

Example /usr/openv/netbackup/bp.conf File

```
SERVER = hare
CLIENT_NAME = freddie
USEMAIL = abc@bdev.com
COMPRESS_SUFFIX = .Addrs
COMPRESS_SUFFIX = .Counts
VERBOSE
RESTORE_RETRIES = 1
BPBACKUP_POLICY = U1userdir
BPBACKUP_SCHED = userbackups
BPARCHIVE_POLICY = U1userdir
BPARCHIVE_SCHED = userarchives
LOCKED_FILE_ACTION = SKIP
```

Example $HOME/bp.conf File

Nonroot users on UNIX clients can have a personal `bp.conf` file in their home directory. A personal `bp.conf` file can have any of the following options

Note A root user cannot have a personal `bp.conf` file. For root users, NetBackup uses the `/usr/openv/netbackup/bp.conf` file.

```
USEMAIL = mars@bdev.com
BPBACKUP_POLICY = user1
BPBACKUP_SCHED = userback
BPARCHIVE_POLICY = user1
BPARCHIVE_SCHED = userarch
LIST_FILES_TIMEOUT = 10
CLIENT_NAME
```

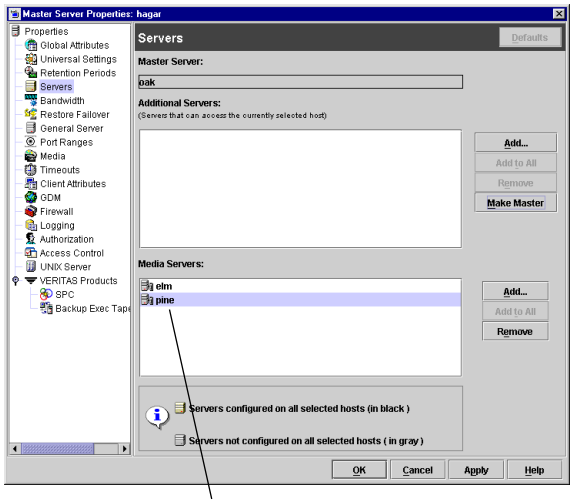
Specify `CLIENT_NAME` only when doing restores to an alternate client. (See "Redirected Restore Examples" on page 434.)

Restricting Administrative Privileges of Media Servers

In the **Servers** host properties, the servers included in the **Media Servers** list are media servers only. (**Host Properties** > **Master Server** *or* **Media Servers** > **Servers**.)

Machines listed as media servers can back up and restore clients, but have limited administrative privileges.

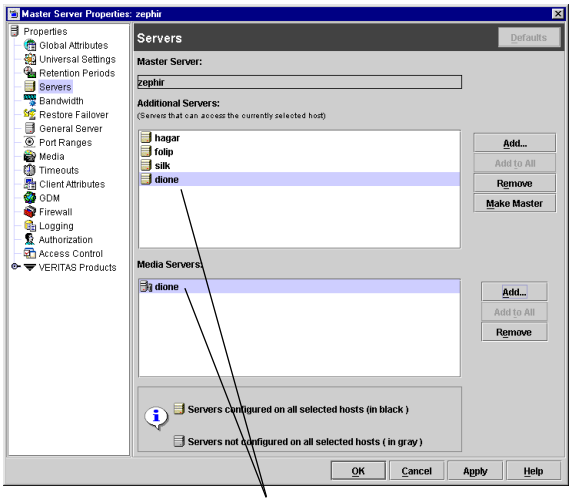
Suppose you have a configuration consisting of master server oak and two media servers—elm and pine. Set up oak as the master server and elm and pine as media servers.



Administrative scope of media servers is limited

If a machine is defined as *both* a master server and a media server, the master server entry takes precedence.

A consequence of listing a server as both a master and media server is that a system administrator on a media server would also be a NetBackup administrator on other master servers.



A machine listed as both an additional server and a media server has full administrative privileges

Using bpadm 4

The NetBackup `bpadm` administrator utility is a character-based, menu-driven interface that you can use at any terminal (or terminal emulation window) for which you have a `termcap` or `terminfo` definition.

This chapter describes procedures for configuring and managing NetBackup using `bpadm`. The areas covered are as follows:

- "Starting bpadm" on page 184
- "Defining and Managing Storage Units" on page 185
- "Defining and Managing Storage Unit Groups" on page 192
- "Defining and Managing Policies" on page 194
- "Defining NetBackup Global Attributes" on page 210
- "Installing NetBackup Software on All Trusting Client Hosts" on page 214
- "Displaying Reports" on page 215
- "Managing bprd (NetBackup Request Daemon)" on page 218
- "Redefining Retention Levels" on page 219
- "Performing Manual Backups" on page 221
- "Backing Up the NetBackup Databases (Catalogs)" on page 222

Starting bpadm

Note Use bpadm only on the master server and ensure that no other instances of bpadm or the NetBackup Administration Console are active when you are modifying the configuration. If you attempt to modify the configuration by using more than one instance or a combination of these utilities, the results will be unpredictable.

Start the bpadm program by running the following command as a root user:

```
/usr/openv/netbackup/bin/bpadm
```

The main menu appears on your screen.

```
NetBackup Server: bunny

NetBackup Administration
------------------------
s)  Storage Unit Management...
t)  Storage Unit Group Management...
p)  Policy Management...
g)  Global Configuration...
r)  Reports...
m)  Manual Backups...
x)  Special Actions...
u)  User Backup/Restore...
e)  Media Management...
h)  Help
q)  Quit

   ENTER CHOICE:
```

The prompts that bpadm provides are generally self-explanatory, and all menus have online help available. If you need more information, the topics in this chapter provide detailed instructions on common operations. You can abort many operations by pressing the escape (**Esc**) key.

Defining and Managing Storage Units

The *NetBackup Media Manager System Administrator's Guide for UNIX* explains how to define storage devices and media using Media Manager. The procedures in this section explain how to define and manage them within NetBackup. The `Storage Unit Management` menu has options for defining and managing storage units. To display this menu, press **s** (`Storage Unit Management`) while viewing the `bpadm` main menu.

```
Storage Unit Label: <ALL>
Storage Unit Host: <ALL>
Storage Unit Type: <ALL>
Output Destination: SCREEN

Storage Unit Management
------------------------
a) Add Storage Unit...
m) Modify Storage Unit...
d) Delete Storage Unit

b) Browse Storage Units Forward
r) Browse Storage Units Reverse
e) Enter Storage Unit
l) List/Display Storage Units
o) Output Destination  (SCREEN or FILE)
h) Help
q) Quit Menu

   ENTER CHOICE:
```

Adding a Removable or Robotic Storage Unit

To add a storage unit, press **a** (`Add Storage Unit`) while viewing the `Storage Unit Management` menu and follow the prompts.

Before adding a Removable or Robotic type storage unit, you must configure the related devices and media within Media Manager. When that configuration is complete, you can add a storage unit so that NetBackup can direct data to those devices and media.

The example below shows the dialog that occurs when adding a DLT tape stacker. User responses are in bold.

```
Adding Storage Unit (<ESC> to abort)
  -----------------------------------
  Enter storage unit label: TSD_1 <Return>
  Enter host name:  (bunny) <Return>

  Storage Unit Type
  -----------------
   1) Disk
   2) Media Manager
   3) Disk Staging
Enter Choice [1-3]: 2 <Return>

  Robot Type Selections
  ---------------------
   1) NONE - Not Robotic
   2) ACS - Automated Cartridge System
   3) LMF - Library Management Facility
   4) ODL - Optical Disk Library
   5) RSM - Removable Storage Manager
   6) TL4 - Tape Library 4MM
   7) TL8 - Tape Library 8MM
   8) TLD - Tape Library DLT
   9) TLH - Tape Library Half-inch
   10) TLM - Tape Library Multimedia
   11) TS8 - Tape Stacker 8MM
   12) TSD - Tape Stacker DLT
   13) TSH - Tape Stacker Half-inch
  Enter Choice [1-13]: 12 <Return>

  Enter this device's robot number: 2 <Return>
  Density Selections
  ------------------
   1) dlt - DLT Cartridge
   2) dlt2 - DLT Cartridge 2
   3) dlt3 - DLT Cartridge 3
  Enter Choice [1-3]: 1 <Return>

  Determine the number of drives you wish to use for
    backups and archives.  The number you use must be
    less than or equal to the number of drives installed.
  Enter number of drives: 1 <Return>

  Use this storage unit only if required
  by a policy or schedule? (y/n) (n):<Return>
```

```
What maximum multiplexing factor should be used per drive?
  (A value of 1 indicates to not do multiplexing)
Enter value [1-32]:  (1) <Return>

Maximum fragment size for backup images is configurable.
  Allowable values are in the range of 50 MB to 1048576 MB (1024GB).
Enter maximum fragment size (in MB):  (1048576) <Return>

Add storage unit? (y/n): y

Adding storage unit ...
```

▼ To add a removable or robotic storage unit

1. Provide a unique label for the storage unit (no spaces are allowed in the label). This is the label you use to associate the unit with a policy or schedule. Select a label that is descriptive of the type of storage you are defining.

2. Provide the name of the host that is controlling the storage unit. This must correspond to the host to which the drives attach. The default host appears in parentheses. Either press **Return** to accept the default or specify a new name.

3. Provide the storage unit type. Press **2** for Media Manager. This brings up a list of choices for robot types.

4. Specify the storage unit's robot type.

   - Pressing **1** (`NONE - Not Robotic`) brings up the list of density choices.

     Specify the density according to the value configured in Media Manager, then specify the number of drives of this density that you want to use. All nonrobotic drives of a given density must belong to the same storage unit. Specifying more than one drive can make it possible for the storage unit to handle more than one job at a time.

   - Selecting a robot brings up a prompt for the device's robot number. This number must match the number you configured in Media Manager.

     If you are prompted for density, set it according to the configuration in Media Manager. Then, specify how many of the robot's drives that you want to use for NetBackup operations. This number must be less than or equal to the number of drives that are installed in the robot.

5. Decide whether you want to use the storage unit only when a policy or schedule specifies it, or to make it available for any schedule.

   - **y** reserves the unit for use only by policies or schedules that specify it.

- **n** makes the storage unit available for any policy or schedule. This is the default.

6. Specify the maximum image multiplexing (MPX) factor to use.

   Image multiplexing sends concurrent, multiple backups from one or several clients to a single disk storage unit and multiplexes the images onto the media.

   Provide a value from 1 to 32. A value of 1 (the default) disables multiplexing by allowing only one backup job at a time to go to any given drive.

7. Provide a value, in megabytes, for the maximum fragment size.

   This is the largest size fragment that you want NetBackup to create when fragmenting images, and can range from 50 MB to 1048576 MB (1024GB) for a Media Manager storage unit

   Press **y** to confirm the addition or **n** to cancel.

8. Review the addition by pressing **l** (`List/Display Storage Units`). To change attributes, press **m** (`Modify Storage Unit`), or else delete the storage unit and add it again.

   If you are configuring NetBackup for the first time and are satisfied with your storage unit configuration, go to "Adding a Policy" on page 195.

Adding a Disk Type Storage Unit

To add a disk type storage unit, press **a** (`Add Storage Unit`) while viewing the `Storage Unit Management` menu, and follow the prompts, as in the following example.

```
Adding Storage Unit (<ESC> to abort)
  -----------------------------------
  Enter storage unit label: unixdisk_1 <Return>
  Enter host name:  (bunny) <Return>

  Storage Unit Type
  -----------------
   1) Disk
   2) Media Manager
   3) Disk Staging
  Enter Choice [1-3]: 1 <Return>

  full path to image directory: /bpimages <Return>
  Enter maximum number of concurrent jobs:  (1) 2 <Return>

  Use this storage unit only if required
    by a policy or schedule? (y/n) (y): <Return>

 What maximum multiplexing factor should be used?
  (A value of 1 indicates to not do multiplexing)
  Enter value [1-32]:  (1) <Return>

 Maximum fragment size for backup images is configurable.
   Allowable values are in the range of 20 MB to 2000 MB (2GB).
  Enter maximum fragment size (in MB):  (2000) <Return>

  Add storage unit? (y/n): y
```

▼ To add a disk type storage unit

1. Provide a unique label for the storage unit (no spaces are allowed in the label). This is the label you use to associate the unit with a policy or schedule. Specify a label that is descriptive of the type of storage you are defining. The label `unixdisk_1` in the example is used for a storage unit on UNIX disk.

2. Provide the name of the server that is controlling the disk. This is the network name of the server as returned by the UNIX `hostname` command.

3. Provide the storage unit type. Press **1** for Disk and specify the pathname.

4. Specify the directory path for the backup and archive images. This can be anywhere on your disk that you have room.

5. Specify the number of concurrent jobs that you are going to allow. This number depends on your server's ability to comfortably execute multiple backup processes.

6. Decide whether you want to use the storage unit only when a policy or schedule specifies it, or to make it available for any policy or schedule.

   - Press **y** to reserve the unit for use only by policies or schedules that specify it. This is the default.
   - Press **n** to make the storage unit available to any policy or schedule.

7. Specify the maximum image multiplexing (MPX) factor to use.

   Image multiplexing sends concurrent, multiple backups from one or several clients to a single drive and multiplexes the images onto the media.

   Provide a value from 1 to 32. A value of 1 (default) disables multiplexing by allowing only one backup job at a time to go to any given drive.

8. Provide a value, in megabytes, for the maximum fragment size.

   This is the largest size fragment that you want NetBackup to create when fragmenting images, and can range from 20 to 2000 (default) for a disk type storage unit.

9. Press **y** to confirm the addition or **n** to cancel. This returns you to the `Storage Unit Management` menu.

10. To review the addition, press **l** (`List/Display Storage Units`). To change attributes, press **m** (`Modify Storage Unit`), or else delete the storage unit and add it again.

    If you are configuring NetBackup for the first time and are satisfied with your storage unit configuration, go to "Adding a Policy" on page 195.

Displaying and Changing Storage Unit Configurations

The `Storage Unit Management` menu has options for viewing the attributes of currently configured storage units or writing the list to a file. It also has options for modifying the configuration by either deleting storage units or changing their attributes.

▼ To use the Storage Unit Management menu

1. Once in a storage management menu, press **b** (`Browse Storage Units Forward`) until the `Label` line at the top of the screen shows the name you want. The next two lines show the host to which the storage unit connects and the type of storage unit.

2. Select the desired option:

   - To modify, press **m** (`Modify Storage Unit`) and follow the prompts (existing values are in parentheses).
   - To delete a storage unit, press **d** (`Delete Storage Unit`). At the prompt, check to ensure that you are deleting the correct storage unit and press **y** if you want to delete it. Deleting a storage unit from the NetBackup configuration does not prevent you from restoring files that are stored on that unit. A restore requires only that the same type of storage unit is available (in Media Manager for a removable or robotic type storage unit).
   - To view the attributes for the storage unit, press **l** (`List/Display Storage Units`). Use the controls at the bottom of the screen to move within the list.
   - To direct the list of attributes to a file, press **o** (`Output Destination`) and specify the desired file path at the prompt. Press **l** to write the list to the file.

Defining and Managing Storage Unit Groups

A *storage unit group* is a list of storage units, ordered by priority. Use the storage unit group to define sets of storage units and to assign priorities to one or more storage units. The `Storage Unit Group Management` menu has options for defining and managing storage unit groups. To display this menu, press **t** while viewing the `bpadm` main menu.

```
Storage Unit Group Label: <ALL>
Output Destination: SCREEN

Storage Unit Group Management
------------------------
a) Add Storage Unit Group...
m) Modify Storage Unit Group...
d) Delete Storage Unit Group

b) Browse Storage Unit Groups Forward
r) Browse Storage Unit Groups Reverse
e) Enter Storage Unit Group
l) List/Display Storage Unit Groups
o) Output Destination  (SCREEN or FILE)
h) Help
q) Quit Menu

   ENTER CHOICE:
```

Adding a Storage Unit Group

To add a storage unit group, press **a** (`Add Storage Unit Group`) while viewing the `Storage Unit Group Management` menu and follow the prompts. The following is an example of creating a group of 2 robots. User responses are in bold.

```
Adding Storage Unit Group (<ESC> to abort)

--------------------------------------------------
Enter Storage Unit Group Name: robot_group <Return>

Enter the storage unit names, 1 per line in order of desired priority.
<CR> with no name to end entry.
<ESC> quit without adding a group
   Enter Name of stunit: TSD_1 <Return>
   Enter Name of stunit: TSD_2 <Return>
   Enter Name of stunit: <Return>

Adding group name: robot_group

Precedence Storage unit name
```

```
---------- -------------------
    1      TSD_1
    2      TSD_2

Add the storage unit group list now? (y/n) (y): y
```

▼ **To add a storage unit group**

1. Provide a unique label for the storage unit group. This is the label you use to associate the group with a policy or schedule.

2. Provide the names of the storage units that are part of the group. List the storage units in priority order: that is, first provide the name of the storage unit that you want NetBackup to use first. Next, provide the name of the storage unit that you want NetBackup to use second, and so on.

   To end the list of storage units, press **Return**. You will see the definition displayed.

3. Press **y** to confirm the addition or **n** to cancel. This returns you to the `Storage Unit Group Management` menu.

4. To review the addition, press **l** (`List/Display Storage Unit Groups`). To change attributes, press **m** (`Modify Storage Unit Group`), or else delete the group and add it again.

If you are configuring NetBackup for the first time and are satisfied with your configuration, go to "Adding a Policy" on page 195.

Displaying and Changing Storage Unit Group Configurations

The Storage Unit Group Management menu has options for viewing the attributes for currently configured storage units or directing the list of attributes to a file. This menu also has options for modifying the configuration by either deleting storage unit groups or changing their attributes.

▼ **To view or change storage unit group configurations**

1. Once in a storage unit menu, press **b** (`Browse Storage Units Groups Forward`) until the `Label` line at the top of the screen shows the name you want.

2. Select the desired option:

- To add or delete a storage unit from a group, to change the name of a storage unit in a group, or to change the precedence of a storage unit in a group, press **m** (`Modify Storage Unit Group`) and follow the prompts (existing values are in parentheses). To modify other attributes, you must delete and then re-add the group.
- To delete a storage unit group, press **d** (`Delete Storage Unit Group`). At the prompt, check to ensure that you are deleting the correct group and press **y** if you want to delete it.
- To view the members of a storage unit group, press **l** (`List/Display Storage Unit Groups`).
- To direct the list of attributes to a file, press **o** (`Output Destination`) and specify the desired file path at the prompt. Press **l** to write the list to the file.

Defining and Managing Policies

The procedures in this section explain how to define and manage NetBackup policies. To display the `Policy Management` menu, press **p** (`Policy Management`) at the `bpadm` main menu.

```
             Policy: <ALL>
           Clients: <ALL>
         Schedules: <ALL>
Output Destination: SCREEN

Policy Management
-------------------------
a) Add Policy...
m) Modify Policy Attributes...
d) Delete Policy
s) Schedule Management...
c) Client List Management...
f) File List Management...

b) Browse Policies Forward
r) Browse Policies Reverse
e) Enter Policy
l) List/Display Policies
o) Output Destination  (SCREEN or FILE)
h) Help
q) Quit Menu

   ENTER CHOICE:
```

Adding a Policy

▼ To add a policy to the configuration

1. Press **a** while viewing the `Policy Management` menu to start a series of prompts for adding a policy. Some choices, such as `Cross Mount Points`, have default values in parentheses. In the following example, user responses are in **bold**.

   Additional options may be presented based on the licenses and optional software installed.

```
Adding Policy (<ESC> to abort)
------------------------------
```

2. Provide a name for the policy. This name must be unique to the configuration (no spaces are allowed in names).

```
Enter Unique Policy Name: W2 <Return>
```

3. Specify whether you want to use an existing policy as a template. This is convenient if another policy has many of the same attributes. You can subsequently make the necessary changes for the policy you are adding. If you use another policy for a template, NetBackup duplicates the following:

   - Policy attributes
   - Selections list
   - Client list
   - All schedules

```
Use an existing policy as a template; if yes, all
attributes and schedules will be duplicated: (y/n)?n
```

4. Configure the policy by selecting the policy attribute choice from the list and pressing **Return**:

```
Policy:         W2

        Modify Policy Attributes (<ESC> to quit)
        ----------------------------------------
1) Policy Type                              : Standard
2) Active                                   : Yes
3) Collect True Image Recovery Information : No
4) Cross mount points                       : No
5) Follow NFS mounts                        : No
6) Client Compression                       : No
--) Client encryption                        : No
```

```
8) Allow multiple data streams             : No
--) Collect disaster recovery information   : No
10) Maximum number of jobs per policy       : Unlimited
11) Required storage unit                   :
12) Volume pool                             : NetBackup
13) Keyword                                 :
14) Priority as compared to other policies  : 0
15) Take checkpoints                        : No
16) Set Policy Attributes for Advanced Client.

Enter Choice (choices marked "--" are unavailable) [1-16]: 1 <Return>
```

Policies contain the following attributes:

1) **Policy Type**

Select the policy type from the list:

```
Policy Type
-----------
1)  Standard
2)  Apollo-wbak
3)  Oracle
4)  NetWare
5)  MS-Windows-NT
6)  OS/2
7)  DB2
8)  FlashBackup
9)  AFS
10)  FlashBackup-Windows
11)  Vault
Enter Choice [1-11]:  (1)
```

2) **Active**

Specify whether to activate the policy. A policy must be active for NetBackup to run any of the automatic or user-directed schedules). Specifying **y** sets the policy to active.

Provide the date for the policy to go into effect. Specifying **n** makes the policy immediately effective:

```
Active? (y/n) (y): y
Enter effective date: (04/04/2004 11:01:11 or (n)ow)
```

3) **Collect True Image Recovery Information**

Specify whether to collect True Image Recovery Information. (See "Collect True Image Restore Information" on page 87 in *NetBackup System Administrator's Guide for UNIX, Volume I*.) The example uses the default which is **n** (no).

`4)` **Cross mount points**

Specify whether to cross mount points when doing backups and archives. The example uses the default, which is **n**.

`5)` **Follow NFS mounts**

Specify whether to follow NFS mounts.

- **y** enables NetBackup to back up and archive NFS-mounted files and directories.
- **n** prevents NetBackup from backing up or archiving NFS-mounted files and directories. The default is **n**.

`6)` **Client compression**

Specify whether to compress the files that you archive or back up from that client. The example uses the default, which is **n** (no).

`7)` **Client encryption**

The Client Encryption policy attribute is selectable only if the NetBackup Encryption option is installed and configured. When using client encryption, the server encrypts the backup for the clients listed in the policy. For more details on client encryption, refer to the *NetBackup Encryption System Administrator's Guide* for more information.

`8)` **Allow multiple data streams**

Specify whether to allow multiple data streams. The example uses the default, which is **n** (no).

`9)` **Collect disaster recovery information**

Specify whether or not you want NetBackup to collect the information required for intelligent disaster recovery during backups of Windows clients using this policy. (See "Configuring NetBackup Policies for IDR" on page 294 in the *NetBackup System Administrator's Guide for UNIX, Volume II*.)

`10)` **Maximum number of jobs per policy**

Specify whether to limit the number of jobs per policy. If you elect to limit the number of jobs per policy, specify the maximum number of jobs that this policy can perform concurrently. (See "Limit Jobs Per Policy" on page 81 in *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`11)` **Required storage unit**

Determine whether to specify a default storage unit for the policy. For example, indicating **TS8_1** means that NetBackup directs backups and archives for this policy to `TS8_1`, except for schedules that specify a storage unit.

`12)` **Volume pool**

Determine whether to specify a default volume pool for the policy. If you do not specify a volume pool for either the policy or the schedule, the `NetBackup` volume pool is used.

13) **Keyword**

Determine whether to use a keyword phrase. (See "Keyword Phrase (Optional)" on page 96 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.) The example uses the default, which is **n** (no).

14) **Priority as compared to other policies**

Provide the priority for this policy relative to other policies. Any non-negative integer is valid. The policy with the highest value has highest priority. The default is **0**.

15) **Take checkpoints**

Specify whether checkpoints should be taken during the backup. (See "Checkpoint Frequency" on page 79 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.) If you indicate **y**, you'll be asked how frequently checkpoints should be taken:

```
Take checkpoints? (y/n) (n): y <Return>
Enter checkpoint interval (minutes) [5-180]:  (15) <Return>
```

16) **Advanced Client**

To specify an Advanced Client configuration, the Advanced Client option must be installed and licensed. For more details on offhost backup, refer to the *NetBackup Advanced Client System Administrator's Guide*.

The Advanced Client configuration contains the following options:

```
Policy:         name
Modify Policy Attributes for Advanced Client (<ESC> to quit)
------------------------------------------------------------
  1) Perform block level incremental backups : No
  2) Perform snapshot backups                : No
 --) Retain snapshots for Instant Recovery   : No
 --) Perform offhost backup                  : No
 --) Use alternate client                    : No
 --) Alternate client name                   :
 --) Use data mover                          : No
 --) Data mover type                         :
 --) Snapshot method                         :
 --) Snapshot method arguments               :

 11) Return to main Policy Attributes menu.
Enter Choice (choices marked "--" are unavailable) [1-11]:
```

5. Press **<ESC>** to add the policy, then:

```
Press y to add the policy or n to cancel.
```

6. To review the addition, press **l** (`List/Display Policies`). To change attributes, press **m** (`Modify Policy Attributes`).

   If you are configuring NetBackup for the first time and are satisfied with your policy configuration, go to "Adding Clients to a Policy" on page 200.

Displaying and Changing Policy Configurations

The `Policy Management` menu has options for viewing the attributes for currently configured policies or directing the list of attributes to a file. This menu also has options for modifying the configuration by either deleting policies or changing their attributes.

▼ To view or change policy configurations

1. Select the desired policy by browsing with the **b** and **r** options until the name of that policy appears on the Policy line at the top of the screen. You can also use the **e** option to specify the policy name.

2. Select the desired option:

   - To modify the attributes, press **m** (`Modify Policy Attributes`). At the prompt, check the top line on the screen to ensure you are modifying the correct policy. Provide new values at the prompts or simply press **Return** to accept the existing values (shown in parentheses).
   - To delete a policy, press **d** (`Delete Policy`). At the prompt, check to ensure that you are deleting the correct policy and press **y** if you want to delete it. Deleting a policy from the NetBackup configuration does not prevent you from restoring files that were backed up or archived by clients in that policy.
   - To list the attributes for the policy, press **l** (`List/Display Policies`). Use the controls at the bottom of the screen to move within the list.
   - To direct the list of attributes to a file, press **o** (`Output Destination`) and specify the desired file path at the prompt. Press **l** to write the list to the file.

Defining and Managing the Client List for a Policy

The procedures in this section explain how to define and manage client lists for policies.

Adding Clients to a Policy

▼ To add clients to a policy

1. From the `Policy Management Menu`, press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

2. Press **c** to bring up the `Client List Management` menu. This menu has options for managing your client list. The policy you selected in the previous step appears on the Policy line at the top of the screen. The example below shows policy `W2`.

```
            Policy: W2
           Clients: <none>
         Schedules: <none>
Output Destination: SCREEN

Client List Management
-----------------------
a) Add Clients
d) Delete Clients

l) List/Display Policy
o) Output Destination (SCREEN or FILE)
h) Help
q) Quit Menu

Enter Choice:
```

3. Press **a** at the `Client List Management` menu. This brings up the list of client types currently installed at your site. In the following example, responses are in bold.

```
Policy:  W2
Adding Clients (<ESC> to abort)
 -------------------------------
   1)  NDMP, NDMP
   2)  Novell, NetWare
   3)  PC, Windows2000
   4)  PC, WindowsNET
   5)  PC, WindowsNT
   6)  PC, WindowsXP
   7)  PC-IA64, WindowsNET
   8)  PC-IA64, WindowsXP
   9)  Solaris, Solaris7
   10)  Solaris, Solaris8
   11)  Solaris, Solaris9
   12)  Solaris, Solaris_x86_7
```

```
   13)  Solaris, Solaris_x86_8
   14)  Solaris, Solaris_x86_9

Enter Selection (or 'q' to quit): 10 <Return>
Enter clients of Solaris, Solaris8 type: (blank line to end)
     Enter Client Name: hagar <Return>
     Enter Client Name: <Return>

Adding clients to policy W2 ...
     hagar
Install client software (y/n) n

[Menu of choices reappears]
```

4. Provide the number corresponding to the type of client you are adding.

5. Specify the names of the clients of this type (one per line). When selecting client host names, always observe the following rules:

   - Use the same name if you put the client in multiple policies.
   - Use a name by which the server knows the client. This name should be 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 `hagar.bdev.null.com` or `hagar.bdev` rather than just `hagar`.

   When you finish naming the clients, leave a blank line and press **Return**. You see a message informing you that the client is being added.

   You are prompted as to whether you want to install client software.

Note The prompt appears only if client software was loaded on the master server during NetBackup installation and is therefore available for installation on clients.

- If you added trusting clients and want to install software now, press **y** to have `bpadm` immediately push client software from the server to the client. A *trusting client* is one that *does* have an `/.rhosts` file with an entry for the NetBackup server. This software installation occurs after the clients are added to the policy. If the software installation fails on any of the clients, NetBackup notifies you, but still keeps the client in the policy. Note that client software installation can take a minute or more per client.
- If you added secure clients, you should press **n** and then install them later as explained under "Installing Software on Secure UNIX Clients" on page 101 in *NetBackup System Administrator's Guide for UNIX, Volume I*. A *secure client* is one that does *not* have an entry for the NetBackup server in its `/.rhosts` file.

- If you added trusting clients but want to install software later, press **n** at the installing software prompt. You can install the software later by selecting `Install All Clients` from the `Special Actions` menu. (See "Installing NetBackup Software on All Trusting Client Hosts" on page 214).

If you press **n** at the prompt or if software installation is complete, `bpadm` returns you to the list of choices so you can add another type of client.

6. Repeat step 4 and step 5 until your list is complete, then press **q** to return to the `Client List Management` menu.

7. To review the addition, press **l** (`List/Display Policy`).

   If you are configuring NetBackup for the first time and are satisfied with your client list for this policy, go to "Adding to a Selections List" on page 203.

Displaying Client Lists and Deleting Clients from a Policy

The `Client List Management` menu has options for viewing a client list for a currently configured policy or directing the list to a file. This menu also has an option for deleting clients from a policy.

▼ To view client lists or delete clients from a policy

1. From the `Policy Management Menu`, press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

2. Press **c** to bring up the `Client List Management` menu. The policy you selected in the previous step appears at the top of the screen.

3. Select the desired option:

   - To delete clients, press **d** (`Delete Clients`). Check to ensure that you are deleting clients from the correct policy and follow the prompts. Deleting a client does not delete any backups or archives that belong to the client.
   - To list the attributes for the policy (including the clients), press **l** (`List/Display Policy`). Use the controls at the bottom of the screen to move within the list.
   - To direct the list of policy attributes (including the clients) to a file, press **o** (`Output Destination`). Provide the desired file path at the prompt, then press **l** (`List/Display Policy`).

Defining and Managing the Selections List for a Policy

The selection list for a policy applies to all full and incremental backups for the clients in that policy. The procedures in this section explain how to define and manage the list of files.

Adding to a Selections List

▼ To add entries to a selections list

1. From the `Policy Management Menu`, press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

2. Press **f** to bring up the `File List Management` menu. This menu has options for managing your client list. The policy you selected in the previous step appears on the `Policy` line at the top of the screen. The example below is for policy `W2`.

```
          Policy:  W2
            Clients:  mars saturn ...
          Schedules:  <none>
 Output Destination:  SCREEN

 File List Management
 --------------------
 a)  Add Files
 d)  Delete Files
 m)  Modify Files List

 l)  List/Display Policy
 o)  Output Destination  (SCREEN or FILE)
 h)  Help
 q)  Quit Menu

 ENTER CHOICE: a
```

3. Press **a** to bring up the `Add Files` menu:

```
Policy: W2
Clients:  mars jupiter ...
Schedules:  <none>
File Paths: <none>

Adding File Paths (<ESC> to Abort, Blank line to end)
(NOTE: Spaces, ' ', are significant in pathnames)
-------------------------------------------------
Enter File Path: /usr <Return>
```

```
Enter File Path: /home <Return>
Enter File Path: /var <Return>
Enter File Path: <Return>

Adding file paths . . .
getting policy list . . .
```

4. Provide the file paths at the prompts. Specify one path per line; each line must be full (absolute) file paths. When finished, leave a blank line and press **Return**. This returns you to the `File List Management` menu (pressing **Escape** aborts the operation without altering the configuration).

   Metacharacters or wildcard characters are allowed when specifying file lists.

   To back up a raw partition, specify the path to the block or character device file, as in the following example:

   ```
   /dev/rdsk/isc0d2s6
   ```

   The character device is preferred as it generally is faster than the block device.

   For some database extension policy types, such as Oracle, specify the scripts that control the backup. For a Vault policy, specify the vault command line. (See the *NetBackup Vault System Administrator's Guide* for more information.)

5. To review the additions, press **l** (`List/Display Policy`). To make changes, press **m** (`Modify Files List`) or **a** (`Add Files`) or **d** (`Delete Files`).

   If you are configuring NetBackup for the first time and are satisfied with your file list, go to "Adding a Schedule" on page 205.

Displaying and Changing a File List

The `File List Management` menu has options for viewing the file list for currently configured policies or directing the list to a file. This menu also has options for deleting or modifying files from a policy.

▼ To view file lists or delete files from a policy

1. From the `Policy Management` menu, press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

2. To bring up the `File List Management` menu, press **f**. The policy you selected in the previous step appears at the top of the screen.

3. Select the desired option:

- To modify files, press **m** (`Modify Files List`). You can insert, delete, or modify the file list.
- To delete files, press **d** (`Delete Files`). Check to ensure that you are deleting files from the correct policy and follow the prompts. Deleting a file from the file list does not prevent you from recovering any backups or archives for that file.
- To list the attributes for the policy (including the files), press **l** (`List/Display Policy`). Use the controls at the bottom of the screen to move within the list.
- To direct the list of policy attributes (including the file list) to a file, press **o** (`Output Destination`). Provide the desired file path at the prompt, then press **l** (`List/Display Policy`) to write the attributes to the file.

Defining and Managing Schedules for a Policy

Each policy must have a set of schedules to control its backup and archive operations. The procedures in this section explain how to define and manage those schedules with `bpadm`.

Adding a Schedule

▼ **To add either an automatic or user-directed schedule**

1. From the `Policy Management` menu, press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

2. To manage schedules, press **s** (`Schedule Management`). The policy you selected in step 1 appears on the `Policy` line at the top of the screen.

```
            Policy: W2
          Schedule: <none>
           Clients: mars jupiter ...
Output Destination: SCREEN

Schedule Management
-------------------------------
a) Add Schedule...
d) Delete Schedule
m) Modify Schedule...

b) Browse Schedules
l) List/Display Schedule
o) Output Destination  (SCREEN or FILE)
h) Help
q) Quit Menu
```

3. To add a schedule, press **a** (`Add Schedule`). All choices except `Schedule Label` have default values in parentheses. Press **Return** to accept default values.

```
Policy:           W2
Add Schedule (<ESC> to abort)
-----------------------------

Enter Schedule Label: W2_daily_differential <Return>

Schedule Type
-------------
  0) Full Backup
  1) Differential Incremental Backup
  2) Cumulative Incremental Backup
  3) User Backup
  4) User Archive
Enter Choice [0-4]:  (0) 1 <Return>

 Frequency scheduling(f) or Calendar scheduling(c) :(f)  <Return>

 Enter Exclude date (mm/dd/yyyy): 07/18/2004 <Return>

   Exclude dates entered so far:
    0 - 07/18/2004
     enter c to clear all, d-# to delete 1 <Return>

 Enter Exclude date (mm/dd/yyyy): <Return>

Backup Frequency can be specified in hours(h), days(d), or
weeks(w).
Enter the unit to be used in specifying backup frequency (h/d/w): (d)
<Return>

Enter Backup Frequency (in days) [1-3500]:  (7) 1

Multiple copies? (y/n) (n): <Return>

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
     .
     .
     .
  23) infinite
  24) infinite

  Enter Choice [0-24]:  (1) 0 <Return>

Require images to be written to a specific storage unit? (y/n) (n): n

Do you want to override the policy volume pool? (y/n) (n): n

Use multiplexing if able? (y/n) (n): y <Return>
What maximum multiplexing factor should be used?
(A value of 1 indicates to not do multiplexing)
Enter value [1-32]:  (1) 2 <Return>

Backup windows can be specified for each day of the week.
Should the backup window be the same every day of the week? (y/n) y): n
  Enter daily windows (start time and duration in hours)
     Sunday    (20:00:00 10): 22 0
     Monday    (22:00:00  0): 22 8
     Tuesday   (22:00:00  8): 22 8
     Wednesday (22:00:00  8): 22 8
     Thursday  (22:00:00  8): 22 8
     Friday    (22:00:00  8): 22 8
     Saturday  (22:00:00  8): 22 0

Schedule Summary
---------------------------------------------
       Policy:         W2
       Schedule:       W2_daily_differential
       Differential Incremental Backup
         EXCLUDE DATE 0 - 02/02/2003
       Frequency=1 days
       Retention Level=0 (1 week)
       Required storage unit not specified
       Schedule not overriding volume pool
       Multiplexing=2
       Daily Windows
         Monday     22:00:00  -->  Tuesday    06:00:00
         Tuesday    22:00:00  -->  Wednesday  06:00:00
         Wednesday  22:00:00  -->  Thursday   06:00:00
         Thursday   22:00:00  -->  Friday     06:00:00
         Friday     22:00:00  -->  Saturday   06:00:00
```

```
---------------------------------------------
       Add schedule W2_daily_differential now(y/n/c-hange) y
```

4. Specify a unique label for the schedule (no spaces are allowed in the label). This name appears on screens and messages from NetBackup, so select a name with a meaning you can remember.

5. Specify the schedule type. Choices `0`, `1`, and `2` select automatically scheduled backups. Choices `3` and `4` are user-directed. The example specifies `1` for Differential Incremental backup.

   If the policy type is for database backups, such as an Oracle-Obackup policy, you see a set of choices similar to the following:

   ```
   Schedule Type
   1. Scheduled Obackup script
   2. Obackup initiated script
   ```

   Choice `1` is for an automatically scheduled database backup that is started by the NetBackup scheduler. Choice `2` is started by the `obackup` process on the client. See the installation guide for the respective products for more information.

6. Specify frequency scheduling (`f`) or calendar scheduling (`c`).

7. Enter one or more exclude dates. Exclude dates are dates when the schedule will not run. Press **Return** to terminate entering exclude dates.

8. Specify the units for the backup frequency you will specify in step 9 (does not apply to user-directed backups and archives). In the example, pressing **Return** selects the default, which is days.

9. Specify the backup frequency (does not apply to user-directed backups and archives). This is the time that should occur between successful backups and is expressed in terms of the units selected in step 8. The example selects 1 day.

10. Specify the retention level for the backups or archives that this schedule creates. (See "Retention" on page 169 in *NetBackup System Administrator's Guide for UNIX, Volume I*.)

11. Specify whether you want to direct the backup images for this schedule to a specific storage unit.

    - Pressing **y** brings up a prompt for the name of the storage unit.
    - Pressing **n** accepts the storage unit as specified at the policy level.

    If you did not specify one at the policy level, NetBackup uses the next storage unit available.

12. Specify whether to specify a volume pool for the schedule.
    - If you provide a volume pool name, this choice overrides the policy level volume pool.
    - If you do not provide a volume pool name, NetBackup uses the volume pool specified at the policy level. If you do not specify one at either the schedule or policy level, NetBackup uses a default of `NetBackup`.

13. Specify whether you want to use multiplexing.

    Multiplexing sends concurrent, multiple backups from one or several clients to a single drive and multiplexes the images onto the media.

    If you answer **`y`** to this prompt, you are asked to specify the multiplexing factor. The *multiplexing factor* is the maximum number of jobs from this schedule that you want to multiplex on any one drive. The number can range from 1 to 32; `1` specifies no multiplexing.

14. Specify the start times and durations for the backup window:
    - Pressing **`y`** (that is, accepting the default) specifies that the backup window opens on each day of the week. NetBackup can attempt backups each day and during the same time frame. The prompts ask you to define when the window opens and how long it remains open each day.
    - Pressing **`n`** brings up prompts for specifying a different window for each day of the week. Specify time in terms of the 24-hour clock. For example, 00:00:00 is 12 am, 12:00:00 is 12 pm, and 23:30:00 is 11:30 pm. The duration is in hours.

    You can specify the time in *hours, hours:minutes*, or *hours:minutes:seconds*. For example, if you specify just the hours or hours and minutes, `bpadm` completes the entry. Specifying 22 results in a time of 22:00:00 and specifying 22:30 results in a time of 22:30:00.

    When completing the daily windows, remember to leave a blank space between the hours and the duration. Specifying 22 8 results in a time of 22:00:00 and duration of 8 hours. Specifying 2 8 results in a time of 02:00:00 and a duration of 8 hours. Specifying 0 for the duration results in no backup window. Specifying 0 for the time results in a start time of 00:00:00.

15. Press **`y`** to add the schedule to this policy, **`n`** to cancel, or **`c`** to change some aspect of it.

    If you press **`c`**, you see the same prompts just described. The values provided are the values you previously entered.

If you are configuring NetBackup for the first time and are satisfied with the schedules for this policy, return to "Adding a Policy" on page 195 and repeat the procedures in this chapter as necessary for the next policy.

Displaying and Modifying a Schedule

The `Schedule Management` menu (see "Adding a Schedule" on page 205) has options for modifying the list of schedules for currently configured policies or directing the list to a file. This menu also has options for modifying schedules or deleting them from a policy.

▼ **To view or modify schedules**

1. From the `Policy Management` menu, press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

2. To bring up the `Schedule Management` menu, press **s**. The policy you selected in the previous step appears at the top of the screen.

3. Press **b** (`Browse Schedules`) until the `Schedule` line at the top of the screen shows the name you want.

4. Select the desired option:
   - To modify a schedule, press **m** (`Modify Schedule`). Check the top line on the screen to ensure that you are modifying the correct schedule. Provide new values at the prompts or press **Return** to accept existing values (shown in parentheses).
   - To delete a schedule, press **d** (`Delete Schedule`). At the prompt, check to ensure that you are deleting the desired schedule. Press **y** to delete it.
   - To list the attributes for the schedule selected in step 3, press **l** (`List/Display Schedule`). Use the controls at the bottom of the screen to move within the list.
   - To direct the list of policy attributes for the schedule selected in step 3 to a file, press **o** (`Output Destination`). Provide the desired file path at the prompt, and press **l** (`List/Display Schedule`) to write the attributes to the file.

Defining NetBackup Global Attributes

The Global Configuration attributes (option **g** from the main `bpadm` Administration menu) define aspects of NetBackup operation not defined elsewhere in the configuration. In the following example, possible user responses are in bold.

```
                Keep Logs: 28 days
       Admin Mail Address: lxk@freddie.bdev.null.com,txz@mars...
          Wakeup Interval: 10 minutes
      Preprocess Interval: 0 hours
             Backup Tries: 2 times in 12 hours
   Maximum Backup Copies: 2
      Output Destination: SCREEN
```

```
   Global Configuration
   --------------------
   m)  Modify Configuration Parameters...
   l)  List/Display All Configuration Parameters
   o)  Output Destination (SCREEN or FILE)
   h)  Help
   q)  Quit Menu

   ENTER CHOICE: m

Modify Configuration
--------------------
m)  Mail Address: lxk@freddie.bdev.null.com,txz@mars...
w)  Wakeup Interval:  10 minutes
j)  Max Jobs/Client:  1
b)  Backup Tries:  2 times in 12 hours
k)  Keep Logs:       28 days
i)  Keep TIR Info:       1 days
t)  Media Mount Timeout:  0 minutes
h)  Display Reports:  24 hours ago
c)  Compress Image DB Files:   (not enabled)
x)  Preprocess time interval:   0
l)  Shared media mount timeout: 0 minutes
e)  Max drives this master:  0
d)  Notify Request Daemon of Changes
n)  Maximum Number of Backup Copies: 2
q)  Quit Menu

ENTER CHOICE: k

 Enter the number of days to keep logs:  (28)  21 <Return>
Changing global attribute....
```

▼ To list or modify Global attributes

1. From the `bpadm` main menu, press **g** (`Global Attributes`) to bring up the `Global Configuration` menu.

2. To modify values, press **m**. The example changes the value of `Keep Logs` from 28 days to 21.

3. To list the current values, press **l** (`List/Display All Configuration Parameters`).

   Global attributes consist of the following properties:

`l)` **Policy Type**

Select the policy type from the list:

The following table defines each of the NetBackup global attributes.

`m)` **Mail Address**

Address to which NetBackup sends notifications on results of failed automatic backups, administrator-directed manual backup operations, and automatic database backups. Provide the administrator's address. The default is none. See "Administrator's E-mail Address" on page 366 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`w)` **Wakeup Interval**

Length of time, in minutes, that the scheduler waits before checking if any backups are scheduled to begin. Long wake up intervals can cause the scheduler to miss too much of a backup window to complete its backups. The default is 10 minutes. See "Wakeup Interval" on page 362 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`j)` **Max Jobs/Client**

Maximum number of jobs that NetBackup clients can perform concurrently. The default is 1. See "Maximum Backup Copies" on page 364 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`b)` **Backup Tries**

Number of times that NetBackup tries a backup job for a client/policy/schedule combination during the specified time period. Ensure that the time period and the number of tries are greater than 0. You can specify 0 for the number of tries, but it stops all scheduled backups. The default is 2 tries in 12 hours. Note that this attribute does not apply to user-directed backups and archives. See "Schedule Backup Attempts" on page 362 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`k)` **Keep Logs**

Length of time, in days, that the NetBackup server keeps its error database, job database, and debug logs. NetBackup derives its Backup Status, Problems, All Log Entries, and Media Log Entries reports from the error database. Therefore, Keep Logs limits the time period that these reports can cover. The default is 28 days. See "Keep Logs" on page 364 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`i)` **Keep TIR Info**

Length of time to keep true image recovery information for those policies that use it. See "Keep True Image Restoration (TIR) Information" on page 364 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`t)` **Media Mount Timeout**

Length of time, in minutes, that NetBackup waits for the requested media to be mounted. This timeout will eliminate excessive waits for operations with nonrobotic devices (operator must mount media) or for media that is outside the robot or off site. The default is 0 (unlimited). See "Media Mount Timeout" on page 387 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

`h)` **Display Reports**

Default time period that NetBackup uses as it searches for information to put into a report. For example, a value of `8` provides a report covering the previous 8-hour period. See "Status Report Interval" on page 362 in the *NetBackup System Administrator's Guide for UNIX, Volume I*.)

The minimum setting is 1 hour. The default is 24 hours.

`c)` **Compress Image DB Files**

Number of days that must elapse (since the image was created) before NetBackup compresses its image database files (also called image catalog files). The image database has information about client backups and archives. A value of 0 means that no compression should be done. See "Compress Catalog Interval" on page 364 in the NetBackup System Administrator's Guide for UNIX, Volume I.)

`x)` **Preprocess time interval**

Minimum time that can elapse between client queries to discover new paths if NetBackup is using auto-discover streaming mode. (See "Backup Selections List Directives for Multiple Data Streams" on page 133 in NetBackup System Administrator's Guide for UNIX, Volume I.)

`l)` **Shared media mount timeout**

`e)` **Max drives this master**

Maximum number of drives (on this master and its media servers) that the master server should consider available when scheduling backups. Limits the total number of drives that the scheduler will use, regardless of the number of drives configured.

`d)` **Notify Request Daemon of Changes**

Signals `bprd` that the configuration parameters have changed. Choosing this parameter puts the changes into effect without restarting `bprd`.

`n)` **Maximum Number of Backup Copies**

Maximum number of copies of a backup that can be stored in the NetBackup database. (See "Maximum Backup Copies" on page 364 in the NetBackup System Administrator's Guide for UNIX, Volume I.)

Installing NetBackup Software on All Trusting Client Hosts

To install software on trusting clients, press **c** (`Install All Clients`) while viewing the `Special Actions` menu. A *trusting* client is one that has an `/.rhosts` file with an entry for the NetBackup server.

The **c** option pushes client software from the server to the client. You can install software on all clients at one time or when you add them to a policy

1. From the `bpadm` main menu, press **x** (`Special Actions`) to bring up the `Special Actions` menu.

```
Special Actions
--------------------
c) Install All Clients...
b) Backup Databases...
r) View and Change Retention Levels

i) Initiate Request Daemon
t) Terminate Request Daemon

h) Help
q) Quit Menu

ENTER CHOICE:
```

2. To start the installation of software on all clients, press **c**. Note that client software installation takes a minute or more per client.

Displaying Reports

The `Reports` menu lets you view problem or status reports from one or more NetBackup servers or clients. To use this menu, press **r** while viewing the `bpadm` main menu.

```
              Server:  ALL
              Client:  ALL
          Start Date:  01/22/2003 13:58:27
            End Date:  01/23/2003 23:59:59
Output Destination:  SCREEN

Reports
-------
b)  Backup Status
l)  List Client Backups
p)  Problems
a)  All Log Entries
m)  Media...

d)  Change Dates
c)  Change Client
s)  Change Server
o)  Output Destination  (SCREEN or FILE)
h)  Help
q)  Quit Menu

ENTER CHOICE:
```

▼ To view reports or change report parameters

1. To select the server that has the reports you want to view, press **s** (`Change Server`).

   The `Server Name` line at the top of the menu displays your choice. Specifying `ALL` (the default) provides a report for all servers (except when viewing `Media reports`).

2. To select the client, press **c** (`Change Client`).

   The `Client Name` line at the top of the menu displays your choice. Specifying `ALL` provides reports for all clients and the selected server.

3. To specify the time period that you want the reports to cover, press **d** (`Change Dates`) and follow the prompts.

   The `Start Date` and `End Date` lines at the top of the screen display your choices. The resulting report shows information ranging from the start date to the end date.

NetBackup derives the `Backup Status`, `Problems`, `All Log Entries`, and `Media Log Entries` reports from the error database. Therefore, the `Keep Logs` attribute sets the maximum time period that these reports can cover. The maximum time limit for other Media reports and the `List Client Backups` report depends on the retention period for the associated backup images.

4. Select from among the following options. See "NetBackup Report Types" on page 263 in *NetBackup System Administrator's Guide for UNIX, Volume I* for detailed information about each report.

   - Press **b** (`Backup Status`) to obtain status and error information on backups completed successfully or failed within the specified time period.
   - Press **l** (`List Client Backups`) to see detailed information on successful backups completed within the specified time period.
   - Press **p** (`Problems`) to see the problems that the server has logged during the specified time period. The information is a subset of the information you get from the `All Log Entries` option.
   - Press **a** (`All Log Entries`) to list all the log entries for the specified time period.
   - Press **m** (`Media`) to bring up the `Media Reports` menu. Prior to executing a media report option, you can select the servers (and clients, if necessary) for which you want the report. For `Media Log` entries, you also can select the range of dates that you want the report to cover.

```
                        Server:  ALL
                        Client:  ALL
                 Media ID/Path:  ALL
                    Start Date:  01/22/2003 13:58:27
                      End Date:  01/23/2003 23:59:59
            Output Destination:  SCREEN

 Media Reports                 Change Parameters
 -------------                 -----------------
l)  Media List            s)  Change Server
u)  Media Summary         c)  Change Client
m)  Media Contents         p)  Change Media ID/Path
i)  Images on Media        d)  Change Dates
e)  Media Log Entries      o)  Output Destination (SCREEN or FILE)
w)  Media Written

h)  Help
q)  Quit Menu

                     ENTER CHOICE:
```

▼ To view media reports or change report parameters

1. From the `Reports` menu, to select the server for which you want to show reports, press **s** (`Change Server`) option.

   The `Server` line at the top of the menu displays your choice. Specifying `ALL` provides a report for all servers (except when viewing `Media reports`).

   When changing the server, the server initiating the request (the server on which you are running `bpadm`) must be able to access the server you select. Otherwise, you receive the message: "`access is not allowed`" or "`no entity was found`." Access to a server is controlled by the `SERVER` entry in its `bp.conf` file. (See "NetBackup Configuration Options" on page 134.)

Note If you fail to connect to a server, the server to which you had previously connected, and any previously displayed report information, will persist.

2. For `Images on Media` reports, select the client by pressing **c** (`Change Client Name`). The name specified with this option appears on the `Client` line at the top of the menu. Specifying `ALL` provides reports for all clients and the selected server.

3. For `Media Log` entries, specify the time period that you want the reports to cover by pressing **d** (`Change Dates`). Follow the prompts. The dates you specify appear on the Start Date and End Date lines at the top of the screen. The resulting report shows information ranging from the start date to the end date.

4. From the Reports menu, select **m** (Media) to bring up the `Media Reports` menu. Choose from among the following report options:

   - Press **l** (`Media List`) to show either a single or all media IDs in the NetBackup media catalog. This option does not apply to Disk type storage units, nor does it show media assigned for the purpose of backing up NetBackup catalogs. You can get information for images on those storage units by using the i (Images on Media) option.
   - Press **u** (`Media Summary`) to list all media in the specified server's catalog, according to whether it is active. The report also shows the expiration date for the media and shows the number of media that are at each retention level.
   - Press **m** (`Media Contents`) to list the contents of a single media ID. You must select only one media ID to use this option. The resulting report shows the contents of the media header and backup headers that are recorded on the media. You cannot use this option for disk type storage units.

The media contents report is useful for determining the backup IDs that are on a specific media ID by reading them from the media itself rather than the catalog. Because it requires a media mount, this option involves a greater delay for tape than for optical disk.

- Press **i** (`Images on Media`) to list the contents of media as recorded in the NetBackup catalog. `bpadm` queries only the NetBackup database on the master server it is running on. You can use this option to list the contents of any type of media (including disk). You can select by client, media ID, or path.
- Press **e** (`Media Log Entries`) to list the media errors or informational messages relating to media that are recorded in the NetBackup error database. You can use the **d** (Change Dates) option to select errors by date.
- Press **w** (`Media Written`) to list the media in the specified server's catalog that has been used for backups within the specified time period. This report does not show media used for image duplication if the original image was created prior to the specified time period.

Managing bprd (NetBackup Request Daemon)

To manage the NetBackup request daemon (`bprd`), press **x** (`Special Actions`) while viewing the `bpadm` main menu. `bprd` daemon functions include starting the scheduler and the NetBackup database daemon (`bpdbm`).

```
Special Actions
    ---------------
c)  Install All Clients...
b)  Backup Databases...
r)  View and Display Retention Levels

i)  Initiate Request Daemon
t)  Terminate Request Daemon

h)  Help
q)  Quit Menu

   ENTER CHOICE:
```

▼ **To manage the request daemon**

1. Press **i** to start bprd, if it is not running. Normally, bprd is started at boot time. You use this option when you stop the daemon to alter the configuration. Starting bprd also starts bpdbm if bpdbm is not already executing.

2. Press **t** to stop bprd. If the daemon has started any activities, they are allowed to complete. With bprd stopped, NetBackup is unable to perform any backup, archive, or restore operations. Note that terminating bprd does not terminate bpdbm. To stop bpdbm, enter bpdbm -terminate (see bpdbm(1M)).

Always stop the NetBackup request daemon (bprd) before making any changes to policies or schedules. This eliminates the possibility of a previously scheduled backup or archive operation invoking the scheduler and reading the configuration while you are making changes.

Use the /usr/openv/netbackup/bin/bpps script to verify that bprd has terminated.

Redefining Retention Levels

To change the retention period associated with any retention level, press **x** (Special Actions) from the main menu and press **r** (View and Display Retention Levels).

```
Level   Period            level   Period
----- -----------         ----- -----------
*  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   infinity
   10  infinity             11  infinity
   12  infinity             13  infinity
   14  infinity             15  infinity
   16  infinity             17  infinity
   18  infinity             19  infinity
   20  infinity             21  infinity
   22  infinity             23  infinity
   24  infinity

Enter 'r' to restore defaults.

'*' indicates the retention is used in a current schedule.

Select the retention level you wish to change. (0-8, 10-24, r, q=quit, s=save)>
```

Note If an asterisk appears in front of a retention level, it indicates that the retention level is referenced in a currently defined schedule and that changing it could have adverse effects on the schedules using it.

▼ To redefine retention levels

1. From the `Special Actions` menu, select **r** (`View and Change Retention Levels`).

2. Select the retention level. A prompt appears for you to specify the units.

   The retention level can be any number listed. You cannot change Level 9. It must remain as infinite (infinite for this application is defined to be 30 years).

3. Specify the units to be used (for example, days).

4. After selecting the units, you are prompted for the period. Specify a period and press **Return**.

   The period may be either infinite (which for this application is defined to be 30 years) or a value from 0 (no retention) up to 30 years.

   When you press **Return**, the screen is updated with the new definition and the following prompt appears (the new definition is not saved yet however).

```
Select the retention level you wish to change. (0-8, 10-24, r, q=quit, s=save)>
```

   - To edit another retention level, specify a number.
   - To restore all the levels to their default values, press **r**.

5. When you are finished changing retention levels, press **q**.

   You will see the following prompt:

```
You have made changes without saving. Do you want to:
q) quit without saving
i) see impact report
r) resume editing

   ENTER CHOICE:
```

   Press **i**.

   You will see a `Building Schedule Report` message. After a short wait, a report appears that summarizes the retention period changes and any possible problems that these changes could cause.

Press **f** to move forward through the report, then press **q** again to receive the following prompt:

```
Do you want to save this definition? (y/n/r=resume editing)>
```

- Press **y** to save the changes and exit the menu.
- Press **n** to discard the changes and return to the Special Actions menu.
- Press **r** to make further changes to retention levels.

Performing Manual Backups

To perform a manual backup of the files associated with any policy, client, and schedule press **m** (`Manual Backups`) on the `bpadm` main menu.

```
  Policy: W2
  Client:<ALL>
Schedule:w2_daily_incr (Incremental)

Manual Backups
--------------
i) Initiate Backup
b) Browse Policies Forward
r) Browse Policies Reverse
s) Browse Schedules
c) Browse Client Workstations
e) Enter Policy/Client/Schedule...
h) Help
q) Quit Menu

   ENTER CHOICE:
```

▼ To perform manual backups

Choose the method in step 1 or 2 to select the policy, client, and schedule for a manual backup; then complete step 3.

1. Press **e** (`Enter Policy/Client/Schedule`) and specify your policy, client, and schedule.

2. Press **b** (`Browse Policies Forward`) until the `Policy` line at the top of the screen shows the name you want.

a. To select either a single client or all clients, press **c** (`Browse Client Workstations`) until the name of the desired client (or `ALL` for all clients) appears on the `Client` line at the top of the screen.

b. To select the schedule or schedules, press **s** (`Browse Schedules`) until the name of the schedule appears on the `Schedule` line at the top of the screen (you cannot do manual backups of user-directed schedules).

3. To start the backup, press **i** (`Initiate Backup`).

Backing Up the NetBackup Databases (Catalogs)

Press **b** (`Backup Databases`) while viewing the `Special Actions` menu to display options for backing up the NetBackup internal databases (also called catalogs).

```
       Backup When: never - must be manually initiated
Output Destination: SCREEN

Backup Databases
-----------------
m)  Modify DB Backup Settings...
d)  Delete DB Backup Media ID...
b)  Backup DB Now...

a)  Add DB Backup File Path...
r)  Remove DB Backup File Path...

l)  List/Display DB Backup Settings
o)  Output Destination  (SCREEN or FILE)
h)  Help
q)  Quit Menu

   ENTER CHOICE:
```

There are two information lines above the menu.

- `Backup When` shows how often the current database backup settings cause the NetBackup databases to be automatically backed up. The three possible values follow:
  - `never - must be manually initiated`
  - `after each backup schedule`
  - `after any successful backup/archive`

  "Modifying Database Backup Settings" on page 226 explains these settings.

- `Output Destination` determines where `bpadm` sends the output of a `List/Display DB Backup Settings` selection. If the word `SCREEN` appears on this line, the output appears on your terminal screen. If a file path appears (for example, `/tmp/bp_db_backup`), the output goes to that file. You can change the output setting by using the **o** option.

The following procedures explain how to use the options while viewing the `Backup Databases` menu.

Caution Before Backing up NetBackup databases, read the precautions listed under "Important Precautions to Observe" on page 151.

Listing Database Backup Settings

To list the current settings for backing up the NetBackup internal databases (also called catalogs), press **1** while viewing the `Backup Databases` menu. "List DB Backup Fields" on page 224 defines the information on the resulting screen.

```
Frequency of DB Backup:  after each successful backup session

Server: bunny
Sequence # 1    Last Media Used: AA0018

Written                 Allocated            Type   Density  Media
-------------------     -------------------  ----   -------  -----
1  11/23/2003 18:30:15  11/11/2003 09:33:45  RMedia odiskwm  AA0016
2  11/24/2003 13:06:33  11/11/2003 09:33:45  RMedia odiskwm  AA0018

Paths Included:
   bunny:/usr/openv/netbackup/db
   bunny:/usr/openv/volmgr/database
   bunny:/usr/openv/var
   bunny.vrt.ov.com:/usr/openv/netbackup/db
   bunny.vrt.ov.com:/usr/openv/volmgr/database

(B)ack  (F)orward  (U)p  (D)own  (Q)uit
```

List DB Backup Fields

Field	Description
`Frequency`	How often the current database backup settings cause the NetBackup scheduler to automatically backup the databases. The paths for these databases are listed under `Paths Included`. The three possibilities follow: - `never - must be manually initiated` - `after each successful backup schedule` - `after any successful backup/archive` See "Modifying Database Backup Settings" on page 226 for option descriptions.
`Server`	NetBackup server with the database.
`Sequence #`	This value currently cannot be changed and is always `1`.
`Last Media Used`	Path (for disk) or media id (for removable or robotic media) that was used to store the last database backup. This path or media ID is one of the two listed, unless you changed media since the last backup. For example, assume `AA0018` has been used many times and you want to start using a different tape. Press **m** (`Modify DB Backup Settings)` to set the media ID to another value, such as `AA0019`. The change erases `AA0018` from line 2 and replaces it with `AA0019`. The `Last Media Used` field shows `AA0018` until after the next database backup.
`1` and `2`	The two media IDs that you assign for use in database backups. If you assign both IDs, NetBackup alternates between them, always using the one that was not used for the previous backup (based on the time in the Written column). If 1 or 2 are removable or robotic type media (see Type below), they must be in the *NetBackup* media pool in Media Manager's volume database. Their media IDs, however, cannot be among those that NetBackup uses for backup or archive images.
`Written`	Date and time the media was last used and is *never* if it has not been written.
`Allocated`	If the Type column indicates that the media is removable or robotic (RMedia), the Allocated column shows the date and time the media was assigned as a NetBackup database backup tape. If the Type column indicates that the media is disk, the Allocated column shows *n/a* because an assignment is not done for disk.
`Type`	Type of media that this media ID represents and is either RMedia (removable or robotic) or Disk.

List DB Backup Fields (continued)

Field	Description
`Density`	Empty if the media type is disk. Otherwise, it shows the density of the media for this ID.
`Media`	Media ID (if removable or robotic media) or path (if disk) of the assigned media.
`Paths Included`	Paths for the databases you are backing up.

Modifying Database Backup Settings

To modify current settings or initially configure the media and other settings for backing up the NetBackup internal databases (also called catalogs), press **m** while viewing the `Backup Databases` menu and follow the prompts.

Caution If you modify any information regarding a media ID previously used for backups, the `Written` date and time for this media ID is overwritten in the database.The contents of the media itself is not destroyed unless it is used again.

For example, assume you change to a different media ID in order to make an extra copy of the databases. When you change to the new media ID, NetBackup replaces the old ID with the new ID and no longer tracks the old ID in its database. This results in the media associated with old ID being made available for reassignment by Media Manager.

1. From the `Backup Databases` menu, select **m** to specify when you want database backups to occur. The choices follow:

   - `1) never - must be manually initiated`: NetBackup will *never* automatically back up its databases. You must do it yourself using the `Backup DB Now` option.
   - `2) after each successful backup schedule`: NetBackup will back up the databases after any regularly scheduled backup sessions that result in the creation of at least one successful backup image. Database backup *does not* occur after a manual or user-directed backup or archive. This is the recommended method.
   - `3) after any successful backup/archive`: NetBackup will back up the databases after any backup session that results in the creation of at least one backup or archive image. This includes scheduled, manual, and user-directed, backups and archives.

   The following example configures NetBackup to back up databases after any successful backup or archive image.

```
Enter Selection [1-3]:  (1) 2 <Return>

Enter Server name:  (bunny.vrt.ov.com) <Return>

Modify ID 1? (y/n): y

   Storage Unit Type Selections:
     1) Disk
     2) Media Manager
```

```
    Enter Type [1-2]:  (1) <Return>

    Enter ID (path): (/opt/openv/netbackup/catalog/) <Return>

Modify ID 2? (y/n): y

    Storage Unit Type Selections:
      1) Disk
      2) Media Manager
    Enter Type [1-2]: 2 <Return>

            Density Selections
            1) 4mm - 4mm Cartridge
            2) 8mm - 8mm Cartridge
            3) 8mm2 - 8mm Cartridge 2
            4) 8mm3 - 8mm Cartridge 3
            5) dlt - DLT Cartridge
            6) dlt2 - DLT Cartridge 2
            7) dlt3 - DLT Cartridge 3
            8) dtf - DTF Cartridge
            9) hcart - 1/2 Inch Cartridge
           10) hcart2 - 1/2 Inch Cartridge 2
           11) hcart3 - 1/2 Inch Cartridge 3
           12) odiskwm - Optical Disk Write-Many
           13) odiskwo - Optical Disk Write-Once
           14) qscsi - 1/4 Inch Cartridge
           Enter Selection [1-14]: 5 <Return>

            Enter ID (media ID): RR1005 <Return>

    Make change now? (y/n): y
```

2. Specify the server to which these backups will be sent.

   The default is the current value shown in parentheses after the `Enter Server Name` prompt. During initial configuration, the default is always the master server.

   If you are changing the destination to a media server, ensure that the server has been previously configured (that is, named in the bp.conf file on the master server when you started bprd and `bpdbm`).

   Also, if you are backing up to a media server, do not forget to modify the database-backup paths for the master server as explained in step 7.

3. Specify whether you want to modify the first of the two available media IDs (`ID 1`).

   - Press **n** to leave the media ID unchanged, then go to step 5.

- Press **y** to change the ID, then go to step 4.

Caution A database backup *does NOT* span a tape volume. All the backup data must fit on one tape. Therefore, it is ***extremely*** important for the administrator to select a media type that can hold all the data to be backed up. The size requirement is dependent on the size of the databases. NetBackup notifies you if the backup fails.

4. Select the storage unit type (the number in parentheses shows the current type).

- Press **1** for Disk type and specify the path to which you want to write the database backup. This should be to a subdirectory. NetBackup creates the path if it does not exist and produces an error if the path exists and is a file rather than a directory.

Note If the path already exists, the error NetBackup reports occurs when the backup is done, *not* when you specify the path.

- Press **2** for a Removable or Robotic type storage unit and select the density (5 in the example).

  Specify the media ID (volume serial number) of the media you want to use.

5. Specify whether you want to modify the second media ID (`ID 2`). If you answer **y**, you are prompted as shown for media `ID 1` in step 3.

6. Specify whether you want to make the changes:

- Press **y** to change the configuration.
- Press **n** to abort the operation and leave the configuration unchanged.

Either choice returns you to the `Backup Databases` menu.

7. If you are backing up the databases to a media server (see step 2), modify the database-backup paths for the master server as follows:

a. Remove each database-backup path for the master server by using the `Removing Database Backup File Paths` option on the `Backup Databases` menu.

b. To add each database-backup path for the master server again, press **a** (`Add DB Backup File Path`) while viewing the `Backup Databases` menu.

When you add the paths again, be certain to specify them as follows:

```
master_name:database_backup_path
```

For example, if the platform is named `bunny`, the paths are as follows:

```
bunny:/usr/openv/netbackup/db
bunny:/usr/openv/volmgr/database
```

Deleting Database Backup Media ID

To delete a media ID from those used for backing up the NetBackup internal databases (also called catalogs), press **d** at the `Backup Databases` menu and follow the prompts, as follows:

```
Delete ID 1 (AA0016)? (y/n): n

Delete ID 2 (AA0018)? (y/n): y

Are you sure you want to delete ID2? (y/n): y
```

Performing Manual Database Backups

To manually start an immediate backup of the NetBackup internal databases (also called catalogs), press **b** (`Backup DB Now`) while viewing the `Database Management` menu.

If you specify this selection, the following prompt appears:

```
WARNING: Backing up the database may take a while.
Are you sure you want to continue? (y/n):
```

Note If the media ID used for the database backup is not in a robot, you get a mount request for that media ID. If the mount request is not honored, a manual database backup must wait for the mount before proceeding. A scheduler-driven database backup must also wait for the mount and, because the scheduler is waiting, all other backups and archives must also wait until the database backup is complete.

- Press **y** to start the database backup. NetBackup uses the least recently used of the two media IDs you have assigned for backups. You must wait for completion of the backup to regain control of your terminal session.
- Press **n** to abort the operation.

Adding Database Backup File Paths

To add database-backup paths, press **a** while viewing the `Backup Databases` menu. This option lets you add NetBackup internal database files (also called catalogs) to the list of files that you back up. In some cases, you will use this option to make additions, and in

other cases, you will use it to change existing paths. For example, if you back up your databases to a media server, you use this option to add the new path specifications for the master server.

```
Adding new DB backup file paths (<ESC> to abort, Blank Line to End)
-----------------------------------------------------
Enter File Path:elk:/usr/openv/netbackup/db/media
Enter File Path:elk:/usr/openv/volmgr/database/ltidevs
Enter File Path:elk:/usr/openv/volmgr/database/robotic_def
Enter File Path: <Return>

Proceed with the change? (y/n): y
```

▼ To add database backup paths

1. Provide the file paths at the `Enter File Path` prompt using one of the following formats:
   - For master-server databases that you are backing up to the master server, provide the file path, as in `/usr/openv/netbackup/db` or `/usr/openv/volmgr/database`
   - For master-server databases that you are backing up to a media server, use *master_name:file_path*, as in the following example for a master server named bunny:

     ```
     bunny:/usr/openv/netbackup/db
     bunny:/usr/openv/volmgr/database
     ```

   - For media-server databases, use *server_name:file_path*, as in the following example for a media server named elk that does not have a volume database:

     ```
     elk:/usr/openv/netbackup/db/media
     elk:/usr/openv/volmgr/database/ltidevs
     elk:/usr/openv/volmgr/database/robotic_def
     ```

2. To end your list of absolute or full file path entries, press **Return**. You will see the following prompt:

   ```
   Proceed with the change? (y/n):
   ```

3. To confirm your entries, press **y**. To abort the operation and leave the configuration unchanged, press **n**.

Removing Database Backup File Paths

To remove database-backup file paths (also called catalog-backup file paths), press **r** while viewing the `Backup Databases` menu. The follow example shows how to delete the media server `elk`:

```
Do you want to remove /usr/openv/netbackup/db? (y/n): n
Do you want to remove /usr/openv/volmgr/database? (y/n): n
Do you want to remove elk:/usr/openv/netbackup/db/media: y
Deleting elk:/usr/openv/netbackup/db/media.....

Proceed with the change? (y/n): y
```

This option lets you delete server database files from the list of files that you back up. In some cases, the removal will be permanent and in other cases it will be part of a change. For example, if you back up your databases to a media server, you use this option to delete the old path specifications for the master server and then add the new path by using the `Add DB Backup File Path` option.

Reference Topics 5

The topics in this chapter provide additional information about various aspects of NetBackup configuration and management.

- "Rules for Using Host Names in NetBackup" on page 234
- "Terminal Configuration on UNIX" on page 238
- "Reading Backup Images with tar" on page 241
- "Factors Affecting Backup Time" on page 244
- "Determining NetBackup Transfer Rate" on page 246
- "How NetBackup Builds Its Automatic Backup Worklist" on page 249
- "Guidelines for Setting Retention Periods" on page 252
- "Guidelines for Setting Backup Frequency" on page 253
- "Determining Backup Media Requirements" on page 253
- "Planning Worksheets" on page 255

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 113.)

Qualifying Host Names

A major consideration when configuring host names is the extent to which you qualify them. In many cases, using the short host name of a computer 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`.

The following two discussions provide more information by explaining:

- How NetBackup uses host names
- How to update NetBackup for client host name changes

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.

Server and Client Name on UNIX Servers and Clients

On both UNIX servers and clients, the `SERVER` entries in the `bp.conf` file define the NetBackup servers that are allowed access. The first `SERVER` entry identifies the master server and it is to this server that client requests are made. For this reason, the `SERVER` name must be one by which all clients can connect to the server.

If more than one `SERVER` entry exists, the additional entries identify other NetBackup servers that can initiate scheduled backups on the client. The `bp.conf` file must have multiple `SERVER` entries if any remote media servers are configured. The NetBackup Request daemon (`bprd`) and NetBackup Database Manager daemon (`bpdbm`) do not run on any server other than a master.

When a client makes a list or restore request to the server, the NetBackup client name, as specified on the client, is used to determine whether to allow the operation. The client name used is usually the `CLIENT_NAME` from the `bp.conf` file of the client, or the actual

host name of the client if not in the `bp.conf` file. In the case of alternate client restores, however, the name can also be a name specified through the user interface or with a parameter on the `bprestore` command.

For a list or restore request to be successful, the NetBackup client name must match the name that is specified for the client in the NetBackup configuration on the server. The only exception to this rule is if the server is configured to allow alternate client restores.

Host Names on Windows Servers and PC Clients

Windows NetBackup servers and clients also have `SERVER` and `CLIENT_NAME` settings. On these systems, specify this through the NetBackup Administration Console.

Policy Configuration

The host name that you specify for a client when adding it to a policy is called the *configured name* of the client, and is the client's host name as it appears in the NetBackup configuration. NetBackup also adds a `CLIENT_NAME` entry to a UNIX client's `bp.conf` file when software is first installed on the client and sets the entry to match the configured name.

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 separate file 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 media 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.)

Catalog Backup Information

Applies to NetBackup Enterprise Server only.

If you configure media servers and include catalog files from the media server in your NetBackup catalog backups, qualify the host name portion of the media server's catalog file path to the extent necessary to allow the master server to make a connection to the media server.

How to Update NetBackup After Host Name Changes

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.

Follow these steps to update the NetBackup configuration if a client's host name is changed.

1. On the master server:
   - Delete the client's old name from all policies in which it exists and add the client's new name to those policies. You do not have to reinstall NetBackup software on the client. The client also still has access to all previous backups.
   - Create a symbolic link from the client's old image directory to its new image directory. For example,

     ```
     cd /usr/openv/netbackup/db/images
     ln -s old_client_name new_client_name
     ```

2. On the client:
   - On PC clients, you can change the client name setting either through the user interface or in a configuration file. (See the client *User's Guide*.)
   - On UNIX clients, change the `CLIENT_NAME` value in the `bp.conf` file to the new name.

Note If users on UNIX clients have a `bp.conf` file in their `$HOME` directory, they must change `CLIENT_NAME` in that file to the new name.

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(2)` 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(2)` 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 in the altnames directory on the master server in order to force the desired translation of NetBackup client host names.

`/usr/openv/netbackup/db/altnames/host.xlate`

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(2)` 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(2)` returned `danr`.
- The master server's network services `gethostbyname(2)` 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.

Terminal Configuration on UNIX

The following provides information that will be useful in setting up and resolving problems with your UNIX displays.

Modifying the XKeysymDB File

The X interface programs depend on the `/usr/lib/X11/XKeysymDB` file to correctly use editing keystrokes such as backspace and delete. The NetBackup installation procedures are designed to install a nominal version of this file if it does not already exist. It does not, however, overwrite any existing version of the file, thereby ensuring that user-customized versions of XKeysymDB are not destroyed.

Sun systems typically already have a version of `XKeysymDB` that does not define some editing keys. Analyze the current content of your `XKeysymDB` file and compare it to the NetBackup standard version which is in the `/usr/openv/netbackup/bin/XKeysymDB` file on NetBackup servers. Then append the NetBackup version onto the existing one, or replace the existing one with the NetBackup version, or edit the existing version to achieve your preferred keyboard support.

Modifying the terminfo File

The following discussion provides information on `terminfo` files that will be useful in resolving terminal problems with the character-based interfaces.

To modify a `terminfo` source file, start with an existing source file. If one is not readily available, obtain one by using `infocmp(1)` and `infocmp(8)` to print out `terminfo(4)` descriptions. For example:

```
infocmp term-type  > /tmp/terminfo.file
```

The `terminfo(4)` and `terminfo(5)` man pages show the symbols that are valid for a `terminfo` source file, along with explanations of their use.

To find the actual character sequence sent by special keys that can subsequently be used in a `terminfo` source file, enter the following at the command line prompt:

```
stty -echo; cat -v; stty echo
```

and then type the special keys, following each with a carriage return. Type **CTRL+D** when you are finished. Another possible way to capture the character sequence is to type **CTRL+V** while in the insert mode of `vi`. This causes `vi` to echo the character sequence generated by the next keypress.

Once you have a suitable `terminfo` source file, use the following steps to install the file:

1. Move the `terminfo` source file to the desired machine.

2. If this `terminfo` change is not to be globalized for all machine users, make a directory to contain the compiled `terminfo` files and set an environment variable to affect the `terminfo` search path:

   ```
   mkdir ~/terminfo
   setenv TERMINFO ~/terminfo
   ```

   Note that if the `terminfo` is to be used by all users on this machine you must run these commands as root in order to have the correct permissions to install the compiled `terminfo` entries.

3. Use `tic(1)` or `tic(8)` to compile the `terminfo` file:

   ```
   tic /tmp/terminfo.file
   ```

To make use of the new `terminfo` file use one of the following commands:

```
setenv TERM new_terminfo
set term=new_terminfo
```

Changing X Resources for xbp

The X-Windows-based user interface program has enough space in its text fields to accommodate user-selected fonts up to the 10x20 size. The windows can also fit on a 1024x768 screen with some room for window manager borders.

The `xbp` program uses default resources for your X server. You might want to change this default if it is not satisfactory to you. For example, the default font might be too small for comfortable viewing. A font that has proportional spacing can also be unsatisfactory because proportional fonts cause column misalignment on certain fields that have columnar text.

For an explanation on how to specify X resources to force a particular font, look near the end of the `xbp` Tutorial help file. If your X server defaults to proportional fonts and you do not know what font names are available for your system, try the generic font name *fixed*.

Because the default window sizes are small enough to fit on a 1024x768 screen, if you use larger fonts, `xbp`'s *verbose* display mode can force you to use a horizontal scroll bar to see all information. Widening the window at runtime with the window manager may eliminate the scroll bar. You can also change X resources as described in the Tutorial help file to enlarge the default geometry and use a smaller font.

Reading Backup Images with tar

NetBackup uses a modified GNU `tar` for reading backup images. The modified `tar` is located in `/usr/openv/netbackup/bin/tar`. Using the modified `tar`, NetBackup can understand compressed files, sparse files, long pathnames, ACL information. It offers features similar to those in `cpio`.

Although non-NetBackup versions of `tar` can be used to restore files, they provide only limited restore capabilities.

Effects of Using a Non-NetBackup tar

Non-NetBackup versions of `tar` do not supply all of the restore capabilities that the NetBackup `tar` provides, resulting in possible problems.

The following is a list of some effects that a non-NetBackup `tar` may encounter in certain situations:

- Compressed backups cannot be recovered.
- Multiplexed backups cannot be recovered.
- Solaris 9 extended attributes cannot be restored to a client.
- VxFS 4.0 named data streams cannot be restored to a client.
- Backups containing raw partitions cannot be recovered. (Includes FlashBackup images.)
- NDMP client backup images cannot be restored, though NDMP vendors may have tools or utilities which could perform a restore directly from the media.
- Non-NetBackup versions of `tar` may have trouble with sparse files and often skip sparse files.
- HP CDFs are restored with non-NetBackup versions of tar, but the directory is no longer hidden and the name of the directory has a + appended to it.
- If the backup spans more than one piece of media, you must read the fragments from the media and concatenate the fragments to give to `tar`. To accomplish this, the system's `dd` command may be useful.

  Another possibility is to use `tar` on the fragments. This may allow recovery of any file in the backup other than the one that spanned the media.

  Some versions of the HP9000-800 `/bin/tar` command are known to give a *directory checksum error* for the second fragment of a backup that crossed media.
- Some versions of Solaris `tar` will combine the `atime`, `mtime`, and `ctime` strings with the file name and create file paths that are not desirable.

Restoring Files Using a Non-NetBackup tar

The following process explains how to use a non-NetBackup `tar` to read a backup from a NetBackup tape. Most versions of `tar` can read NetBackup-created tapes after using the `mt` command to position to the proper tape location.

This sequence assumes that the media is known to Media Manager and that the tape drive is under the control of Media Manager's.

Before starting, obtain the following information:

- Media id of the tape containing the required backup
- Tape file number of the backup on the tape (see the NetBackup Images on Media report for this tape)
- Tape type/density
- Tape pool

▼ To restore files using a non-NetBackup tar

1. `tpreq -m` *`media_id`* `-a r -d` *`density`* `-p` *`poolname`* `-f /tmp/tape`

   Where:

   `media_id` is the media id of tape containing the backup.

   `density` is the density of the tape.

   `poolname` is the volume pool to which the tape belongs

2. `mt -f /tmp/tape rew`

3. `mt -f /tmp/tape fsf` *`file_#`*

   Where:

   file_# is the tape file number of the backup on tape. Determine the tape file number by checking the NetBackup Images on Media report for the tape.

4. `mt -f /tmp/tape fsr`

5. `/bin/tar -tvfb /tmp/tape` *`blocksize`*

   Where:

   - *`blocksize`* is 64 (assuming that the tape is written with 32K blocks)

6. `tpunmount /tmp/tape`

Notes:

1. This procedure does not work for optical platters.

2. This procedure does not work for compressed backups using NetBackup client software compression.

3. This procedure does not work if the backups were encrypted by NetBackup Encryption. The backups are recoverable, however, the backups will be encrypted and you will not be able to decrypt them.

   To determine if a backup is encrypted, run `tar -t` prior to the recovery. The output for an encrypted backup will be similar to the following:

   ```
   erw-r--r-- root/other Nov 14 15:59 1997 .EnCryYpTiOn.388
   -rw-r--r-- root/other Oct 30 11:14 1997 /etc/group.10-30
   ```

   Where the e at the beginning of line one indicates that the backup is encrypted. There will also be other messages if you attempt the recovery.

4. This procedure will not work for multiplexed backup tapes.

5. This procedure will not work as-is if the backup you desire spans tapes.

6. This procedure will not work on the Solaris platform. You cannot use `/usr/sbin/tar` on Solaris to read NetBackup's because that `tar` command uses the `ctime` and `atime` fields differently than other `tar` commands.

   When trying to restore using `/usr/sbin/tar`, you will see directories with large numbers being created at the top level. These directories are from the `ctime` and `atime` fields being read as pathnames.

   You can, however, use `/usr/openv/netbackup/bin/tar` or GNU `tar` to read the backups on Solaris platforms.

7. Steps 1 and 6 are optional in a standalone environment. If step 1 is skipped, DOWN the drive, then substitute the `/dev` path of the drive in place of `/tmp/tape` in the other steps. Remember to UP the drive when you are done.

Example

The following example was successful on an HP9000-800 using a DOWNed 4mm standalone drive and the NetBackup `tar`.

```
mt -t /dev/rmt/0hncb rew
mt -t /dev/rmt/0hncb fsf 1
mt -t /dev/rmt/0hncb fsr 1
/usr/openv/netbackup/bin/tar tvfb /dev/rmt/0hncb 64
```

Some platforms require other options on the `tar` command. The following is required on Solaris 2.4:

```
/usr/openv/netbackup/bin/tar -t -v -f /dev/rmt/0hncb -b 64
```

Possible Files Generated By tar

Using any version of tar (including NetBackup-modified `tar`), can generate a number of specially-named files depending on the circumstances of the recovery:

- `@@MaNgLeD.`*nnnn*

  For backups containing pathnames longer than 100 characters, `tar` generates files named `@@MaNgLeD.`*nnnn* that contain the actual file.

- `@@MaNgLeD.`*nnnn*`_Rename`

  `tar` generates another file (`@@MaNgLeD.`*nnnn*`_Rename`) that explains how to rename the `@@MaNgLeD.`*nnnn* files in order to return the files to the correct location.

- `@@MaNgLeD.`*nnnn*`_Symlink`

  For long names of symbolic links, `tar` generates files named `@@MaNgLeD.`*nnnn*`_Symlink`. These files contain descriptions of the symbolic links that need to be made in order to return a link to the correct file.

- For cross-platform ACLs restores, `tar` creates and stores the ACLs in `.SeCuRiTy.`*nnnn* files in the `root` directory. The files can either be deleted or read and the ACLs regenerated by hand to the corresponding files. (See "Restoring Files and Access Control Lists" on page 440.)

- For cross-platform VxFS extent attribute restores, `tar` creates and stores extent attributes in `.ExTeNt.`*nnnn* files in the `root` directory. The files can either be deleted or read and the extent attributes regenerated by hand to the corresponding files.

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, incremental backups are larger.

Transfer Rate

Transfer rate depends on factors such as the following:

- Speed of the backup device. For example, sending backups to a tape having a maximum transfer rate of 800 kilobytes per second normally takes less time than to a tape that transfers at only 400 kilobytes per second (assuming other factors allow taking advantage of the faster transfer rate).
- Available network bandwidth. The available bandwidth is less than the theoretical network bandwidth 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.
- Network configuration can affect performance. For example, in an Ethernet environment, having some machines running full-duplex and some running half-duplex will significantly reduce throughput.

See “Determining NetBackup Transfer Rate” on page 246 for methods to compute the transfer rate for your clients.

Compression

If you use software compression, it often multiplies the backup time by a factor of two or three for a given set of data.

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

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 rate 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
04/28/03 23:10:37 windows giskard begin writing backup
                  id giskard_0767592458, fragment 1 to
                  media id TL8033 on device 1 . . .
04/29/03 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:                04/28/03 23:07:38
Elapsed Time:               001:27:32
Expiration Time:            05/05/03 23:07:38
Compressed:                 no
Kilobytes:                  1161824
Number of Files:            78210
```

The following three rates were compiled using the backup data from the example reports above:

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

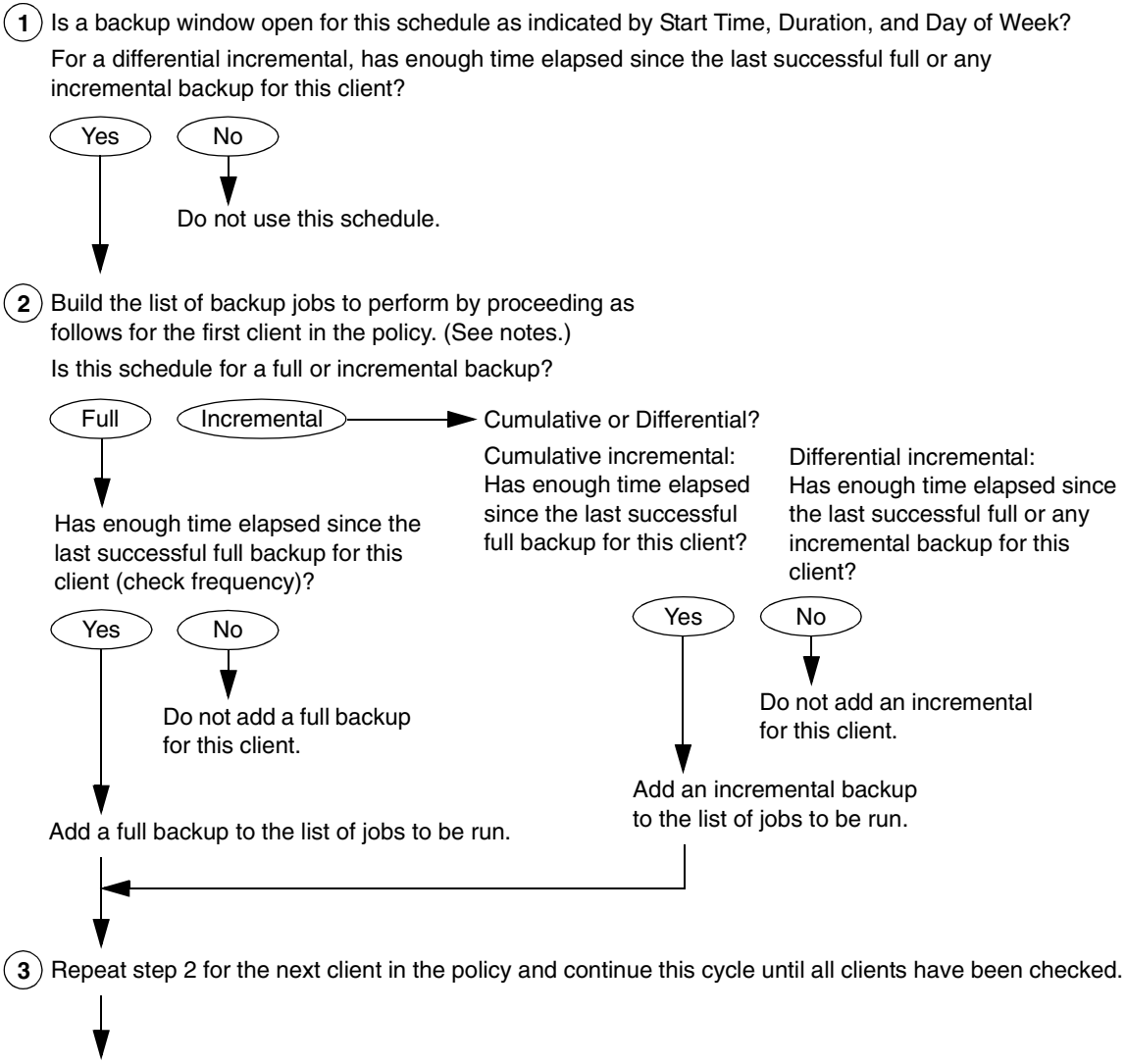
1161824 Kbytes/5252 = 221.216 Kbytes per second

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 to determine whether or not to add the client backups for that schedule to the worklist (queue). The following figure shows this process:



NOTES:

– If more than one schedule for this policy is due for a client, the backups from the schedule that is backed up least often are added first.

– If the NetBackup scheduler encounters a backup policy with two schedules (one full, one incremental) that are each due to run, are each within their defined backup window, and are each configured with the same frequency value, the schedule that is alphabetically first will be chosen to run.

– Cumulative and differential incremental backups have the same priority.

Prioritizing the Worklist

The worklist typically contains jobs from different policies and schedules. NetBackup checks for the following items when determining the order in which to run the backups that are in the worklist:

1. If multiplexing is enabled, a job will join an existing multiplexed group if allowed, even if a job of higher priority is on the worklist.

2. Highest priority backup as determined by the policy **Job Priority** setting.

   Backup jobs from the policy with the highest priority run 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.

3. 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.

4. 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 incremental backups in addition to full backups for as long as you need the data. If incremental backups only track work in progress toward monthly reports, then you can probably expire the incremental backups 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 offsite 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 offsite 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 offsite storage facility. To restore the data, you get the media from offsite storage (a total directory or disk restore with incremental backups requires the last full backup plus all incremental backups).
- You can also configure an extra set of schedules for the backups to create duplicates for offsite storage.

Regardless of the method you use for offsite 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 incremental backups that record the changes since the last incremental or full backup. This conserves resources because incremental backups use less storage and take less time to perform than full backups.

Full backups usually occur less frequently than incremental backups but should occur often enough to avoid accumulating too many consecutive incremental backups. Too many incremental backups between full backups increases restoration time because of the effort required to merge those incremental backups 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 incremental backups 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 approximately half of the files in a policy selection list change frequently enough to require a full backup every week, but the remaining files 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 or to consider using synthetic backups.

Determining Backup Media Requirements

To assist you in determining how much media is available, NetBackup provides:

- The NetBackup Media Summary report, which lists the active and nonactive media that is available to a server.

- The `available_media` script in the `/usr/openv/netbackup/bin/goodies` directory, which lists all the media IDs that are available on the server where you run the script.

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 offsite 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 and the results from running the `available_media` script to verify that enough media IDs and disk space are available.

For long term planning, review the following considerations:

- How long you want to retain the data. A related consideration is that all backups on a given tape or optical disk have the same retention level unless the **Allow Multiple Retentions per Media** property is enabled. If not enabled, additional media is required for each different retention level.
- Duplicates for offsite 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 incremental backups) 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.

Media Catalog

NetBackup keeps a media catalog with information that correlates backups to the volumes where the backups are stored. Each NetBackup server maintains a media catalog for the storage units attached to that server.

During installation, the media catalog is created in the `/usr/openv/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).

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 the *NetBackup System Administrator's Guide, Volume I* for information about the items on the worksheets.

Policies Planning Worksheet (Sheet 1)

Policy Name	
Clients	
Selection List	
Policy type	
Policy storage unit	Label:
Policy volume pool	Label:
☐ Limit jobs per policy	Value:
Job priority	
Keyword phrase	
☐ Active	Date
☐ 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)	
Selection List /usr, /home, /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	Date *Current date*
☐ 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 venus (Windows), pluto (Windows), saturn (Windows)	
Selection 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	Date *Current date*
☐ 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				

NetBackup Notify Scripts 6

Note Before using the notify scripts, ensure that they are executable by *other*. Do this by running `chmod 755` *script_name*, where *script_name* is the name of the script.

NetBackup uses 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`

`backup_exit_notify`

`dbbackup_notify`

`diskfull_notify`

`restore_notify`

`session_notify`

`session_start_notify`

`userreq_notify`

Scripts that run on clients:

`bpstart_notify.`

`bpend_notify.`

* On Windows 2000 or NT clients, `bpstart_notify.bat` and `bpend_notify.bat` scripts are not supplied with the software. You must create them on the client following the criteria in "bpstart_notify.bat (Microsoft Windows clients only)" on page 271 and "bpend_notify.bat (Microsoft Windows clients only)" on page 276.

The scripts that run on a server are installed during NetBackup server installation and are in:

`/usr/openv/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

```
/usr/openv/netbackup/bin/goodies
```

on the server to

```
/usr/openv/netbackup/bin
```

on the client.

For further information, refer to the comments in the scripts.

Caution *Applies to NetBackup Enterprise Server only.*
If you use either the `bpstart_notify` or `bpend_notify` scripts, do not include commands that write to stdout. If you do, NetBackup sends this output to the server as part of the backup and the resulting backup can abort with an error message pertaining to block sizes. Also, ensure that all commands in the scripts are appropriate to the client platform. For example, the `-s` parameter is invalid for the UNIX `mail` command on some UNIX platforms and its use can cause data to be written to stdout or stderr, resulting in the same problem noted above.

backup_notify

The `backup_notify` 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 bptm bilbo_0695316589
```

Note *Applies to NetBackup Enterprise Server only.*
If NetBackup backed up files to a UNIX disk storage unit that is being managed by Storage Migrator, the `backup_notify` script notifies Storage Migrator to perform migration as quickly as possible. The released script does not, however, have commands to force a backup of the managed file system after NetBackup has stored its backups. To back up the managed file system, modify the script as necessary to meet site requirements for backup.

backup_exit_notify

The `backup_exit_notify` 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`
`exitstatus`	Exit code for the entire backup job.

For example:

```
backup_exit_notify freddie production fulls FULL 0
backup_exit_notify danr production incrementals INCR 73
```

bpstart_notify (UNIX clients only)

On UNIX clients, NetBackup calls the `bpstart_notify` script each time the client starts a backup or archive operation. To use this script, copy

```
/usr/openv/netbackup/bin/goodies/bpstart_notify
```

from the server to

```
/usr/openv/netbackup/bin/
```

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 2004
```

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`.

`RESTARTED` can be used for checkpointed restarts or checkpointed backup jobs. A value of 0 indicates that the job was not resumed. (For example, upon first initiation.) A value of 1 indicates that the job was resumed.

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. To use this script, copy:

install_path`\NetBackup\bin\goodies\bpstart_notify.bat`

from the server to the client, in the same directory as the NetBackup client binaries:

install_path`\NetBackup\bin\goodies`

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 `bpstart_notify.bat`

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 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.

Parameter	Description
%4	One of the following: FULL, INCR, CINC, UBAK, UARC
%5	Status of the operation is always 0 for bpstart_notify.
%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.

For a UNIX client, if you need notification whenever the client completes a backup or archive operation, copy

```
/usr/openv/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 pol_1 fulls FULL 0
bpend_notify danr pol_1 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 2004
```

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.

FINISHED can be used for checkpointed restarts of backup jobs. A value of 0 indicates that the client was not finished sending all of the data. A value of 1 indicates that the client was finished sending all the of data.

bpend_notify.bat (Microsoft Windows clients only)

For Windows 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\goodies

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 bpend_notify.bat

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

The dbbackup_notify 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 DISK /disk1/bpsync1 SUCCESS
dbbackup_notify OPTICAL AA0001 FAIL
dbbackup_notify 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.

Note *Applies to NetBackup Enterprise Server only.*
If the NetBackup catalog files are backed up to a UNIX disk storage unit that is being managed by Storage Migrator, the dbbackup_notify script notifies Storage Migrator to perform migration as quickly as possible. The script does not, however, have commands to force Storage Migrator to back up its own catalog after a backup of the NetBackup catalog. You must modify the script to meet site requirements for backup of the Storage Migrator catalog.

diskfull_notify

The `diskfull_notify` 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 bpdm /disk1/images/host_08193531_c1_F1
```

restore_notify

Note *Applies to NetBackup Enterprise Server only.*
If the files are restored to a UNIX disk storage unit that is being managed by Storage Migrator, the `restore_notify` script notifies Storage Migrator to perform migration as quickly as possible after the restore is complete.

The `restore_notify` 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 name or path.
`operation`	One of the following: `restore`, `verify`, `duplication`, `import`

For example:

```
restore_notify bptm bilbo_0695316589 duplication
```

session_notify

The `session_notify` 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

The `session_start_notify` 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

The `userreq_notify` 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 backup mercury jdoe
userreq_notify archive mercury jdoe
userreq_notify manual_backup mercury jdoe
userreq_notify restore mercury jdoe
```

```
userreq_notify list mercury jdoe
```

Using NetBackup With AFS 7

This chapter explains how to install, configure, and use NetBackup to back up AFS file servers. (AFS is an acronym for Andrew File System.)

Installation

System Requirements

- AFS file servers that will be NetBackup AFS clients:
  - Solaris 2.6, Solaris 7, HP-UX 11.0, or IBM AIX 4.3.3 platform
  - NetBackup 4.5 or later
  - AFS level 3.6 installed
- NetBackup servers that will be backing up the clients must have NetBackup 4.5 or later installed.

Server and Client Installation

Both the AFS server software and the AFS client software are installed automatically with NetBackup. There are no additional instructions for installing AFS software.

Configuration

To configure backups for NetBackup AFS clients, add an AFS policy to the NetBackup configuration on the master server. Except for the differences mentioned here, the requirements are the same as for other NetBackup policies. To back up files and directories that are not in AFS volumes, create a separate policy.

General Policy Attributes

When selecting the general attributes for the policy, specify AFS as the policy type.

Client List

In the client list, specify the names of the AFS file servers to be backed up. These systems must have NetBackup client and NetBackup AFS software installed.

Backup Selections

In the backup selection list for the AFS policy, specify the AFS volumes and (or) vice partitions to be backed up by the schedules in this policy. The following example shows both volumes and vice partitions:

```
user.abc
/vicepb
/vicepc/user.*
```

In this instance, NetBackup backs up:

- The volume `user.abc`
- All volumes in vice partition `vicepb`
- All volumes in `vicepc` that begin with *user*.

  When the list includes a vice partition, all the volumes in the partition are backed up one at a time.

Note NetBackup supports the maximum AFS 3.6 volume size of 8 GB.

Backup Selection List Directives

The following directives can be in the backup selection list in an AFS policy:

- `CREATE_BACKUP_VOLUMES`

  This directive causes NetBackup to create .backup volumes prior to performing the backup. If a `.backup` volume already exists, NetBackup overwrites it, thus creating a more recent copy.

  Because NetBackup backs up only the .backup copy of AFS volumes, this directive is useful if an automated mechanism is not in place to create .backup copies. Creating `.backup` copies also ensures that the backups include the latest changes.

Caution If an automated mechanism is not in place to create .backup copies, you must include the `CREATE_BACKUP_VOLUMES` directive in the backup selection list or AFS volumes are not backed up.

- `REMOVE_BACKUP_VOLUMES`

  This directive causes NetBackup to remove .backup volumes after performing the backup. The directive removes .backup volumes created using the `CREATE_BACKUP_VOLUMES` directive or created by another mechanism.

- `SKIP_SMALL_VOLUMES`

  This directive allows you to skip small or empty volumes during backups. For example:

  ```
  SKIP_SMALL_VOLUMES=5
  ```

  (do not include spaces on either side of the = sign)

  In this example, NetBackup skips volumes ≤ 5 KB. You can specify any number for the volume size.

  If you do not specify a number, the size defaults to 2 KB. For example:

  ```
  SKIP_SMALL_VOLUMES
  ```

  The following rules also apply to the directives:

  - Directives must be all upper case.
  - Directives can be anywhere in the backup selection list but it is best to place directives at the top. For example:

    ```
    CREATE_BACKUP_VOLUMES
    SKIP_SMALL_VOLUMES
    /user.abc
    /vicepb
    ```

Regular Expressions

NetBackup supports regular expressions in backup selection list entries. These are useful if you want to:

- Add or move volumes without having to change the backup selection list.
- Add vice partitions without having to change the backup selection list.
- Split volumes and (or) vice partitions on AFS file servers into groups that can be backed up by separate policies. This allows concurrent backups or multiplexing.

The following examples use regular expressions:

```
user.[a-m]*
/vicep[a-c]
```

Exclude and Include Lists

Exclude lists can be created on the client in order to exclude certain specific volumes from automatic backups. An exclude list cannot contain vice partitions but it can contain individual volumes within a vice partition.

An include list adds back volumes specified in the exclude list. For example, if a range of volumes is excluded, the include list can add back specific volumes within the range.

Backups and Restores

Backups

Note You cannot perform user backups or archives of AFS volumes.

Automatic Backup

The most convenient way to back up NetBackup for AFS clients is to configure an AFS policy and set up schedules for automatic, unattended backups.

Manual Backup

The administrator on the master server can use the NetBackup Administration Console to manually run a backup for an AFS policy. For information about manual backups, see "Performing Manual Backups" on page 197 in *NetBackup System Administrator's Guide for UNIX, Volume I*.

Restores

All restores must be performed by the administrator either on the NetBackup AFS client or the master server. Restores are performed on the basis of volumes. To restore a vice partition, the administrator must select all the volumes in that partition.

Caution If you select the **Overwrite Existing Files** option, the volumes are overwritten and all changes or files created since the last backup are lost.

Restore From the NetBackup for AFS Client

An administrator on a NetBackup AFS client (AFS file server) can use the NetBackup Backup, Archive, and Restore interface to restore volumes to that client. It is also possible to perform a redirected restore. A redirected restore will restore a volume to another volume or vice partition.

Restore From the NetBackup Master Server

The administrator can use the NetBackup Backup, Archive, and Restore interface on the master server to restore volumes to the same NetBackup AFS client (AFS file server) or do a redirected restore. This is called a server-directed restore. For instructions, see the *NetBackup User's Guide for UNIX*.

Notes About Restores

- On UNIX, the NetBackup Backup, Archive, and Restore user interface (`jbpSA`), provides a convenient mechanism for specifying an alternate name for a volume and (or) vice partition. Specifying an alternate volume name prevents an existing volume from being overwritten by the restore.
- If the administrator does not specify **Overwrite Existing Files** or an alternate name for the volume, then NetBackup adds an *R* to the name of the restored volume as follows:
  - If the volume name is less than 22 characters long, NetBackup adds a leading *R* to the name of the restored volume. For example:

    If the volume name is

    ```
    /AFS/shark/vicepa/user.abc
    ```

    The restored name is

    ```
    /AFS/shark/vicepa/Ruser.abc
    ```
  - If the volume name is 22 characters long (maximum allowable length for a volume name), the first character of the original volume name is replaced with an *R*. For example:

    If the volume name is

    ```
    /AFS/shark/vicepa/engineering.documents1
    ```

The restored name is

```
/AFS/shark/vicepa/Rngineering.documents1
```

- If you are restoring to an alternate path and specify an existing volume, you must select the **Overwrite Existing Files** option for the restore to succeed. In this case, the entire volume is overwritten. If you do not select the **Overwrite Existing Files** option, the restore fails.
- When restoring a volume to an alternate vice partition, the vice partition must exist or the restore fails.

Troubleshooting

The following sections provide tips and information for troubleshooting problems with NetBackup for AFS. See the *NetBackup Troubleshooting Guide for UNIX and Windows*for overall troubleshooting information.

Troubleshooting Backups

To increase the level of detail in the logs:

- Add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file on the NetBackup for AFS client.
- Create the following debug log directory on the NetBackup for AFS client:

  ```
  /usr/openv/netbackup/logs/bpbkar
  ```

  If the AFS backup terminates with a status code of 9 (an extension package is needed, but was not installed), it means that NetBackup AFS client software was not properly installed on the client.

  If the AFS backup terminates with a status code of 78 (`afs/dfs` command failed), it indicates an AFS `vos` command failure. The NetBackup Problems Report provides additional information on why the command failed. The `bpbkar` debug log shows the command that was run. You can run the `vos` command manually to attempt to duplicate the problem.

  Also, examine the `/usr/openv/netbackup/listvol` file on the NetBackup client for irregularities. The `vos listvol` command can be very demanding on system resources so NetBackup caches the output of the `vos listvol` command in this file. If the cached `listvol` file was created less than four hours prior to the backup, NetBackup uses it to obtain the list of volumes instead of running another `vos listvol` command.

Troubleshooting Restores

If the restore of an AFS volume fails, check the restore process log for additional information. If a `vos restore` command failure is indicated, create a `/usr/openv/netbackup/logs/tar` debug log directory, retry the operation, and check the resulting log to see that the `vos restore` command was run.

Intelligent Disaster Recovery 8

Intelligent Disaster Recovery (IDR) for Windows is a fully-automated disaster recovery solution that allows you to recover your Windows computers quickly and efficiently after a disaster. The IDR wizards guide you in preparing for disaster recovery and in recovering your computer to its pre-disaster state.

The information about protected computers applies to all Windows server types that NetBackup supports unless otherwise specified.

This chapter contains the following sections:

- "Requirements for IDR" on page 292 explains the prerequisites for using IDR.
- "Overview of IDR Use" on page 293 explains the main steps involved in using the disaster recovery software.
- "About the DR Files" on page 294 introduces the DR (Disaster Recovery) files and explains their importance in disaster recovery.
- "Configuring NetBackup Policies for IDR" on page 294 explains how to configure policies that contain clients that are using IDR.
- "Backing Up the System to be Protected" on page 295 explains that you must backup the system before you create the bootable media used in recovery.
- "Creating IDR Media" on page 295 explains how to use this wizard to prepare the bootable media that is used to recover your data.
- "Updating IDR Media" on page 302 explains how and when to update the IDR media so it is always ready when you need it.
- "Recovering Your Computer" on page 305 explains how to perform disaster recovery.
- "Notes on Recovering Specific Platforms" on page 311 provide information on recovering data on specific types of platforms.
- "IDR Frequently Asked Questions" on page 313 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
- Windows Server 2003 (Standard Edition, Enterprise Edition, and Web Edition)

Requirements for IDR

The following are the requirements for IDR:

- NetBackup 5.1 or later must be installed on both the machine that collects the disaster recovery information and the Windows systems that you are going to protect. The NetBackup master server that collects the disaster recovery information can reside on either a Windows or UNIX system.
- The Intelligent Disaster Recovery software must be installed on the Windows systems that you want to protect. IDR software is installed automatically on each Windows system on which NetBackup server or client software is installed. The software is not required and cannot be installed on UNIX systems.
- The NetBackup master server that collects the disaster recovery information must be licensed for IDR.
- The IDR Preparation Wizard can only be used to generate recovery media for systems that have the same version of IDR software installed. For example, the IDR Preparation Wizard running on a NetBackup 5.1 master server cannot generate recovery media for a NetBackup 4.5 client.
- The machine to be protected must be an Intel system running Windows NT 4.0 (with Service Pack 3 or later); Windows 2000; Windows XP; or Windows Server 2003 (Standard Edition, Enterprise Edition, Web Edition).
- At least 40 MB of hard drive space to hold the minimal recovery system on the machine to be protected.
- Sufficient space on the machine to be protected for the data that is being restored.
- Sufficient swap space on the machine to be protected 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 that stores 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 on the machine to be protected 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 service pack to be installed. 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 drive on a protected computer must be supported by Windows. *Windows NT systems*: If the IDR Preparation Wizard detects that the driver on the system being protected is different than the driver on the Windows NT installation CD, you can choose which driver to use. VERITAS recommends that you use the SCSI drivers currently installed on the computer being protected because the drivers on the Windows CD may not be up to date. If you have an IDE hard disk greater than 8 GBs you must use the SCSI driver currently installed on the system.

Overview of IDR Use

Using IDR involves the following steps:

- Installation. The IDR software is installed automatically when NetBackup server or client software for Windows is installed. 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 systems.
- Configuration. On the NetBackup master server, select the **Collect disaster recovery information** general attribute when setting up the policy configuration for protected clients. You can use a NetBackup master server on either a Windows or UNIX system to collect disaster recovery information.
- Backup. An initial full backup must be completed before you create IDR media. Also, you should backup your computer frequently and update the DR files often.
- Preparing the IDR media. The IDR Preparation Wizard guides you through the preparation of media used to recover protected systems.
- Recovery. A Disaster Recovery Wizard guides you through the steps for rebuilding the protected system and then restoring data to that system. The systems to be protected should have their data backed up regularly by NetBackup.

The installation, configuration, backup, and media preparation steps are prerequisites for successfully recovering a Windows system through a network connection to a NetBackup server.

About the DR Files

The disaster recovery (DR) files are mentioned frequently in this chapter and in the screens that you see in the wizards. A DR 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 and the server is configured to collect disaster recovery information, 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.

On the NetBackup master server, the DR files for all clients are stored in the NetBackup catalogs on the server.

Configuring NetBackup Policies for IDR

Set up the policy configuration on the NetBackup master server as follows:

- 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.

- The NetBackup master server that collects disaster recovery information must be licensed for IDR; 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.
- NetBackup 5.1 will collect the DR information from clients that have versions of NetBackup earlier than 5.1. However, you must use the IDR software revision on the client to prepare the bootable media for that client (for example, if the client software is NetBackup 4.5, you must use that version of IDR to prepare the IDR media).
- 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.

Backing Up the System to be Protected

Before you prepare the IDR media, which includes the DR file used in recovery, you must perform at least one full backup of the system to be protected. The NetBackup master server that performs the backup must be configured to collect disaster recovery information. The backup information collected is used when creating the DR file.

You can prepare IDR bootable media if differential or incremental backups have occurred since the full backup.

Ensure that all local drives are backed up, and, for Windows 2000, ensure that System State is backed up.

Ensure that any utility partitions are backed up. Utility partitions are small partitions created on the hard drive, usually by the computer vendor, that may contain system configuration and diagnostic utilities.

Creating IDR Media

The IDR Preparation Wizard guides you in creating the IDR media used in recovery. A set of IDR media includes the following:

- Bootable media used to boot the computer and install and configure the operating system.
- System specific drivers and the Disaster Recovery Wizard.
- The disaster recovery (DR) file.
- For Windows XP and Windows Server 2003 systems, Windows Automated System Recovery files.

To create IDR media, you must have:

- At least one full backup of the system to be protected.
- The Windows installation CD for the version and language installed on the protected system.
- The license key for your Windows 2000, Windows XP, or Windows Server 2003 operating system.
- Administrative privileges for the protected system.
- A device capable of creating bootable media:
  - CD-R drive (CD Recordable CD-ROM)
  - CD-RW drive (CD Rewritable CD-ROM)
  - Diskette drive (IDR does not support bootable diskette media for Windows XP or Windows Server 2003)

More information about media is provided later in this chapter.

You must prepare the media before a disaster. For CD-R or CD-RW, you should 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 306.)

Choosing the Bootable Media

For Windows NT and Windows 2000, the IDR Preparation Wizard can create both bootable diskettes and bootable CD-Recordable (CR-R) or CD-Rewritable (CR-RW) media.

Note IDR does not support bootable diskette media for Windows XP or Windows Server 2003.

When choosing between diskettes and CD-ROM media, consider the following:

- Diskettes work on most systems but require more time for preparation and recovery than CDs.
- Diskettes require the Windows installation CD during recovery.

- Diskettes will hold SCSI driver information for only one computer (because of space limitations). If you want to use one set of diskettes to protect more than one computer, you must choose one computer that represents all the other computers and create bootable media for it. If you have computers with different SCSI drivers, you must create a set of diskettes for each computer with a different driver.
- CDs require less time for preparation and recovery than diskettes.
- CD media has enough space to store SCSI driver information for multiple systems, so you can use a single CD for multiple systems during disaster recovery.
- CD media requires that the computer being protected has BIOS that supports booting from a CD.
- CD media requires CD writing hardware. The computer to be protected does not have to have a CD writer; the IDR Preparation Wizard creates a bootable image that you can write to a CD on any computer that has a CD writer.
- For CD media, third party CD writing software is required if the computer being protected does not have a CD writer or if the IDR Preparation Wizard cannot detect the CD writer attached to the system being protected. The CD hardware and software must be able to write ISO 9660 CD images.
- With both diskettes and CDs, you must prepare separate media for each operating system level and language being protected.

Creating Bootable Diskettes

The IDR Preparation Wizard guides you through creating a full set of diskette media for booting a computer during recovery and running the Disaster Recovery Wizard. A full set of IDR diskette media includes the following:

- Windows Setup diskettes created by a utility that is on the Windows installation CD. IDR modifies these setup diskettes for use specifically with NetBackup for Windows.
- Intelligent Disaster Recovery diskettes that contain the computer specific information that is necessary to perform disaster recovery, including the DR file. (Alternatively, you can store the DR file on a diskette other than one of the IDR diskettes.)

If you select diskettes for the bootable media, you need five (for Windows NT) or six (for Windows 2000) blank, formatted 1.44 MB diskettes for each set of disaster recovery diskettes.

Note Windows XP and Windows Server 2003 do not support bootable diskettes.

Note The Windows installation CD is required both to prepare disaster recovery diskettes and for disaster recovery using those diskettes. You also need the Windows 2000 license key, either during bootable diskette preparation or during recovery.

▼ To create bootable diskettes

1. Format the diskettes that you are going to use.

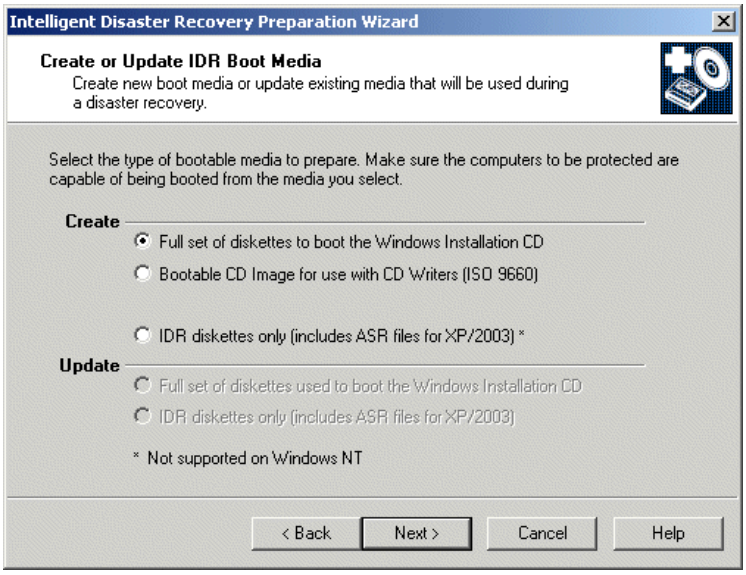
   Windows NT requires five diskettes and Windows 2000 requires six. Windows XP and Windows Server 2003 do not support bootable diskettes.

2. On the computer where you are going to prepare the diskettes, select **Start** > **Programs** > **VERITAS NetBackup** > **Intelligent Disaster Recovery PrepWizard**.

   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 **Create - Full Set of Diskettes to boot the Windows Installation CD** and click **Next**.

   The Starting Bootable Diskettes Creation screen appears.

5. Follow the prompts until the IDR Preparation Wizard is completed.

Windows 2000: If the **Let IDR Automatically Partition the Boot and System Drive** option is selected when recovery media is prepared, you must create a complete set of recovery diskettes for each Windows 2000 computer to be protected. However, if you do *not* select the **Let IDR Automatically Partition the Boot and System Drive** option, you can use the same diskettes 2 through 5 for all IDR-protected Windows 2000 computers — but you must reinstall any utility partitions by using the OEM-supplied installation media before recovery and then during recovery you must select the option to partition and format the drives manually. For details, see "Modifying Diskette Sets for Use with Multiple Windows 2000 Computers" on page 299.

Modifying Diskette Sets for Use with Multiple Windows 2000 Computers

If **Let IDR Automatically Partition the Boot and System Drive** option is *not* selected, you can use use the same diskettes 2 through 5 for all of the Windows 2000 computers that you want to protect. However, you have to create a different diskette 1 for each computer protected with IDR.

Diskette 1 contains a file named `winnt.sif`, which is the script used to automate the installation of Windows 2000 for disaster recovery when using the IDR option. This scripted installation of Windows 2000 requires that the name of the computer being recovered be listed in the `winnt.sif` file.

Therefore, for each Windows 2000 computer that will share diskettes 2 through 5, make a copy of diskette 1 (and its files). For each copy of diskette 1, edit the `winnt.sif` file and change the computer name to that of the machine to be protected. If the computer name is not modified, duplicate computer names on the network may occur and may prevent the recovered system from participating on the network.

Creating a Bootable CD Image

The IDR Preparation Wizard guides you through creating a bootable CD image. You then can write that image to a CD using the IDR Preparation Wizard or other writing software. If the system on which you are running the IDR Preparation Wizard does not have a CD-R or CD-RW drive, you can write the image onto a CD on a different machine using third-party CD writing software.

The CD image contains all the necessary IDR files unless you choose to store the Windows Server 2003 Automated System Recovery files on a diskette. If stored on the CD, the ASR files will always be read from the CD even if a more recent version is on an IDR diskette. For example, if you create IDR diskettes after you create the bootable CD, the ASR files will be read from the CD during recovery even though more recent versions may be on the IDR diskettes.

The Windows installation CD is required only during media preparation.

The license key for your Windows 2000, Windows XP, or Windows Server 2003 operating system is required. If you do not enter the license key while creating the bootable CD, you must enter it during recovery.

Note On Windows NT 4.0 systems, the IDR software cannot write to a CD; therefore, you must use other CD writing software to create the CD.

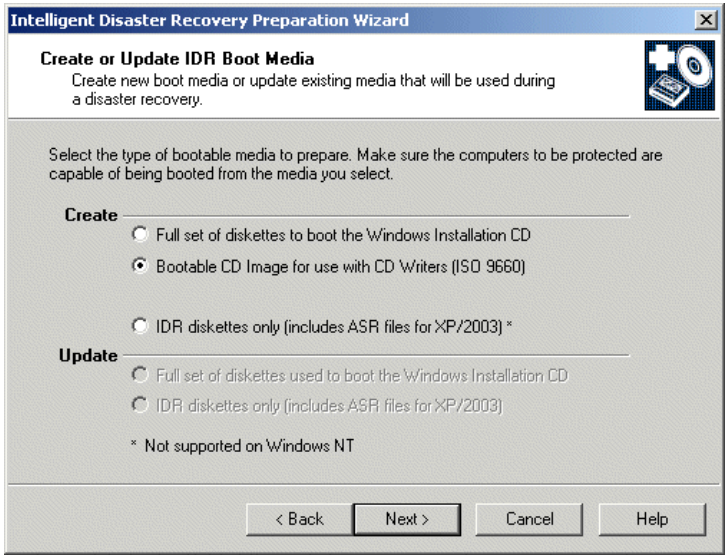
▼ To create a bootable CD image

1. On the computer where you are going to prepare the bootable CD image, select **Start** > **Programs** > **VERITAS NetBackup** > **Intelligent Disaster Recovery PrepWizard**.

   The Welcome screen for the IDR Preparation Wizard appears.

2. Click **Next** to continue.

   The Create or Update IDR Boot Media screen appears.



3. Select **Create - Bootable CD Image for Use with CD Writers (ISO 9660)** and click **Next**.

   The Starting CD Image Creation screen appears.

4. Follow the prompts until the IDR Preparation Wizard is completed.

Windows 2000: If you do *not* select **Let IDR Automatically Partition the Boot and System Drive**, before recovery you must reinstall any utility partitions by using the OEM-supplied installation media and then during recovery you must select the option to partition and format the drives manually. For details, see "Modifying Diskette Sets for Use with Multiple Windows 2000 Computers" on page 299.

Caution Test your bootable CD to ensure that your system can boot from it. (See "Step 1: Boot Your Computer" on page 306.)

Creating IDR Diskettes

Two formatted, 1.44 MB floppy diskettes are required to create IDR diskettes.

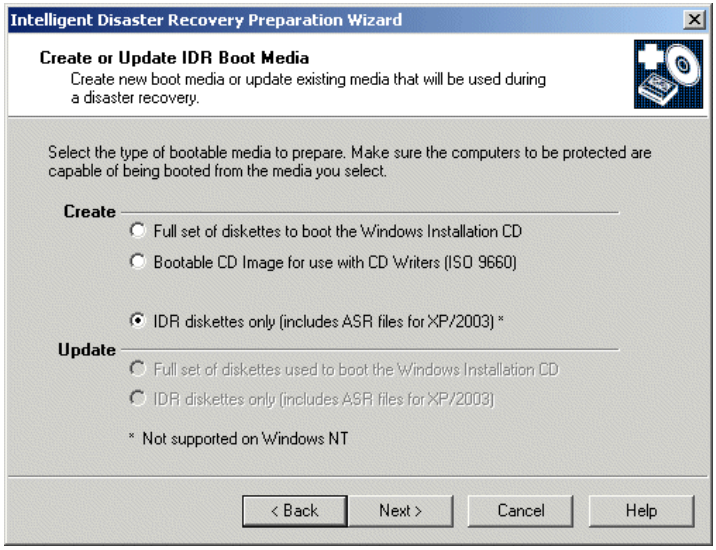
▼ To create IDR diskettes

1. On the computer where you are going to prepare the IDR diskettes, select **Start** > **Programs** > **VERITAS NetBackup** > **Intelligent Disaster Recovery PrepWizard**.

   The Welcome screen for the IDR preparation wizard appears.

2. Click **Next** to continue.

   The Create or Update IDR Boot Media screen appears.



3. Select **Create - IDR Diskettes Only (Includes ASR Files for XP/2003)** and click **Next**.

   The Creating the IDR Diskettes screen appears.

4. Follow the prompts until the IDR Preparation Wizard is completed.

Updating IDR Media

You should update your IDR media if your hardware configuration changes, if SCSI drivers were updated, or if other system drivers were updated.

Also, VERITAS recommends that you update the IDR diskettes periodically so they contain the latest DR files.

Updating a Bootable CD

You cannot update a bootable CD, you must create a new bootable CD image and then burn a new CD. If you install new hardware or change components on a protected system (such as a new SCSI card that is not supported by the Windows installation CD), create a new bootable CD as explained in "Creating a Bootable CD Image" on page 299.

Updating Bootable Diskettes

You can update the bootable diskette set by using the IDR Preparation Wizard. Use this option if you changed hardware, updated SCSI drivers, or updated other system drivers, and you already have a full set of bootable diskettes that you want to update.

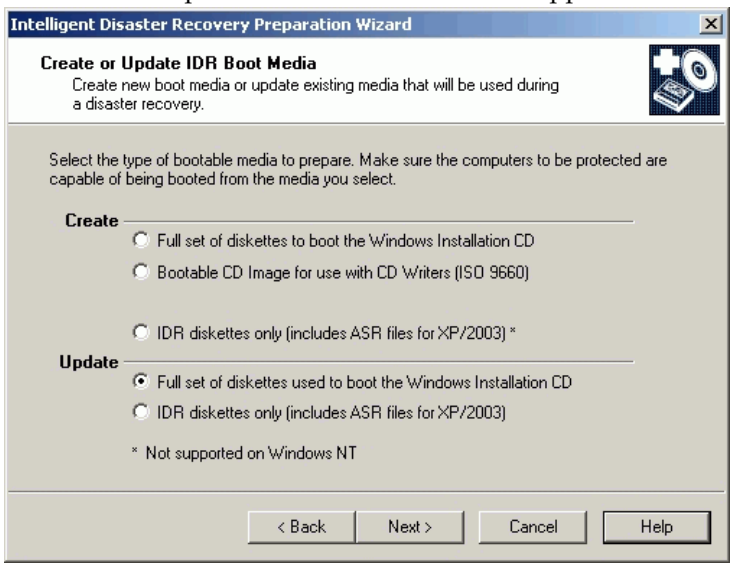
▼ To update IDR bootable diskettes

1. On the computer where you are going to prepare the IDR diskettes, select **Start** > **Programs** > **VERITAS NetBackup** > **Intelligent Disaster Recovery PrepWizard**.

   The Welcome screen for the IDR preparation wizard appears.

2. Click **Next** to continue.

The Create or Update IDR Boot Media screen appears.



3. Select **Update - Full Set of Diskettes Used to Boot the Windows Installation CD** and click **Next**.

4. Follow the prompts until the IDR Preparation Wizard is completed.

Updating IDR Diskettes Only

You can update the IDR diskettes with the latest DR file (and ASR files for Windows XP and Windows Server 2003 systems) by using the IDR Preparation Wizard.

Alternatively, to update the DR file only, you can run the `drfile.exe` file from a command prompt, which creates a new DR file, and then copy the DR file to the diskette. (See "Using drfile.exe to Create or Update a DR File" on page 304.)

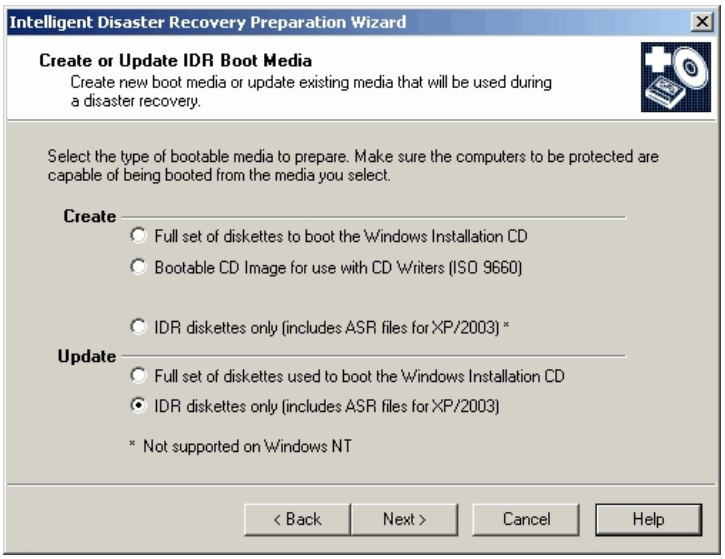
▼ To update IDR diskettes using IDR Preparation Wizard

1. On the computer where you are going to prepare the IDR diskettes, select **Start** > **Programs** > **VERITAS NetBackup** > **Intelligent Disaster Recovery PrepWizard**.

   The Welcome screen for the IDR Preparation Wizard appears.

2. Click **Next** to continue.

The Create or Update IDR Boot Media screen appears.



3. Select **IDR Diskettes Only (Includes ASR Files for XP/2003)** and click **Next**.

4. Follow the prompts until the IDR Preparation Wizard is completed.

Using drfile.exe to Create or Update a DR File

If IDR diskettes have already been created, you can update the DR file only by running the `drfile.exe` program on the client and then copying the DR file to the diskette that contains the DR file. The name of the DR file should always match 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.

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.

   The DR file name is of the form *`computer_name`*`.dr`, as in `bison.dr`. The name of the DR file will match the computer name of the client, which is the name required by IDR, even if the name is different from the one used in the NetBackup policy configuration.

2. Insert the diskette that contains the DR file into your drive and copy the DR file to it.

The diskette can be one of the IDR diskettes or a separate diskette. If using a separate diskette, insert the other diskette when prompted for the DR file during disaster recovery.

Recovering Your Computer

Restoring the computer to its pre-disaster status with IDR includes the following steps:

- Step 1: Boot Your Computer. Use the previously prepared IDR bootable media to boot the computer being recovered.
- Step 2: Windows Setup in IDR Recovery. Use the Windows Setup program to partition and format the system drive on the computer being recovered. The IDR bootstrap process loads and runs the Windows Setup program from the Windows installation CD.
- Step 3: Disaster Recovery Wizard. Use the NetBackup IDR Disaster Recovery wizard to restore your system to its pre-disaster state and restore your data files.

Automating the recovery with the Disaster Recovery wizard requires the following:

- A NetBackup server that can restore the latest backups to the computer being recovered.
- The latest DR file for the machine being recovered.

  If you have not updated the DR file since the last backup, it may contain out-of-date hard disk partition, network-interface-card driver, or backup set information.
- Bootable IDR CD media or the original Windows installation CD.
- The license key for your Windows operating system (if you did not enter the license key during preparation of the IDR bootable media).
- For Windows XP and Windows Server 2003 systems, the ASR files for the machine being recovered.
- If your network adapter requires special driver software, you need the installation media provided by the CD manufacturer. Special drivers are ones that are not on the operating system installation media, such as a driver for a network interface card (NIC) supplied by the manufacturer.

Note For Windows 2000 systems, if **Let IDR Automatically Partition the Boot and System Drives** was *not* selected during IDR preparation, before beginning the recovery process you must reinstall any utility partitions by using the OEM-supplied installation media. Then, during recovery, you must select the option to partition and format the drives manually.

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 device capable of booting from the bootable media.

Caution Disconnect any storage area network or cluster systems that are attached to the computer being recovered; if you do not, the hard drives on those computers may also be repartitioned and reformatted.

▼ To boot a computer using a bootable diskette

1. Insert the bootable diskette.
2. Start the computer.
3. Follow the boot process instructions on screen and continue with "Step 2: Windows Setup in IDR Recovery" on page 307.

▼ To boot from a bootable CD

1. Insert the bootable CD.
2. Start the computer and perform the tasks necessary to boot from the CD. For example, depending on the BIOS in the computer, you may have to press a function key to boot from the CD drive.

   The NetBackup Intelligent Disaster Recovery Bootstrap screen appears.
3. Do one of the following:
   - If you are testing the CD to determine if it can boot the computer, press Esc to exit and then remove the CD from the drive.
   - If you are performing disaster recovery, press Enter to continue with the boot process.
4. Depending on the system, do one of the following:
   - For Windows NT and Windows 2000, go to "Step 2: Windows Setup in IDR Recovery" on page 307.
   - For Windows XP and Windows Server 2003, press F2 to load the ASR files when prompted by the boot process. If you have an ASR diskette, place it in the floppy disk drive so the ASR files can be loaded.
5. Continue by going to "Step 2: Windows Setup in IDR Recovery" on page 307.

Step 2: Windows Setup in IDR Recovery

During the recovery process, the DR boot process uses the Windows Setup program to partition and format the system drive on the computer being recovered. If you booted from the IDR bootable CD, Windows Setup is started from that CD; if you booted from diskette, you will be prompted to insert the Windows installation CD so the Windows Setup can be started.

▼ **To use Windows setup in IDR recovery**

1. Follow the instructions on screen to continue the boot process.

   If you booted from diskette, you will be prompted to insert the Windows installation CD.

   At this point of the recovery, the Windows Setup program is loaded and performs the tasks necessary to partition and format drives and install a limited version of the operating system.

2. During Windows Setup, you may have to make choices about the following:

   - For Windows NT, **Express Setup** or **Custom Setup**. Usually, **Express Setup** is the best choice. Use **Custom Setup** if SCSI drivers are not present on the boot media or if you have RAID hardware that needs to be reconfigured.
   - For Windows NT, FAT or NTFS file system. If a new hard drive is detected on your system, you will be asked which file system format to use. Select FAT format for the C drive. IDR cannot repartition to the old layout if you build the partition as NTFS.

3. When prompted to reboot, ensure that no diskettes or CDs are in the drives and press **Enter** to reboot the system.

   After the reboot, the Disaster Recovery Wizard starts automatically.

4. Go to “Step 3: Disaster Recovery Wizard” on page 307.

Step 3: Disaster Recovery Wizard

After Windows Setup finishes its tasks, the Disaster Recovery Wizard is started as part of the recovery process. Follow the instructions to recover the computer; although these instructions do not provide a step-by-step procedure because different conditions affect the process, the process will be similar to the following.

▼ To use the Disaster Recovery Wizard

1. If you have a DR file, when prompted 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** to proceed. A message stating that the recovery file was not selected appears. Click **Yes** to continue in manual mode.

2. One or more screens about hard disk layout may appear:
   - You may be prompted about replacing the current hard drive partition with the partition information contained in the DR file or to keep the current hard drive partitions.
   - You may to prompted to run the Windows Disk Administrator (or Disk Manager) program, which allows you to make additional changes to your partition information. To make partition changes, click **Run Disk Administrator** (or **Run Disk Manager)**. (See "Notes on Altering Hard Drive Partition Sizes" on page 311.) Otherwise, click **Next** to continue the recovery process.

     For more information about Disk Administrator and fault tolerant configurations, see the operating system documentation.

3. For Windows 2000, Windows XP, and Windows Server 2003, a Completed IDR Phase 1 dialog appears. Do one of the following:
   - If your network adapter requires special driver software, click **Pre-install Custom Network Driver** and then follow the prompts to find and install the appropriate driver software. Special drivers are ones that are not on the operating system installation media, such as a driver for a network interface card (NIC) supplied by the NIC manufacturer.
   - To continue, click **Next** and go to step 5 to continue the recovery.

4. For Windows NT only, you will be asked to select either **Automatic Restore** or **Manual Restore** for network installation. Do one of the following:
   - If your network adapters use the drivers and software included with the operating system, select **Automatic Restore**, click **Finish** to complete the network installation, and then go to step 5 to continue the recovery.
   - If your network adapters require special drivers and software, select **Manual Restore**, select **Wired to the Network**, click **Next**, and proceed to step a.

a. 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.

b. The next screen lists the default network protocols. Select the networking protocols used on your network and click **Next**.

c. 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. (If you created a bootable CD, it may include the appropriate network drivers if they were found during the IDR preparation process.)

Note If additional screens about setting up your network interface card appear, respond as appropriate.

d. 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 appears.

e. Click **Next** to start the network and complete the installation of the networking components.

f. 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.

g. Click **Finish** to complete the network installation and continue with recovery.

5. Select either **Automatic** or **Manual**:

- If you selected **Automatic**, click **Next** and proceed to step 6.
- If you select **Manual**, click **Next** and proceed to step 8.

6. When recovering the registry, normally the restore process merges hardware information from the current *live* version of the registry into the *saved* version of the registry. (The saved version is the registry version that was backed up.) This ensures that the machine will reboot after the restore if the hardware changed.

If the hardware changed, select the server from which you want to restore files, then click **Start Restore** to submit the restore request to the selected server. By clicking **Start Restore**, the files will be restored and the hardware information from the current *live* version of the registry will be merged with the *saved* version of the registry. Go to step 7.

If the hardware on the machine that is being recovered has not changed, the live version and the saved version of the registry do not need to be merged because the hardware registry settings will be identical to what they were in the saved version of the registry. If you do not want to merge the registries, continue with step a:

a. Start a command window by pressing F1.

b. Navigate to the following directory (the default location; %SYSTEMROOT% is usually C:\Windows) :

```
%SYSTEMROOT%\System32\VERITAS\NetBackup\Bin
```

c. Type the following command, then press **Enter**.

```
W2KOption -restore -display -same_hardware 1
```

The following output appears:

```
NetBackup Restore Options
----------------------------------------
            SYSVOL Restore: Primary
         Hard Link Restore: Perform secondary restore
     Same Hardware Restore: Assume different hardware

NetBackup Restore Options
----------------------------------------
            SYSVOL Restore: Primary
         Hard Link Restore: Perform secondary restore
     Same Hardware Restore: Assume same hardware
```

d. Make sure that **Assume Same Hardware** is displayed in the `Same Hardware Restore` field, then continue with the restore process.

7. After the restore is complete, click **Next**. Go to step 10.

8. Select **Start NetBackup Interface** to start the NetBackup Backup, Archive, and Restore interface.

   Using this interface, you can make changes to the NetBackup configuration and you also have more control over the restore. (See the *NetBackup User's Guide for Microsoft Windows* for more information on using the interface.)

   When the restore is complete, close the Backup, Archive, and Restore interface and any other open NetBackup windows.

9. The **Next** button will be available when the restore is complete. Click **Next**.

10. Remove any diskettes from drive A and click **Finish** to reboot the computer.

Notes on Altering Hard Drive Partition Sizes

Note This section applies only to Windows NT and Windows NT 4.0. Reformatting and repartitioning is not supported on Windows 2000, Windows XP, or Windows Server 2003.

IDR defaults to restoring hard drive partitions to the same sizes they were before recovery. If the computer being recovered has a larger hard drive than before the recovery (for example, a larger hard drive was installed or the DR file is from a computer with a smaller hard drive), there will be unused and unallocated hard drive space. If so, you can run the Windows NT Disk Administrator program (during the IDR recovery process from within the Recovery Wizard) to alter the partition sizes to match the larger hard drive size. For information about 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 discusses restoring a Dell system, the steps outlined can be used with any system that requires 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 load the PowerRaid II driver manually, which is not bundled with the Windows operating system.

After loading the PowerRaid II driver, you must load the Adaptec controller driver manually. 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 that allows 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 before performing recovery.

Recovering Compaq Computers

If you are using a Compaq computer and the drive that contains 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

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.

I ran a full backup of my system but when I run the IDR Preparation Wizard again, I do not 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 304.

Why does the recovery wizard warn me that one or more of my hard drives are smaller than the originals?

If this is not actually the case, the reason may be because the minimal version of Windows that runs the recovery wizard has detected the hard drives in a different order than they were configured originally.

Be sure that your hard drive and controller configuration matches the original configuration before a disaster occurs.

If the original configuration does not match, you may be able to control the hard drive numbering. The following chart lists the normal order that Windows uses to assign disk drive numbers. Keep in mind that this chart can change if third party drivers are used.

Windows 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)

Windows Hard Drive Numbering Scheme (continued)	
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 only: If you cannot get the IDR Recovery Wizard to properly detect the hard drive order, you can still set up hard drive partitions manually by using the Windows NT Disk Administrator option within the Disaster Recovery Wizard. Then, you can continue with automated restore of your backup media.

If you have drives greater than eight GBs and the recovery wizard reports them as being only eight GBs, you must create bootable diskettes with the option **Use SCSI drivers currently installed on this system**.

Index

Symbols

.ExTeNt.nnnn files 244
.SeCuRiTy.nnnn files 244
@@MaNgLeD.nnnn files 244
@@MaNgLeD.nnnn_Rename files 244
@@MaNgLeD.nnnn_Symlink files 244

A

access control
  lists (ACLs) 244
  nbac_cron utility 49
  to a server or client 178
  user groups
    Administrator 55
    configuration 56
    Default User 55
    description 54
    Operator 55
    renaming user groups 57
    Security Administrator 54
    Vault Operator 55
accessibility features xxiii
Activity Monitor jobs database 100
adjust time zone 131
Administrator Access Control user group 55
Administrator's E-mail Address
  property 129
Allow Media Overwrite property 136
Allow Multiple Retentions per Media
  property 137
ALLOW_MEDIA_OVERWRITE 136, 169
ALLOW_MULTIPLE_RETENTIONS_PER_
  MEDIA 137, 170
ALLOW_NON_RESERVED_PORTS 137
  client 167
alternate client restores, host.xlate file 237
Andrew File System (AFS)
  backup selection list 284
  directives 284
  installing 283
  regular expressions 285
  restores 286
  troubleshooting 288
atime 175
authentication
  commands 78
  configuration files 72
  configuring enhanced 82
  port 48
  procedure 82
AUTHENTICATION_DOMAIN 137, 167
AUTHORIZATION_SERVICE 138
authorize.txt file 95
available_media script 254

B

backup selection list, AFS 284, 285
backup_exit_notify script 269
backup_notify script 268
backups
  AFS clients 286
  backup_exit_notify script 269
  backup_notify script 268
  bpend_notify script
    UNIX client 274
    windows client 276
  bpstart_notify script
    UNIX client 269
    windows client 271
  compressed 241
  diskfull_notify script 279
  estimating time required 244
  frequency
    guidelines for setting 253
  media requirements 254
  multiplexed 241
  multiplexing (see multiplexing)
  offsite storage 252

session_notify script 280
session_start_notify script 280
boot managers and IDR 313
booting a computer
with IDR bootable media 306
bp.conf entries
ALLOW_MEDIA_OVERWRITE 136
ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA 137
ALLOW_NON_RESERVED_PORTS 137
AUTHENTICATION_DOMAIN 137, 167
AUTHORIZATION_SERVICE 138
BPBRM_VERBOSE 139
BPDBJOBS_COLDEFS 140
BPDBM_VERBOSE 142
BPEND_TIMEOUT 145
BPRD_VERBOSE 143
BPSCHED_VERBOSE 144
BPSTART_TIMEOUT 145, 146
BPTM_QUERY_TIMEOUT 146
BPTM_VERBOSE 144
CHECK_RESTORE_CLIENT 146
CLIENT_CONNECT_TIMEOUT 146
CLIENT_PORT_WINDOW 146
CLIENT_READ_TIMEOUT 147
CLIENT_RESERVED_PORT_WINDOW 147
CONNECT_OPTIONS 148
CRYPT_CIPHER 171, 172
DISABLE_JOB_LOGGING 149
DISABLE_SCSI_RESERVE 150
DISABLE_STANDALONE_DRIVE_EXTENSIONS 150
DISALLOW_BACKUPS_SPANNING_MEDIA 150
DISALLOW_CLIENT_LIST_RESTORE 150
DISALLOW_CLIENT_RESTORE 151
FAILOVER_RESTORE_MEDIA_SERVERS 151
FORCE_RESTORE_MEDIA_SERVER 152
GENERATE_ENGLISH_LOGS 152
INCOMPLETE_JOB_CLEAN_INTERVAL 152
INITIAL_BROWSE_SEARCH_LIMIT 153
KNOWN_MASTER 153
LIMIT_BANDWIDTH 153, 154
MASTER_OF_MASTERS 154
MEDIA_ID_PREFIX 155
MEDIA_REQUEST_DELAY 155
MEDIA_SERVER 156
MEDIA_UNMOUNT_DELAY 155
MPX_RESTORE_DELAY 156
MUST_USE_LOCAL_DRIVE 156
QUEUE_ON_ERROR 156
RANDOM_PORTS 157
RE_READ_INTERVAL 157
REQUIRED_INTERFACE 158
SERVER 156, 159
SERVER_CONNECT_TIMEOUT 162
SERVER_PORT_WINDOW 160
SERVER_RESERVED_PORT_WINDOW 160
SKIP_RESTORE_TO_SYMLINK_DIR 161
SPC_SERVER 162
TIMEOUT_IN_QUEUE 162
UNLINK_ON_OVERWRITE 162
USE_VXSS 163, 179
VERBOSE 164
VXSS_NETWORK 164, 180
WAIT_IN_QUEUE 165
bp.conf file 136
personal
for UNIX nonroot user 136, 166, 168, 180
for UNIX root user 166
UNIX client options 129, 166
UNIX server options 136
bpadm, using
allowing multiple data streams 197
backup frequency, specifying 208
Backup Tries Global property 212
bpdbm, starting with bprd 218
bprd, managing 218
client compression 197
clients
adding clients 200
deleting from policies 202
install software 201, 214
collecting disaster recovery information 197
compress
backup files 197

Compress Image DB Files Global property 213
cross mount points 197
Display Reports Global property 213
follow NFS mounts 196, 197, 212
following NFS mounts 197
Global properties, specifying 210
indicating policy type 196, 212
install client software 201, 214
Keep Logs Global property 212
keep TIR Information, set time 212
keyword phrase, specifying 198
limit jobs per policy 197
Mail Address Global property 212
making a policy active 196
manual backups
    of clients 221
    of schedules 221
Max Drives this Master Global property 213
Maximum jobs per Client Global property 212
Maximum Number of Backup Copies Global property 213
Media Mount Timeout Global property 213
menu overview 184
mpx
    specify for schedule 209
    specify for storage unit 188
NetBackup-database backup
    adding file paths 229
    automatic 222
    changing backup attributes 226
    delete DB Backup ID 229
    manual 229
    removing file paths 231
Notify Request Daemon of Changes 213
policies
    adding 195
    adding clients 200
    deleting 199
    modify attributes 199
    schedules 205
    selection list 203
Preprocess Time Interval Global property 213
printing policy properties 199
priority for policy 198
reports, displaying 215
retention period, specifying 208
schedules
    adding 205
    display and modify 210
selection list
    adding 203
    changing 204
    deleting files 205
    raw partition backups 204
    wildcard characters 203
setting Advanced Client options 198
Shared Media Mount Timeout Global property 213
starting bpadm 184
storage unit groups
    deleting 194
    displaying configuration 193
storage units
    adding disk type 189
    adding Media Manager type 185
    changing attributes 190, 193
    deleting 191
    displaying configuration 190
    for policy 197
    for schedule 208
taking checkpoints during backups 198
true image recovery
    setting 196
utility 183
volume pool
    for policy 197
    for schedule 209
Wakeup Interval Global property 212
BPARCHIVE_POLICY 167
BPARCHIVE_SCHED 168
BPBACKUP_POLICY 168
BPBACKUP_SCHED 168
BPBRM_VERBOSE 139
BPDBJOBS_COLDEFS 140
BPDBM_VERBOSE 142
bpdynamicclient 117
bpend_notify script
    UNIX client 274
    windows client 276
BPEND_TIMEOUT 145
BPRD_VERBOSE 143
BPSCHED_VERBOSE 144
bpstart_notify script

UNIX client 269
Windows client 271
BPSTART_TIMEOUT 145, 146
BPTM Logging Level property 145
BPTM_QUERY_TIMEOUT 146
BPTM_VERBOSE 144
BUSY_FILE_NOTIFY_USER 169
busy-file processing
configuration overview 122
creating action files 125
logs 127
logs directory
busy log 127
logs file 127
retry file 127
modifying
bp.conf 123
bpend_notify_busy 128

C

catalogs
backup notification script 278
media 254
cautions
AFS backup volumes 285
overwriting files on AFS 287
CHECK_RESTORE_CLIENT 146
checkpoint restart
bp.conf entry for maximum incomplete status 152
CLIENT_CONNECT_TIMEOUT 146
CLIENT_NAME 170
CLIENT_PORT_WINDOW 146, 170
CLIENT_READ_TIMEOUT 145, 147, 170
on server 147
CLIENT_RESERVED_PORT_WINDOW 147, 171
clients
changing host names 236
dynamic UNIX client 117
IGNORE_XATTR bp.conf entry 175
IGNORE_XATTR_SOLARIS bp.conf entry 175
clients, NetBackup
bp.conf options
non-UNIX clients 134
UNIX clients 134
Compaq computers
recovering with IDR 312
COMPRESS_SUFFIX 171
compressed backups 241
configuration 136
host names 234
Intelligent Disaster Recovery 294
mail notifications 129
terminals 238
CONNECT_OPTIONS 148, 171, 172
CREATE_BACKUP_VOLUMES 284
CRYPT_KEYFILE 174
CRYPT_LIBPATH 173
CRYPT_STRENGTH 173
ctime 179
custom setup, when to use in IDR 307

D

Daylight Savings Time, setting 132
dbbackup_notify script 278
Default User Access Control user group 55
Dell PowerEdge 6100/200 with RAID
recovering with IDR 311
device delays 246
DHCP server 113
directives for AFS 284
DISABLE_JOB_LOGGING 149
DISABLE_SCSI_RESERVE 150
DISABLE_STANDALONE_DRIVE_EXTENSIONS 150
DISALLOW_BACKUPS_SPANNING_MEDIA 150
DISALLOW_CLIENT_LIST_RESTORE 150
DISALLOW_CLIENT_RESTORE 151
DISALLOW_SERVER_FILE_WRITES 174
disaster recovery
diskettes, updating 302, 303
procedure 305
Disk Administrator 311
disk overhead, for catalogs 254
diskfull_notify script 279
DO_NOT_RESET_FILE_ACCESS_TIME 175
Domain Name Service (DNS)
hostnames 237
drfile.exe command 304

E

e-mail notifications 129
encryption 243
English error log 152, 175
extended attribute files

Solaris 9 241
to ignore during backup 175
ExTeNt.nnnn files 244

F

FAILOVER_RESTORE_MEDIA_SERVERS 151
files
.ExTeNt.nnnn 244
.SeCuRiTy.nnnn 244
/usr/lib/X11/XKeysymbDB 238
@@MaNgLeD.nnnn 244
@@MaNgLeD.nnnn_Rename 244
@@MaNgLeD.nnnn_Symlink 244
catalog space requirements 254
files in /usr/openv/netbackup/bp.conf 136
host.xlate 237
terminfo 238
FlashBackup 241
fonts, changing for xbp 239
FORCE_RESTORE_MEDIA_SERVER 152

G

GENERATE_ENGLISH_LOGS 152, 175
Global Data Manager (GDM) 153, 154
Global Logging Level property 144, 164
Glossary. *See* NetBackup Help.
GNU tar 241

H

hashed file 80
host names
changing client name 236
changing server name 236
client peername 235
correct use 234
short 236
host.xlate file 237

I

IBM computers, recovering with IDR 312
IDR preparation wizard
preparing bootable media 295
updating disaster recovery diskettes 302, 303
INCOMPLETE_JOB_CLEAN_INTERVAL 152
INFORMIX_HOME 175
INITIAL_BROWSE_SEARCH_LIMIT 153
set on UNIX client 175
inode change time 179
Intelligent Disaster Recovery
bootable media
choosing type 296
creating CD image 299
creating diskettes 297
preparing 295
configuration 294
custom setup, when to use 307
diskettes, preparing 295
diskettes, updating 302, 303
DR files
obtaining from server 294
overview 294
update with drfile.exe 304
frequently asked questions 313
hard disk partition changes 308
hard drive partition, altering sizes 311
overview 293
preparation wizard 295
recovery wizard 305
requirements for using 292
supported Windows NT editions 292
updating IDR media
disaster recovery CD 302
recovery diskettes 302, 303
using drfile.exe 304
when to update 302
using boot managers 313
Windows NT
Disk Administrator 308
editions supported 292
setup 307
wizards
disaster recovery 305
IDR preparation 295

K

KEEP_DATABASE_COMM_FILE 176
KEEP_LOGS_DAYS 176
keyboard support
terminfo 238
XKeysymbDB 238
KNOWN_MASTER 153

L

LIMIT_BANDWIDTH 153, 154
LIST_FILES_TIMEOUT 176
LOCKED_FILE_ACTION 176
Logging

host properties
BPBRM Logging Level 139
BPDBM Logging Level 142
BPRD logging level 143
BPSCHED logging level 144
BPTM logging level 144
Global Logging Level 164
logs, retaining database extension logs 176

M

mail notifications, USEMAIL on UNIX clients 179
manual backups, with bpadm 221
MASTER_OF_MASTERS 154
Media
determining requirements 254
host properties
Allow Media Overwrite 136
Allow Multiple Retentions per Media 137
Disable SCSI Reserve/Release 150
Media ID Prefix 155
using tar to read images 241
Media ID Prefix option 155
Media Request Delay property 155
media servers, configuring 106
Media Unmount Delay property 155
MEDIA_ID_PREFIX 155
MEDIA_REQUEST_DELAY 155
MEDIA_SERVER 156, 176
MEDIA_UNMOUNT_DELAY 155
MEGABYTES_OF_MEMORY 177
methods.txt file 72
methods_allow.txt file 73
methods_deny.txt file 74
MPX_RESTORE_DELAY 156
mtime 179
multiple servers 105
multiplexing (MPX)
demultiplexing 105
Maximum Jobs per Client property 104
recovering backups 241
schedule media multiplexing 101
storage unit max per drive 101
Must Use Local Drive property 156
MUST_USE_LOCAL_DRIVE 156

N

named data streams
to ignore during backups 175
VxFS 4.0 241
names_allow.txt file 75
names_deny.txt file 76
nbac_cron utility 49
NBU_Admin Access Control user group 55
NBU_Operator Access Control user group 55
NBU_Security Admin Access Control user group 54
NBU_User Access Control user group 55
NDMP 241
NetBackup
authorization, process description 92
configuration options 134
network transfer rate 246
NFS_ACCESS_TIMEOUT 177
notification scripts 267

O

open files (see busy-file processing)
Operator Access Control user group 55
OS/2, boot manager and IDR 313
overhead, for catalogs 254
Overwrite Existing Files property 161
Overwrite Existing Files restore option 162

P

peername, client 235
planning, worksheets 255
preferred group, specify 96
PREFERRED_GROUP 96
priority for jobs in worklist 251

Q

QUEUE_ON_ERROR 156

R

RANDOM_PORTS 157
bp.conf entry 157
set use on client 177
raw partitions 241
RE_READ_INTERVAL 157
regular expressions, AFS file list 285
REMOVE_BACKUP_VOLUMES 285
REQUIRED_INTERFACE 158
bp.conf entry 158
set on client 177
Re-read Interval property 157
restore_notify script 279
RESTORE_RETRIES 177
restores

adjust time zone for 131
AFS clients 286
notes on AFS 287
restore_notify script 279
retention period
guidelines for setting 252
retry
restores 177

S

SANPoint Control
bp.conf entry 162
Schedule
default for user backups 168
schedules
automatic, how processed 249
retention period
guidelines 252
scripts
add_slave_on_clients 111
available_media 254
backup_exit_notify 267
backup_notify 267
bpend_notify 267
bpstart_notify 267
dbbackup_notify 267
diskfull_notify 267
notification 267
restore_notify 267
session_notify 267
session_start_notify 267
userreq_notify 267
SCSI Reserve/Release 150
Security Administrator Access Control user group 54
SeCuRiTy.nnnn files 244
Sequent 96
SERVER 156, 159
bp.conf option on client 178
SERVER bp.conf entry 159
Server Port Window property 160
Server Reserved Port Window property 161
server, NetBackup
controlling access 178
SERVER_CONNECT_TIMEOUT 162
SERVER_PORT_WINDOW 160, 178
SERVER_RESERVED_PORT_WINDOW 160
servers
changing host names 236
NetBackup
configuring bp.conf file 136
master 106
media 106
multiple 105
session_notify script 280
session_start_notify script 280
SKIP_RESTORE_TO_SYMLINK_DIR 161
SKIP_SMALL_VOLUMES 285
SLAVE_CONNECT_TIMEOUT, (see SERVER_CONNECT_TIMEOUT)
Solaris 9 extended attributes 241
SPC_SERVER 162
specify a preferred group 96
subnets
address formats 120
and bandwidth limiting 119
SYBASE_HOME 178
System Commander and IDR 313

T

tape marks 254
tape overhead, for catalogs 254
tar
GNU 241
to read backup images 241
terminals, configuring 238
terminfo file for bp users 238
time zones
adjustment for restores 131
setting Daylight Savings Time 132
timeout
bpend 145
client read 147, 170
Timeout in Queue property 162
TIMEOUT_IN_QUEUE 162
TIR (see True image restore)
transfer rate 245, 246
troubleshooting
AFS backups 288

U

unhashed file 80
UNLINK_ON_OVERWRITE 162
updating IDR bootable media 302
Use VERITAS Security Subsystem property 163
USE_CTIME_FOR_INCREMENTALS 179
USE_VXSS 163, 179

USEMAIL on UNIX clients 179
user groups
Administrator 55
Default User 55
description 54
Operator 55
renaming user groups 57
Security Administrator 54
Vault Operator 55
userreq_notify script 280

V

Vault Operator User Access Control user group 55
Vault_Operator Access Control user group 55
VERBOSE 164, 180
VERBOSE bp.conf entry 164
VERITAS Security Subsystem (VxSS)
AUTHENTICATION_DOMAIN 137, 167
AUTHORIZATION_SERVICE 138
USE_VXSS bp.conf entry 163, 179
VXSS_NETWORK bp.conf entry 164, 180
vopie method of authentication 82
vopie, definition 82
vopied 79
VxFS 4.0 named data streams 241
VxFS extent attributes 244
VXSS_NETWORK 164, 180

W

WAIT_IN_QUEUE 137, 138, 163, 164, 165, 167, 179, 180
wildcard characters
in AFS file list 285
wizards
disaster recovery 305
IDR preparation 295
worklist, prioritizing 251
worksheets, planning 255

X

X resources, xbp 239
xbp
changing X resources 239
XKeysymDB file for xbp users 238